

# ANNEXE

## EXEMPLES DE DISPOSITIONS SUR L'IDENTITÉ NUMÉRIQUE QUI POURRAIENT ÊTRE INCLUSES DANS LES ACCORDS COMMERCIAUX<sup>1</sup>

### ARTICLE 1 : RECONNAISSANCE MUTUELLE DES IDENTITÉS NUMÉRIQUES DE CONFIANCE

1. Les Parties reconnaissent que les dispositifs d'identité numérique de confiance contribuent à améliorer la sécurité et la souplesse des chaînes d'approvisionnement et peuvent être un catalyseur pour faciliter les échanges.
2. Les Parties conviennent de mettre en place et de maintenir un cadre juridique propice à un système d'identité numérique de confiance. Ce cadre devrait être conforme aux principes de la CNUDCI et aux normes et principes pertinents déjà existants.
3. Les Parties conviennent de procédures mutuellement reconnues pour la délivrance et le contrôle des identités (entités légalement constituées sur le territoire des Parties), y compris :
  - (a) Accord sur le niveau et le type minimum d'informations (ou d'attributs) à contrôler et à valider pour délivrer des identités de confiance. Cet "identifiant numérique"<sup>2</sup> comportera un ou plusieurs attributs permettant de caractériser de manière unique une entité.
  - (b) Accord sur les informations électroniques ou les sources de données à utiliser pour prouver qu'une entité est une entité juridique sur le territoire spécifique des Parties.
  - (c) Toutes les Parties doivent veiller à ce que les mises à jour du statut juridique d'une entité soient maintenues en permanence et immédiatement communiquées. Dès qu'une entité juridique change de statut, cette nouvelle information devrait pouvoir être consultée en ligne par toutes les parties intéressées qui entendent interagir avec l'entité juridique.
  - (d) Chaque Partie a le droit d'autoriser un organisme (partie de confiance) à approuver l'établissement d'une entité juridique sur son territoire.
  - (e) Se mettre d'accord sur les institutions qui peuvent agir en tant que partie de confiance (les institutions financières, par exemple) confirmant la validité d'une preuve physique de constitution en société (et délivrant ensuite une identité numérique). Ces parties de confiance doivent être reconnues comme telles par toutes les Parties.
  - (f) Les nouvelles parties de confiance proposées devraient être approuvées par toutes les Parties à l'Accord.
  - (g) S'il n'existe pas encore de processus de numérisation, les autorités de confiance de chaque Partie s'efforceront de numériser le processus de constitution d'une entité juridique dès que possible.
4. Chaque Partie s'efforcera d'éviter d'imposer une charge réglementaire inutile.
5. Les Parties s'efforceront de recommander l'utilisation des normes existantes lorsque cela est possible et d'élaborer des normes communes lorsque cela est nécessaire.
6. Toutes les Parties devraient adopter ou maintenir des lois et réglementations sur la protection des informations personnelles communiquées. Le système d'identité numérique de confiance devrait être mis en œuvre de manière à permettre aux institutions concernées de protéger les données sensibles et de reconnaître les attentes de type

## ARTICLE 2 : GARANTIR LA FIABILITÉ DES DOCUMENTS COMMERCIAUX SIGNÉS NUMÉRIQUEMENT

culturel et éthique en matière de protection des données et de la vie privée. Il tiendra dûment compte des normes internationales relatives à la protection des données.

7. La reconnaissance mutuelle des systèmes d'identité numérique de confiance peut être temporairement interrompue ou totalement suspendue si les systèmes et processus gouvernementaux de délivrance d'identité sont compromis ou détruits/corrompus. Les Parties s'efforcent d'évaluer les solutions de rechange ou les autres mécanismes à disposition.
  8. Rien n'empêche une Partie d'adopter ou de maintenir des mesures incompatibles avec les points ci-dessus pour atteindre un objectif légitime de politique publique.
  9. L'authentification de l'identité d'une entité juridique n'est qu'une première étape vers le commerce sans papier. Une deuxième étape consisterait à utiliser le système pour l'autorisation et la communication de documents commerciaux tels que les licences et les certificats. Les Parties pourraient envisager d'inclure dans leur ACR, outre les dispositions énumérées ci-dessus, un libellé du type de celui qui suit.
1. Les Parties reconnaissent l'importance de veiller à ce que les documents commerciaux signés numériquement soient délivrés par un agent agréé, qu'ils n'aient pas été altérés et que seules les entités autorisées y aient accès.
  2. Les Parties conviennent mutuellement des autorités publiques ou des autres organismes qui sont autorisés à signer les documents commerciaux, à déclarer les transactions et à délivrer ces documents. Ces autorités publiques doivent être identifiées comme dignes de confiance par toutes les Parties.
  3. S'agissant des documents commerciaux, les Parties conviennent mutuellement d'accepter les signatures électroniques qui sont considérées comme ayant un effet juridique équivalent à celui d'une signature manuscrite selon la législation d'une Partie, à moins qu'une Partie ne puisse démontrer un doute raisonnable concernant la fiabilité de la signature électronique.
  4. Un agent du pays importateur peut vérifier que l'agent exportateur qui a signé numériquement le document commercial est un émetteur autorisé d'un document spécifique sur le territoire du pays exportateur.

## ARTICLE 3: COOPÉRATION

1. Les Parties s'efforceront de maintenir le dialogue sur les questions réglementaires soulevées par les dispositifs d'identité numérique de confiance. En particulier, elles s'efforceront :
  - (a) d'échanger des informations et des bonnes pratiques concernant :
    - (i) le fonctionnement et la gestion des dispositifs d'identité numérique de confiance;
    - (ii) les politiques, les réglementations, l'exécution et la conformité en ce qui concerne la sécurisation des systèmes informatiques;
  - (b) de coopérer pour remédier aux obstacles législatifs, réglementaires et techniques dès que possible sur le plan pratique.
2. Les Parties collaboreront en vue d'aider les PME à participer pleinement à ces dispositifs.
3. Les Parties affirment l'importance de participer activement aux instances pertinentes, y compris les instances multilatérales, afin de promouvoir le développement de dispositifs d'identité numérique de confiance et la délivrance de documents commerciaux signés numériquement fiables.

Il convient également d'envisager d'inclure des dispositions similaires dans d'autres accords commerciaux, à commencer par le nouvel ensemble de règles en cours d'élaboration dans le cadre de l'initiative conjointe de l'OMC sur le commerce électronique.

## NOTES DE FIN

1. Sur la base de <https://www.unescap.org/sites/default/files/86%20Final-Team%20Hanna%20Norberg-Sweden.pdf>.
2. Un identifiant numérique comprend un ou plusieurs attributs qui caractérisent de manière unique une entité dans un contexte donné. Il sert de clé aux parties pour s'accorder sur l'entité représentée (ISO/CEI 29115:2013).