Nations Unies A/CN.9/WG.IV/WP.141

Assemblée générale

Distr. limitée
30 janvier 2017
Français
Original: russe

Commission des Nations Unies pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Cinquante-cinquième session
New York, 24-28 avril 2017

Questions juridiques liées à la gestion de l'identité et aux services de confiance

Note du Secrétariat

La Fédération de Russie a soumis au Secrétariat un document à examiner à la cinquante-cinquième session du Groupe de travail. Le texte reçu par le Secrétariat est reproduit en annexe à la présente note.

V.17-00121 (F)

Annexe

Proposition de la Fédération de Russie

Amélioration des systèmes de gestion de l'identité par l'utilisation d'un espace de confiance transfrontière et d'une infrastructure de confiance commune pour les opérations électroniques internationales

Introduction

À sa soixante-douzième session, le 24 mai 2016, la Commission économique et sociale pour l'Asie et le Pacifique (CESAP) a adopté l'Accord-cadre sur la facilitation du commerce transfrontière sans papier en Asie et dans le Pacifique.

Cet instrument a pour objectif "de promouvoir le commerce transfrontière sans papier en créant les conditions voulues pour l'échange et la reconnaissance mutuelle des données et documents sous forme électronique relatifs au commerce et en facilitant l'interopérabilité entre des guichets uniques nationaux et sous-régionaux et/ou d'autres systèmes de commerce sans papier, en vue de rendre les transactions commerciales internationales plus efficaces et plus transparentes tout en améliorant le respect des réglementations".

L'article 5 de l'Accord-cadre cite, parmi les principes généraux qui le guident, "l'amélioration de l'espace de confiance transfrontière" (par. 1 g)).

Le présent document vise à poursuivre les travaux menés pour améliorer l'espace de confiance transfrontière dans le commerce électronique, point important de l'ordre du jour de la CESAP et de la Commission des Nations Unies pour le droit commercial international (CNUDCI).

Une version antérieure de la proposition, qui figure dans le document A/CN.9/WG.III/WP.136, a été soumise au Groupe de travail III de la CNUDCI (Règlement des litiges en ligne) pour qu'il l'examine à sa trente-deuxième session, tenue à Vienne (30 novembre-4 décembre 2015). Sur la recommandation du Groupe de travail, ce document a été transmis pour examen au Groupe de travail IV (Commerce électronique), vu le rapport qu'il présentait avec l'ordre du jour de ce dernier. Les principaux points abordés sont les mécanismes techniques, organisationnels et juridiques propres à renforcer l'espace de confiance transfrontière pour le commerce électronique dans la région de l'Asie et du Pacifique. À la cinquante-troisième session du Groupe de travail IV, la délégation de la Fédération de Russie a exprimé son intention de soumettre au Groupe, pour qu'il l'examine à sa session suivante, une proposition sur la gestion de l'identité, sous réserve que cette question soit inscrite à l'ordre du jour de cette session. Pour en faciliter l'examen, les délégations ont été invitées à soumettre des informations concernant cette question.

La sécurité de l'échange transfrontière de documents électroniques est une question hautement pertinente qui a été mise en évidence dans des déclarations mondiales et régionales, notamment pour ce qui est de:

– Promouvoir la recherche et la coopération pour permettre l'utilisation efficace des données et des logiciels, notamment aux fins des documents et des opérations électroniques, y compris les moyens électroniques d'authentification, et améliorer les méthodes de sécurité (document du Sommet mondial sur la société de l'information intitulé "SMSI+10, Vision pour le SMSI au cours de

l'après-2015", C5. Renforcer la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC), al. f));

– Promouvoir la confiance à l'égard de l'environnement électronique à l'échelle mondiale en favorisant les flux de données internationaux sécurisés, y compris les documents électroniques, et les efforts faits pour élargir et renforcer l'Infrastructure informatique de l'Asie-Pacifique ainsi que pour accroître la confiance dans les technologies de l'information et de la communication (Déclaration de Vladivostok faite par les dirigeants de l'Association de coopération économique Asie-Pacifique (APEC) en 2012, "Intégrer pour grandir, innover pour prospérer").

Il existe actuellement, dans le monde, plusieurs exemples de bonnes pratiques en la matière:

– Dans l'Union européenne, fondées sur le Règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (Règlement eIDAS)[1];

– Dans l'Union économique eurasienne, fondées sur le Traité sur l'Union économique eurasienne et sur le document-cadre exposant le concept relatif à l'utilisation des services et des documents électroniques ayant valeur légale dans le cadre des échanges d'informations entre États[2];

– Dans la région Asie-Pacifique, fondées sur l'Alliance panasiatique pour le commerce électronique[3].

Le développement de l'économie mondiale requiert, particulièrement en temps de crise, une intégration renforcée dans divers domaines économiques et sociaux, y compris par l'utilisation novatrice des technologies actuelles de l'information et de la communication (TIC).

L'un des principaux problèmes qui se posent, en ce qui concerne le commerce international, est celui de la sécurité et de la confidentialité des informations transmises via Internet. Pour résoudre ce problème, on utilise un système de gestion de l'identité. Celle-ci recouvre un ensemble de fonctions et de capacités (administration, gestion et maintenance, production de pièces, échanges de communications, corrélation et liaison, application de politiques, authentification et assertions, par exemple) utilisées pour:

• Garantir les informations relatives à l'identité (identifiants, justificatifs et attributs, par exemple);

• Garantir l'identité d'une entité (utilisateurs/abonnés, groupes, dispositifs utilisateurs, organisations, fournisseurs de réseaux et de services, éléments et objets de réseaux et objets virtuels, par exemple);

• Appuyer les applications commerciales et sécuritaires[4].

La gestion de l'identité a pour objectifs:

• Le contrôle de l'accès (le matériel ne doit être accessible que par des utilisateurs autorisés et aux fins prévues par les propriétaires);

---

[1] http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond.

[2] www.eurasiancommission.org/docs/Download.aspx?IsDlg=0&print=1&ID=5713.

[3] www.paa.net/.

[4] https://www.itu.int/rec/T-REC-X.1252-201004-I/fr.

- La confidentialité de l'accès;
- L'intégrité du système.

Pour ce faire, un système de gestion de l'identité doit:

- Garantir le fonctionnement requis du système en regard d'indicateurs de résilience définis;
- Assurer la fonction de gestion des données d'identification (création, modification, gel, archivage ou suppression d'informations d'identification);
- Assurer la protection des données d'identification;
- Garantir l'utilisation de mécanismes d'identification et d'authentification sécurisés (signature électronique, protection par double mot de passe et authentification biométrique, par exemple);
- Assurer l'interopérabilité des solutions de sécurité utilisées;
- Assurer l'intégrité du système et des informations d'identification.

Il existe deux types de système de gestion de l'identité: centré sur l'application et centré sur l'utilisateur[5].

Dans les grands systèmes de gestion de l'identité, un système centré sur l'application signifie que les services et les politiques sont conçus pour satisfaire aux exigences des fournisseurs d'identité et optimisés pour tenir compte de celles des applications (fourniture d'informations d'un compte utilisateur, par exemple). Il existe, dans ce système, un fournisseur d'identité et une partie qui se fie au système. Lorsqu'un service d'identité est fourni à l'utilisateur, l'échange d'identité s'effectue habituellement entre ces deux entités. L'identification doit s'entendre comme la représentation d'une entité sous la forme d'un ou de plusieurs éléments d'information qui permettent à l'entité ou aux entités de se distinguer suffisamment dans le contexte. Aux fins de la gestion de l'identité, cette dernière s'entend comme étant contextuelle (sous-ensemble d'attributs), l'éventail des attributs étant limité par un cadre aux frontières définies (contexte) dans lequel l'entité existe et interagit. Traditionnellement, les technologies de gestion de l'identité et de l'accès s'attachent principalement à authentifier les utilisateurs finaux pour un accès fédéré aux applications et aux services (dans le modèle de l'accès fédéré, il existe plusieurs fournisseurs d'identité auxquels un utilisateur peut se fier et qui peuvent, au besoin, gérer les informations partielles d'identité d'utilisateurs. Les informations que possède chaque fournisseur d'identité peuvent être partagées). L'exigence de sécurité, par conséquent, se limite au périmètre de ses domaines d'application.

La gestion de l'identité centrée sur l'utilisateur est principalement axée sur les utilisateurs finaux et optimisée pour tenir compte de leurs besoins. Cela signifie que l'objectif principal d'un tel système est de fournir des services d'identité pratiques et complets aux utilisateurs. Le principal point est de permettre à l'utilisateur de contrôler totalement son identité. Lorsqu'une information d'identité d'un utilisateur est diffusée, elle doit passer par ce dernier pour lui donner la possibilité de faire appliquer, au besoin, une politique personnelle, comme un choix de préférences personnelles en matière de confidentialité ou d'autorisation personnelle. Dans le système centré sur l'utilisateur, il faut que ce dernier dispose d'un programme client pour pouvoir récupérer des informations d'identité dans le serveur. Il a donc besoin de directives simples et complètes pour installer et déployer en toute sécurité ledit programme. Ce programme doit gérer certaines des informations relatives à la sécurité

[5] https://www.itu.int/rec/T-REC-X.1253-201109-I/fr.

de l'utilisateur. L'approche centrée sur l'utilisateur se distingue des autres modèles de gestion de l'identité en soulignant que c'est l'utilisateur, et non une autorité, qui contrôle la façon dont les attributs d'identification d'un utilisateur sont créés, diffusés, actualisés et supprimés. Cela signifie que l'utilisateur a pleine autorité sur le cycle de vie de son identité. Le niveau de contrôle pourra dépendre des exigences de confidentialité de l'utilisateur.

Les questions de gestion de l'identité ont d'abord été examinées dans le cadre de l'Union internationale des télécommunications (UIT) et de son Secteur de la normalisation des télécommunications (UIT-T) en 2006, lorsque le Groupe spécial sur la gestion de l'identité a été créé par la Commission d'études 17 de l'UIT-T, qui travaille sur les questions de sécurité des télécommunications et des TIC. L'objectif du Groupe spécial était d'examiner les questions de gestion de l'identité et les principes communs dans les télécommunications et les TIC. Les activités du Groupe spécial se sont transformées en une initiative mondiale de l'UIT sur la gestion de l'identité qui a été lancée en 2008. Les commissions d'études 2, 9, 11, 13, 16 et 17 de l'UIT-T ont collaboré à cette initiative. L'Activité conjointe de coordination pour la gestion de l'identité est dirigée par la Commission d'études 17 depuis 2009. Dans le cadre de cette activité, il a été élaboré un plan de normalisation de la gestion de l'identité, avec des contributions des organisations suivantes: Alliance for Telecommunications Industry Solutions (ATIS), Institut européen des normes de télécommunications (ETSI), Internet Engineering Task Force (IETF), Commission électrotechnique internationale (ISO), UIT, National Institute of Standards and Technology (NIST), Organization for the Advancement of Structured Information Standards (OASIS), Kantara Initiative et Third Generation Partnership Project (3GPP) (on trouvera une description des activités et des normes de gestion de l'identité publiées par l'UIT et ces organisations sur le site Web de l'UIT: http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/ict-part06.aspx).

La création d'un espace de confiance transfrontière dans le domaine du commerce électronique aidera à simplifier les procédures et à développer le commerce international, et facilitera l'identification et la gestion de l'identité pour les pays participants. Le terme "confiance", dans le contexte de la sécurité, peut s'entendre comme une certitude quant à la fiabilité et à la véracité d'une information ou à la capacité et à la volonté d'une entité d'agir de façon appropriée dans une situation donnée. En créant un espace de confiance entre les États, on aidera ainsi à harmoniser l'utilisation des mécanismes de sécurité (tous les pays, par exemple, appliqueront une approche commune pour le choix de mécanismes tels que les signatures électroniques et la protection par double mot de passe) et à accroître le niveau de confiance (confiance continue et mesurable dans la réputation, les capacités, la validité ou l'authenticité de quelqu'un ou de quelque chose) entre les acteurs du commerce électronique.

Dans le contexte du commerce électronique, un espace de confiance transfrontière doit s'entendre comme une combinaison de conditions juridiques, organisationnelles et techniques recommandées par les institutions spécialisées et les organismes compétents des Nations Unies pour garantir la confiance dans l'échange international de documents et de données électroniques entre des parties (entités) qui interagissent par voie électronique dans leur activité commerciale. Son objectif principal est de proposer aux utilisateurs différents niveaux (élémentaire, moyen, élevé) de services de confiance à l'aide d'un système de gestion de l'identité lorsqu'ils interagissent par voie électronique. Cela permettra de donner à l'interaction électronique une signification légale à la discrétion des utilisateurs, quelles que soient leur situation géographique et la juridiction dont ils relèvent. L'un des principaux axes

de recherche dans ce domaine sera l'étude de mécanismes possibles de gestion de l'identité.

Il est proposé que l'on entende par "parties (entités) qui interagissent par voie électronique" toutes autorités publiques et personnes physiques et morales qui, dans une activité commerciale, interagissent dans le cadre de rapports découlant de la création, de l'envoi, de la transmission, de la réception, du stockage et de l'utilisation de documents et de données électroniques.

Ces propositions ont pour but d'aider à définir les approches et les questions à examiner dans le cadre de l'élaboration, par les organismes compétents des Nations Unies, d'un ensemble de recommandations relatives à la création et au fonctionnement d'un espace de confiance transfrontière dans le commerce électronique. Elles doivent faciliter la mise en place de l'infrastructure technologique, institutionnelle et juridique requise pour faire appliquer ces recommandations et, en particulier, simplifier le système de gestion de l'identité pour assurer la sécurité des transactions commerciales électroniques.

Approches conceptuelles

1. Il est proposé que les recommandations ci-dessus visent à garantir les droits et les intérêts légitimes des citoyens et des organisations qui relèvent de la compétence d'États Membres de l'ONU lorsqu'ils transmettent des informations ayant une valeur juridique sous forme électronique au moyen d'Internet et d'autres systèmes informatiques ouverts à usage de masse.

2. Ces garanties institutionnelles seront données dans le cadre des activités commerciales d'opérateurs spécialisés qui:

- Fournissent aux utilisateurs des services informatiques de confiance pour la gestion de l'identité;
- Respectent des régimes juridiques établis qui prévoient, entre autres dispositions, des restrictions au traitement des données personnelles.

3. Il est proposé de décrire les divers régimes juridiques possibles:

- Ceux fondés sur des accords internationaux (conventions) et/ou sur des règlements internationaux directement applicables;
- Ceux fondés sur des accords commerciaux et/ou sur les pratiques commerciales courantes;
- Ceux qui ne sont pas régis par une réglementation internationale particulière.

Avec la reconnaissance mutuelle de documents électroniques authentifiés par des services informatiques de confiance, les régimes juridiques peuvent également être appuyés par des institutions traditionnelles (organes gouvernementaux, organismes de règlement judiciaire, d'assurance-risques, institutions notariales, etc.).

Ces régimes peuvent également prévoir la mise en place d'exigences particulières concernant l'appui matériel et financier aux activités commerciales d'opérateurs spécialisés en cas de dommages causés à leurs clients, notamment en cas d'atteinte à l'intégrité de données personnelles.

Il est proposé que les questions de garantie institutionnelle et de régime juridique afférentes à la création et au fonctionnement de grappes régionales et mondiales d'espaces de confiance pour le commerce électronique, ainsi qu'aux services fonctionnels fournis dans le cadre de ces grappes, soient traitées dans une recommandation distincte de la CNUDCI.

4. Il est proposé de décrire les ensembles possibles de services informatiques de confiance en fonction du degré d'importance des applications fonctionnelles. L'un des axes de recherche les plus importants à cet égard sera l'étude de mécanismes possibles de gestion de l'identité. Les services informatiques de confiance et le niveau actuel de confiance dans ces services peuvent être déterminés par les opérateurs fonctionnels des systèmes d'information (opérateurs qui organisent et/ou assurent le stockage et le traitement des données d'identité dans un système d'information et définissent les objectifs et les actions (opérations) effectuées avec ces données dans ce système) en fonction des menaces, des risques, des régimes juridiques et des besoins des utilisateurs. Pour garantir le niveau de confiance requis, les opérateurs de gestion de l'identité pourront fonctionner dans un environnement international neutre défini par des régimes juridiques donnés. Il est proposé de décrire les structures organisationnelles requises pour créer et maintenir un tel environnement.

Des dispositions communes concernant la création et le fonctionnement de grappes régionales et mondiales d'espaces de confiance pour le commerce électronique, les services fonctionnels fournis dans le cadre de ces grappes et les services informatiques de confiance pourront être envisagées dans le cadre de la Recommandation conjointe du Centre pour la facilitation du commerce et les transactions électroniques (CEFACT) de la Commission économique pour l'Europe (CEE) en vue d'assurer des échanges électroniques transfrontières de confiance à valeur légale.

La mise en œuvre de la gestion de l'identité et la description de certains services informatiques de confiance pourront faire l'objet de normes et de recommandations techniques de l'UIT, du Comité technique mixte 1 (JTC-1) de l'Organisation internationale de normalisation (ISO) et de la Commission électrotechnique internationale (CEI), de l'Institut européen des normes de télécommunication (ETSI) et d'autres organismes.

5. Les ensembles d'attributs utilisés aux fins de la gestion de l'identité devront être définis par les régimes juridiques qui régissent les activités commerciales des opérateurs spécialisés dans l'identification et des opérateurs fonctionnels, leur maintenance pouvant être assurée par les services informatiques de confiance appropriés. Les activités des opérateurs peuvent être réglementées par des prescriptions organisationnelles et techniques particulières axées, notamment, sur la protection des données personnelles.

Les ensembles d'attributs utilisés aux fins de la gestion de l'identité et les procédures d'identification elles-mêmes peuvent servir de base pour définir les niveaux de confiance dans les systèmes correspondants. Ces niveaux de confiance pourront revêtir une grande importance pour ce qui est de réglementer l'interaction entre différentes grappes de confiance (voir section 9).

6. Il est proposé de décrire les mécanismes d'interaction des États et de leurs alliances internationales avec d'autres organismes internationaux dans le cadre de la création d'un espace de confiance commun:

6.1. Sur la base de l'adhésion à un régime juridique existant qui fournit des garanties institutionnelles aux parties qui interagissent par voie électronique:

– L'adhésion totale d'un État à un régime juridique existant sur la base de traités internationaux et/ou de règlements internationaux directement applicables dans lesquels la création d'un espace de confiance régional, y compris les services fonctionnels fournis dans le cadre de cet espace, est soit envisagée, soit prévue;

– L'adhésion partielle d'un État à un régime juridique existant sur la base de traités internationaux et/ou de règlements internationaux directement applicables par

l'adoption de dispositions spécifiques relatives à la création d'un espace de confiance régional et/ou fonctionnel.

6.2. Sur la base de l'interaction entre diverses alliances internationales:

– Dans un premier temps, un groupe d'États crée une grappe régionale d'espaces de confiance isolée, y compris les services fonctionnels fournis dans le cadre de ces espaces, donnant des garanties institutionnelles aux parties qui interagissent par voie électronique selon le régime juridique spécifié par ces États et assurant la sécurité des transactions commerciales électroniques;

– Dans un second temps, les protocoles et mécanismes d'interaction de confiance avec d'autres alliances internationales sont définis en liaison avec la reconnaissance mutuelle de différents régimes juridiques. Cette reconnaissance mutuelle devra tenir compte des garanties institutionnelles et des critères qu'applique, en matière de sécurité des informations, chacun de ces organismes internationaux, utilisant éventuellement des passerelles de sécurité de l'information opérant dans le cadre de régimes juridiques spéciaux et responsables de la gestion de l'identité.

6.3. Sur la base de l'interaction entre un État et d'autres États ou associations internationales:

– Dans un premier temps, un État crée une grappe nationale d'espaces de confiance isolée qui opère dans le cadre d'un régime juridique national déterminé par ledit État;

– Dans un second temps, les protocoles d'interaction de confiance avec d'autres États et/ou associations internationales sont définis en liaison avec la reconnaissance mutuelle de différents régimes juridiques. Cette reconnaissance mutuelle devra tenir compte des garanties institutionnelles et des critères qu'appliquent, en matière de sécurité des informations, ces États et organismes internationaux, utilisant éventuellement des passerelles de sécurité de l'information opérant dans le cadre de régimes juridiques spéciaux et responsables de la gestion de l'identité.

7. Il est proposé de décrire les mécanismes de formation de grappes, semblables à ceux décrits à la section 6, pour les régimes juridiques fondés sur des accords commerciaux et/ou les pratiques commerciales courantes.

8. Il est proposé de décrire les mécanismes de création d'un espace de confiance mondial sur la base de l'intégration des différentes grappes en une matrice unique construite selon les paramètres suivants:

– Types de services fonctionnels et portée régionale;

– Types de régimes juridiques et leurs variantes.

9. Il est proposé de décrire les méthodes utilisées pour créer plusieurs types de passerelles de sécurité de l'information, éléments clefs de la construction d'une matrice mondiale d'espace de confiance, afin d'assurer la sécurité des transactions commerciales électroniques.

La création de passerelles de ce type pourra notamment avoir pour objectifs de faire en sorte que les conditions d'interaction entre les différentes grappes mondiales d'espaces de confiance soient respectées et que cette interaction soit sûre. Les aspects technologiques, organisationnels et juridiques requis pourront tous être pris en considération lors de la création des passerelles.

Il faudra que les méthodes de création de passerelles génériques intègrent les divers niveaux d'interaction possibles entre les différentes grappes d'espaces de confiance. La création de passerelles de gestion de l'identité pourra, par exemple, s'effectuer uniquement aux niveaux juridique et organisationnel ou à un niveau plus complexe, à savoir juridique, organisationnel et technologique.

Il faudra également que ces méthodes incluent l'utilisation de profils de transition qui décrivent et définissent la transition d'une grappe à une autre. Ces profils pourront tenir compte du degré de confiance accordé dans les systèmes d'identification utilisés dans les grappes qui interagissent (voir section 5).

La description de plusieurs types de passerelles de sécurité de l'information pourra faire l'objet de normes et de recommandations techniques de l'UIT et du Comité technique mixte 1.

Création d'un espace de confiance transfrontière au moyen d'une infrastructure unifiée

Comme cela est dit plus haut, la création d'un espace de confiance transfrontière a principalement pour objet d'utiliser un système de gestion de l'identité qui propose aux utilisateurs différents niveaux (élémentaire, moyen et élevé) de services de confiance pendant leur interaction électronique.

L'espace de confiance transfrontière est une plate-forme fondamentale facile à faire évoluer qui offre un accès unifié et sécurisé à des services de confiance électroniques grâce à la gestion de l'identité. Puisque les systèmes et mécanismes existants de gestion de l'identité sont pris en compte, on s'attend à ce que les exigences de mise à niveau à respecter pour les inclure dans l'espace de confiance transfrontière soient minimes.

Lors de l'élaboration de l'espace de confiance transfrontière, on a proposé l'architecture d'une infrastructure de confiance commune, décrit les interconnexions entre ses différentes composantes et leur interaction avec les utilisateurs, et travaillé simultanément dans trois domaines: technologique, organisationnel et juridique. L'analyse des options de mise en œuvre et des scénarios d'utilisation de l'infrastructure a permis de produire une liste des documents requis pour une spécification complète du système. L'architecture de l'infrastructure a été conçue de façon qu'il soit facile de l'ajuster. On peut facilement la porter à tout niveau par l'ajout de nouvelles composantes (systèmes juridiques, participants supranationaux ou opérateurs de services de confiance et d'identité).

Aspects techniques et technologiques de l'infrastructure de confiance commune

Il peut exister, pour la gestion de l'identité et la prestation de services de confiance, de nombreux mécanismes technologiques. Le principal critère, pour les éléments de l'infrastructure de confiance commune, est qu'ils garantissent l'interopérabilité. La réglementation, à ce niveau, s'effectue par l'application des différentes normes et instructions énoncées dans les documents du Conseil de coordination des régulateurs de l'échange de données informatisé en confiance. Dans les interactions transfrontières, le fonctionnement technologique des services de confiance peut passer par la vérification de la signature électronique. À des fins de comparaison, il est proposé, pour la mise en œuvre de l'infrastructure de confiance commune, deux options: un système décentralisé offrant un niveau de confiance théoriquement faible entre les participants à un échange d'informations (voir fig. 1) et un système centralisé offrant un niveau de confiance moyen entre les parties (voir fig. 2).

Le tableau 1 présente, en ce qui concerne l'infrastructure de confiance commune, les caractéristiques des systèmes décentralisés et centralisés. La procédure d'utilisation d'une signature électronique comme mécanisme de gestion de l'identité pour les deux schémas de mise en œuvre de l'infrastructure est décrite au tableau 2.

Tableau 1
Caractéristiques d'un mécanisme de gestion de l'identité dans une infrastructure de confiance commune utilisée pour l'échange d'informations, avec des niveaux de confiance faibles et moyens

Niveau de confiance faible (fig. 3)	Niveau de confiance moyen (fig. 4)
1. Des services d'apostille sont fournis par les opérateurs nationaux de services d'apostille. Ces opérateurs peuvent également fournir d'autres services de gestion de l'identité. 2. Absence d'organisations internationales (opérateurs et régulateurs). 3. Les régulateurs nationaux interagissent directement et échangent les certificats entre eux. 4. Les régulateurs nationaux fournissent aux opérateurs nationaux de services de confiance de leur pays leur certificat et les certificats des régulateurs nationaux d'autres pays.	1. Des services d'apostille sont fournis par les opérateurs internationaux de services d'apostille. Ces opérateurs peuvent également fournir d'autres services de gestion de l'identité. 2. Présence d'organisations internationales: régulateur international de l'infrastructure de confiance commune et opérateurs internationaux de services de confiance. 3. Les régulateurs nationaux de l'infrastructure de confiance commune interagissent uniquement par l'intermédiaire du régulateur supranational de l'infrastructure. De même, les opérateurs nationaux de services de confiance interagissent uniquement par l'intermédiaire de leur opérateur international. 4. Le régulateur international de l'infrastructure de confiance commune fournit des certificats de manière centralisée aux opérateurs nationaux de services de confiance et aux régulateurs nationaux de l'infrastructure. 5. Les régulateurs nationaux fournissent aux opérateurs nationaux de services de confiance de leur pays leur certificat et le certificat du régulateur international.

Tableau 2
Procédure d'utilisation d'une signature électronique comme mécanisme de gestion de l'identité dans les deux schémas de mise en œuvre de l'infrastructure

Niveau de confiance faible (fig. 3)	Niveau de confiance moyen (fig. 4)
1. Le particulier/l'entité 1 envoie les documents portant la signature électronique du pays J, sélectionnant le niveau de qualification proposé par l'infrastructure de confiance commune (élémentaire, moyen ou élevé). 2. Une demande de vérification de documents portant la signature électronique du pays J est envoyée à l'opérateur national du service d'apostille du pays Q. 3. La demande de vérification de documents est envoyée à l'opérateur national du service d'apostille du pays J. 4. Vérification mathématique de la signature électronique dans le pays J. 5/6. Une demande/réponse relative au statut du certificat est envoyée à l'opérateur national du service de signature du pays J. 7. L'opérateur national du service d'apostille du pays Q reçoit une confirmation de la validité de la signature électronique du pays J. 8. L'opérateur national du service d'apostille du pays Q certifie la demande et la fait suivre au particulier/à l'entité 2.	1. Le particulier/l'entité 1 envoie les documents portant la signature électronique du pays J, sélectionnant le niveau de qualification proposé par l'infrastructure de confiance commune (élémentaire, moyen ou élevé). 2. Une demande de vérification de documents portant la signature électronique du pays J est envoyée à l'opérateur international du service d'apostille I-J-Q. 3. Vérification mathématique de la signature électronique dans le pays J. 4/5. Une demande/réponse relative au statut du certificat est envoyée à l'opérateur national du service de signature du pays J. 6. L'opérateur international du service d'apostille I-J-Q certifie la demande et la fait suivre au particulier/à l'entité 2.

Figure 1

Vérification de la signature électronique dans le cadre d'un espace transfrontière à faible niveau de confiance (option décentralisée)

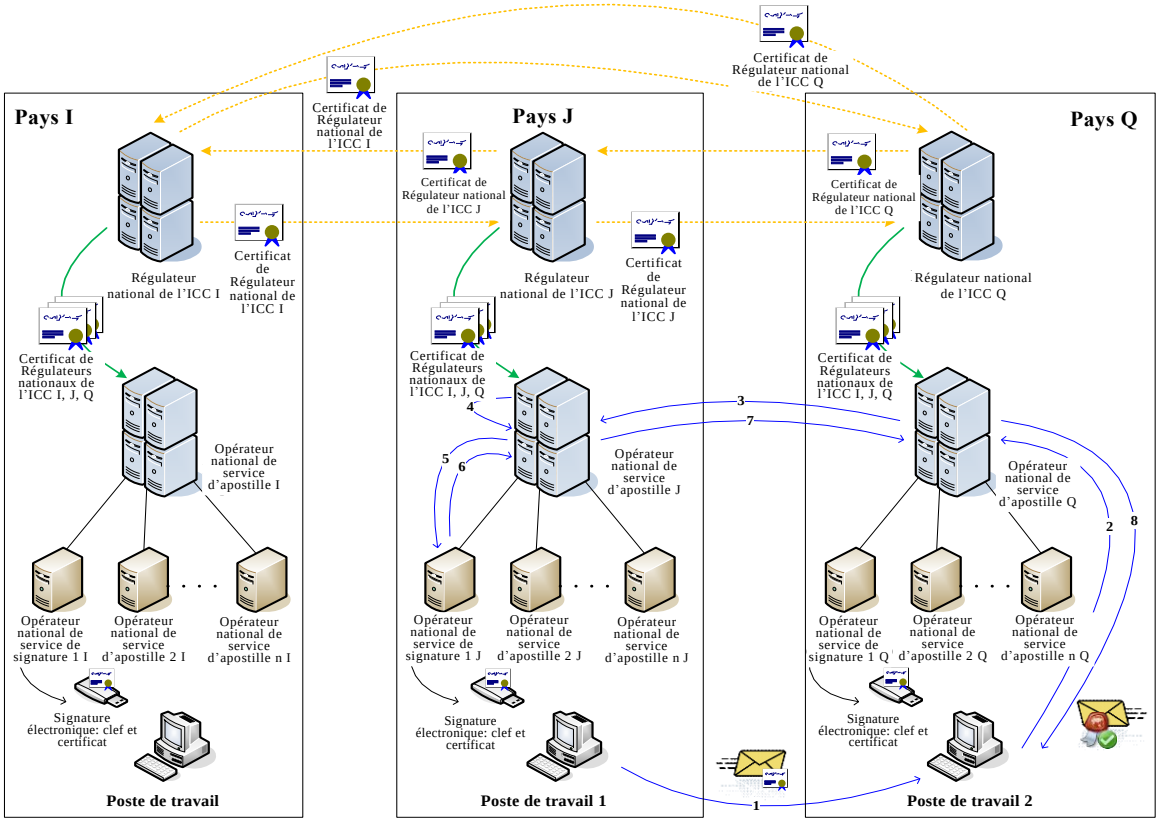
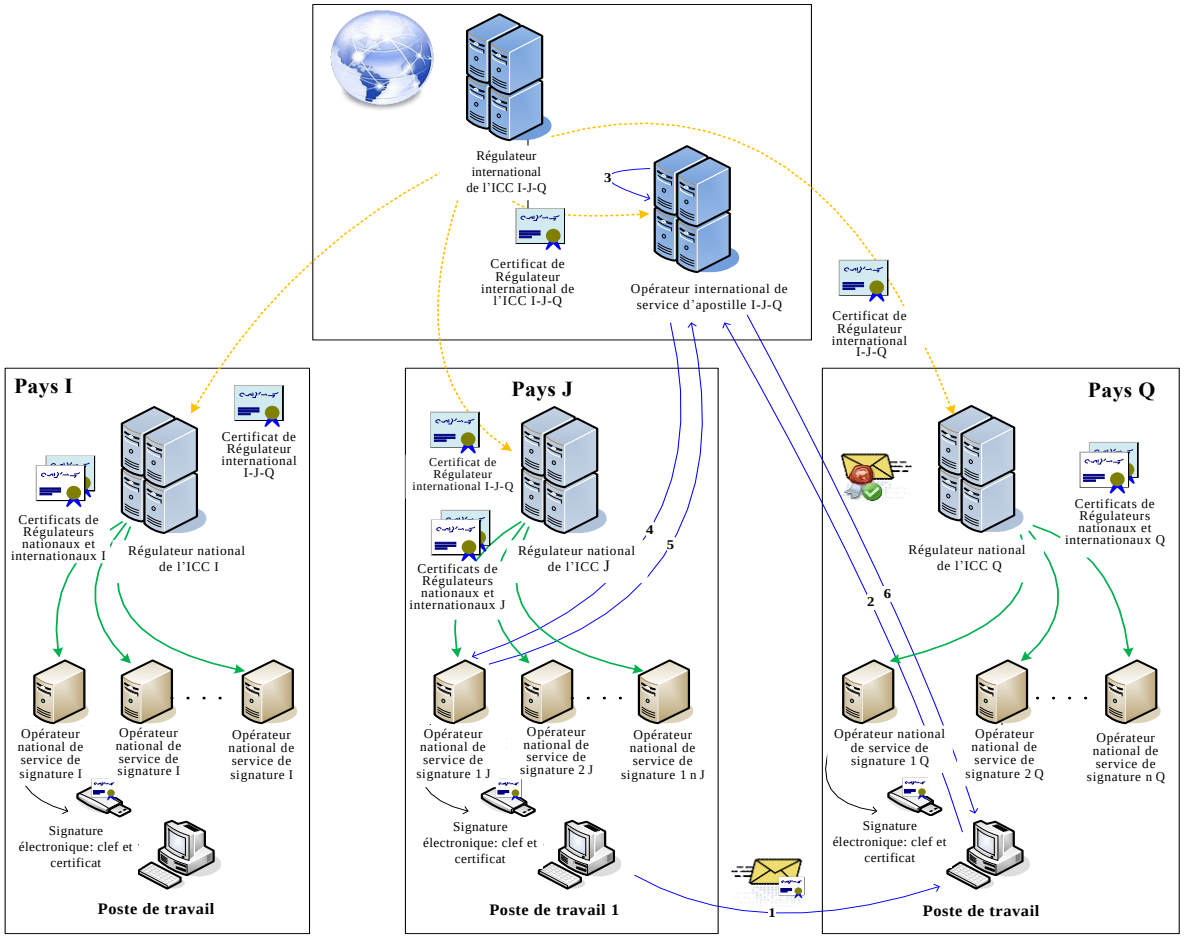


Figure 2
Vérification de la signature électronique dans le cadre d'un espace transfrontière à niveau de confiance moyen (option centralisée)

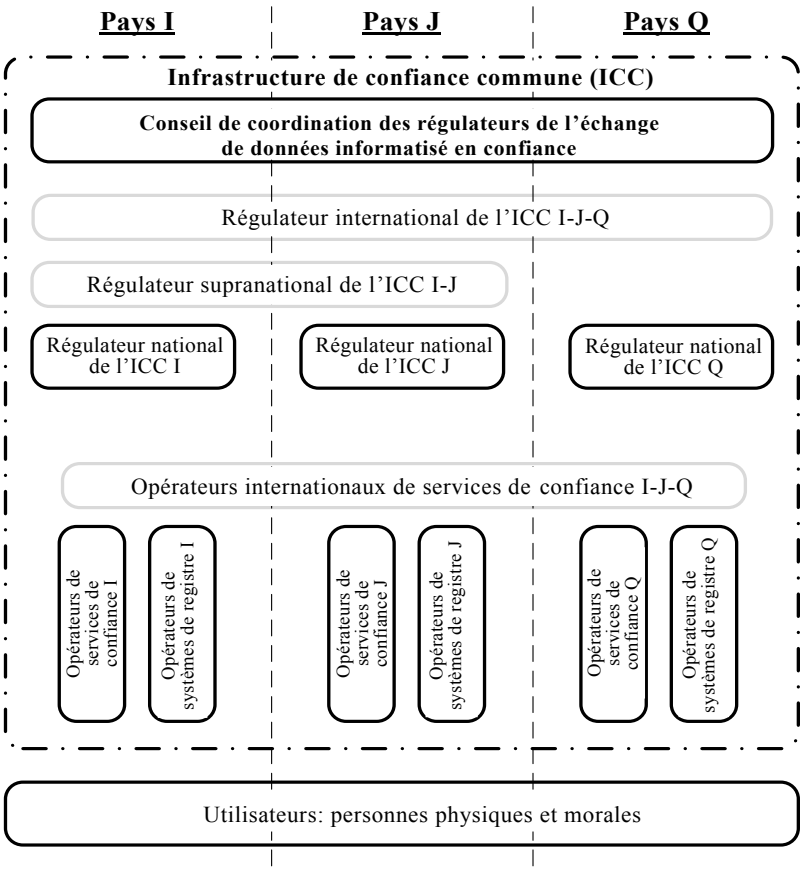


Aspects organisationnels

La reconnaissance mutuelle à valeur juridique de services de confiance relevant de la compétence des différents États passe par la création et la mise en œuvre du Conseil de coordination des régulateurs de l'échange de données informatisé en confiance, dont les activités sont régies par une charte qui doit être reconnue et signée par tous les membres agréés, à savoir les organismes de réglementation de l'échange de données informatisé, représentés essentiellement par les régulateurs nationaux de l'infrastructure de confiance commune.

Le schéma suivant représente la réglementation organisationnelle (voir fig. 3):

Figure 3
Réglementation organisationnelle de l'espace de confiance transfrontière
(les éléments facultatifs apparaissent dans les cadres grisés)



Le Conseil de coordination émet des documents liés à sa charte, qui concernent notamment:

- Les conditions que les membres du Conseil doivent remplir pour en être membres à part entière;
- Des lignes directrices concernant la supervision "parallèle" à mener en vue de l'admission au Conseil et les vérifications mutuelles périodiques à effectuer pour maintenir la participation volontaire au Conseil;
- Les critères de conformité que doivent respecter les opérateurs des services liés à l'infrastructure de confiance commune et les opérateurs des systèmes de gestion de l'identité, et les méthodes d'application de ces critères;
- Les mécanismes d'évaluation ou de vérification des opérateurs des services liés à l'infrastructure de confiance commune et des opérateurs des systèmes de gestion de l'identité en ce qui concerne le respect des critères ci-dessus.

Dans un espace de confiance transfrontière, chaque système juridique est représenté par son régulateur national de l'infrastructure de confiance commune (voir fig. 3, régulateurs nationaux de l'infrastructure I, J, Q), qui réglemente les activités des opérateurs de services de confiance et des opérateurs de systèmes de gestion de l'identité dans son territoire de compétence.

Pour les groupements d'États à forte intégration (Communauté économique eurasienne ou Union européenne, par exemple), il est possible de créer un régulateur supranational de l'infrastructure de confiance commune (voir fig. 3, Régulateur supranational de l'infrastructure I-J). Ainsi, un seul régulateur supranational I-J remplace un groupe de régulateurs nationaux I et J.

La procédure d'admission de nouveaux membres au Conseil de coordination (nouveaux systèmes juridiques et participants supranationaux) et le système de vérification de la conformité des opérateurs de services de confiance et des opérateurs de systèmes de gestion de l'identité aux critères publiés par le Conseil (pour les nouveaux opérateurs de services de confiance) confèrent à l'infrastructure de confiance commune une évolutivité naturelle.

Si des membres du Conseil de coordination (voir ci-après) ont atteint un niveau de confiance théoriquement "moyen", ils peuvent lancer la création d'un régulateur international de l'infrastructure de confiance commune et d'opérateurs internationaux de services de confiance (voir fig. 3, Régulateur international de l'infrastructure I-J-Q et opérateurs internationaux de services de confiance I-J-Q). Le régulateur international de l'infrastructure de confiance commune coordonnera les interactions des opérateurs internationaux de services de confiance, des régulateurs nationaux de l'infrastructure (en vertu de la charte du Conseil) et/ou de ses régulateurs supranationaux.

Pour pouvoir devenir opérateur national de services de confiance ou opérateur d'un système de registre, tout prestataire des services respectifs devra être accrédité par le régulateur de l'infrastructure de confiance commune de son pays. Les opérateurs internationaux de services de confiance devront être accrédités par le régulateur international de l'infrastructure. Les conditions d'accréditation des opérateurs de services de confiance et des opérateurs de systèmes de registre, ainsi que les conditions régissant leurs activités, sont établies par les critères de conformité définis par le Conseil ainsi que par d'éventuels additifs nationaux émis par le régulateur approprié.

Les utilisateurs de services électroniques au sein de l'espace de confiance transfrontière peuvent être aussi bien des particuliers que des entités juridiques. Ils choisissent le niveau de qualification voulu du service de confiance, à leur discrétion ou par accord.

Les services sont fournis par les prestataires et opérateurs de services de confiance respectifs. Dans certains cas, ils peuvent également être fournis par les opérateurs de systèmes de registre. Les opérateurs de services de confiance et les opérateurs de systèmes de registre sont intégrés dans l'infrastructure de confiance commune.

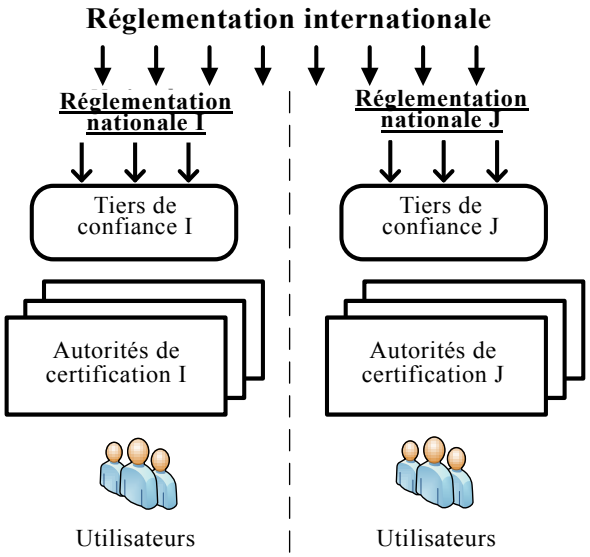
Les services de confiance, éléments de l'espace de confiance transfrontière, peuvent se présenter différemment, selon le niveau de confiance entre les participants aux échanges d'informations. Par exemple, si le niveau de confiance mutuelle entre les membres du Conseil est théoriquement "élevé" ou "moyen", il peut être efficace d'utiliser des services internationaux centralisés fournis conformément aux normes convenues. Si ce niveau est "faible", les services de confiance sont organisés selon le principe de la décentralisation, c'est-à-dire que l'on crée des services nationaux dans chaque État.

Aspects juridiques

L'espace de confiance transfrontière peut s'élaborer sur la base d'un domaine unique ou de domaines multiples. Du point de vue juridique et organisationnel, la

seconde option est la plus complexe, car elle nécessite l'intervention d'un tiers de confiance. La figure 4 présente un schéma général de réglementation juridique.

Figure 4
Réglementation juridique de l'espace de confiance transfrontière



La réglementation juridique des échanges d'informations transfrontières à valeur légale comprend deux volets: national et international. La réglementation juridique internationale se fonde sur les types de documents suivants:

- Traités/accords internationaux;
- Instruments de différentes organisations internationales;
- Normes et règlements internationaux;
- Accords entre parties à des échanges d'informations transfrontières sur des questions données;
- Lois types.

De même, la réglementation nationale se fonde sur un ensemble d'instruments prescriptifs spécifiques à chaque système juridique.

Résumé

Le texte présenté ci-dessus montre que la création d'un espace transfrontière de confiance est le meilleur moyen d'améliorer le système de gestion de l'identité, cela pour les raisons suivantes:

- La création de grappes de confiance nationales, régionales et internationales permettra d'assurer une plus grande interopérabilité de mécanismes de gestion de l'identité tels que les signatures électroniques;
- La reconnaissance juridique mutuelle des services de confiance fournis dans divers États permettra de définir une approche commune de la normalisation de ces systèmes;
- L'adoption de traités et d'accords internationaux ainsi que de normes et de règlements internationaux régissant l'utilisation de l'espace transfrontière de

confiance permettra d'accroître le niveau de confiance des participants dans le commerce électronique, ce qui simplifiera la mise en œuvre de la gestion de l'identité;

- Les activités du Conseil de coordination permettront d'élaborer des critères de conformité unifiés à satisfaire par les opérateurs de services de confiance, ainsi que la méthodologie d'application de ces critères.

L'amélioration du système de gestion de l'identité créera à son tour un environnement sûr pour les activités commerciales transfrontières. La mise en place d'un espace transfrontière de confiance nécessitera de prendre un certain nombre de mesures liées au système, à savoir:

- La mise en œuvre de solutions techniques propres à assurer la sécurité et la confidentialité des informations;
- La mise en œuvre de solutions organisationnelles par la mise en place d'un organe de coordination;
- La mise en œuvre de solutions juridiques et réglementaires par l'élaboration de traités internationaux relatifs à l'utilisation d'un espace transfrontière de confiance.

La mise en place d'un espace transfrontière de confiance obligera également à assurer, entre les organisations qui travaillent sur les questions de gestion de l'identité et de commerce transfrontière (ISO, UIT, CEFACT, CEE, CNUDCI et APEC, notamment), une coordination en vue d'élaborer une approche commune tant de la normalisation de l'utilisation d'un espace transfrontière de confiance en tant que mécanisme de gestion de l'identité que de l'utilisation d'un espace transfrontière de confiance pour les interactions électroniques et les activités commerciales transfrontières.

Pour encourager ce dispositif, la prochaine étape pourrait consister à examiner l'expérience et les connaissances accumulées avec différents partenaires (experts et organisations) désireux de faciliter et de simplifier les services électroniques transfrontières ainsi que de les doter d'une valeur légale.

Ces partenaires seront sans doute essentiellement des institutions politiques et économiques[6]. Les structures politiques qui interviennent déjà partiellement dans ce domaine de travail sont aussi bien des organisations supranationales (CEI, APEC, UE et Organisation de Shanghai pour la coopération, par exemple) que des États ayant des relations bilatérales. Les structures économiques qui s'intéressent à la réalisation de cet objectif peuvent être, par exemple, des organismes des Nations Unies tels que le CEFACT, la CNUDCI (Groupes de travail III et IV), la CEE, l'Espace économique européen et la Communauté économique eurasienne. On peut supposer que du fait des particularités naturelles (historiques, culturelles, politiques, économiques, techniques, etc.) des différentes régions du monde, diverses organisations internationales ou régionales créeront leurs propres organes de coordination (conseils de coordination des régulateurs de l'échange de données informatisé en confiance) et infrastructures de confiance communes en fonction du niveau de confiance qui existe au sein de chaque structure et des particularités naturelles mentionnées ci-dessus.

---

[6] Des structures humanitaires peuvent également s'intéresser à ce dispositif, par exemple, dans le domaine du droit, la Conférence de La Haye de droit international privé, ainsi que dans les domaines de la médecine et de l'éducation; nous sommes toutefois d'avis que de telles organisations seront plus susceptibles d'utiliser l'espace de confiance transfrontière déjà créé que d'appuyer une nouvelle création.

Nous supposons donc que durant les étapes initiales du projet, plutôt qu'un seul "domaine de confiance" pour toute la planète (au niveau d'un organisme des Nations Unies, par exemple), il coexistera, au niveau régional ou même au niveau des pays, plusieurs d'entre eux[7]. Quoi qu'il en soit, même la création de domaines de confiance distincts améliorera le système de gestion de l'identité, étant donné la nécessité d'assurer l'interopérabilité au sein de ces domaines.

Une fois l'architecture de l'infrastructure de confiance commune sélectionnée (au sein du domaine de confiance pertinent), on pourra commencer à élaborer une nouvelle série de documents organisationnels, normatifs et techniques convenue dans le cadre du Conseil de coordination. L'interopérabilité sera ainsi assurée dans le cadre de ce domaine de confiance.

L'adoption de cet ensemble de documents par les membres du Conseil de coordination (au sein du domaine de confiance pertinent) facilitera le passage à l'étape finale de mise en œuvre des systèmes d'interaction électronique transfrontière à valeur légale.

Remarques à l'attention des experts du Groupe de travail IV de la CNUDCI sur le commerce électronique

Le problème qui consiste à assurer la sécurité et l'identification des entités et objets dans le domaine du commerce électronique pourra être résolu grâce à la proposition énoncée ci-dessus (modèle de création et d'exploitation d'un espace de confiance transfrontière en tant que matrice fondée sur des grappes régionales et mondiales interconnectées incluant les services fonctionnels prévus dans le cadre dudit espace) de la manière suivante:

- Création d'une grappe fonctionnelle d'espaces de confiance transfrontières spécialisée dans la création d'une zone de confiance pour la gestion de l'identité en rapport avec les opérations internationales de commerce électronique;
- Tous les États Membres de l'Organisation des Nations Unies peuvent, indépendamment de leur situation géographique, être inclus dans cette grappe;
- Le fonctionnement de cette grappe est assuré par un opérateur spécialisé ou par un groupe d'opérateurs associés;
- Les activités commerciales des opérateurs spécialisés pourront inclure la prestation de services de confiance fondés sur un ensemble de régimes d'identification adoptés dans le cadre de plates-formes de commerce électronique;
- Le régime juridique applicable aux activités commerciales des opérateurs spécialisés sera déterminé par des accords conclus avec des plates-formes de commerce électronique.

[7] Espace informationnel et juridique utilisant la même infrastructure de confiance commune.