Nations Unies ECE/TRADE/C/CEFACT/2014/6

Conseil économique et social

Distr. générale
23 janvier 2014
Français
Original: anglais

Commission économique pour l'Europe

Comité du commerce

Centre pour la facilitation du commerce et les transactions électroniques

Vingtième session
Genève, 10 et 11 avril 2014
Point 5 de l'ordre du jour provisoire
Recommandations et normes du CEFACT-ONU

Révision de la Recommandation n° 14: Authentification des documents commerciaux[1]

Document présenté par le Domaine des procédures du commerce international (ITPD), Secteur de l'élaboration des programmes relatifs au commerce et au transport, pour approbation

Résumé

À sa neuvième session, en mars 1979, le Groupe de travail de la facilitation des procédures du commerce international (WP.4), prédécesseur du CEFACT-ONU, a adopté la Recommandation n° 14 intitulée «Authentification des documents commerciaux par des moyens autres que la signature» (documents TRADE/WP.4/INF.63, TD/B/FAL/INF.63).

Cette recommandation a pour but d'encourager l'utilisation des moyens électroniques de transmission des données dans le cadre du commerce international en recommandant que les gouvernements examinent les dispositions nationales et internationales exigeant que les documents établis dans le contexte du commerce international soient signés, afin de supprimer l'obligation d'établir des documents sur papier et de remplacer la signature manuelle obligatoire par des méthodes d'authentification applicables dans le cadre d'une transmission électronique.

[1] Étant donné l'évolution technologique et l'emploi d'un vocabulaire nouveau depuis la publication de la version originale (1979) de cette recommandation, l'ITPD propose que le titre original, à savoir «Authentification des documents commerciaux par des moyens autres que la signature», soit modifié en «Authentification des documents commerciaux».

GE.14-20346 (F) 180314 190314
1420346

En outre, la Recommandation n° 14 vise à encourager les milieux d'affaires et les fournisseurs de services commerciaux à examiner les processus commerciaux afin de recenser les cas dans lesquels les signatures (de tout type) peuvent être éliminées et, lorsque cela n'est pas possible, à s'efforcer de transmettre les données commerciales par voie électronique et d'adopter des méthodes d'authentification autres que la signature manuelle.

Le présent document renferme la deuxième édition de la Recommandation n° 14, établie par le Domaine des procédures du commerce international (ITPD) du CEFACT-ONU. La présente révision, approuvée par le Bureau du CEFACT-ONU, annule et remplace la première édition (TRADE/WP.4/INF.63).

Elle est soumise pour examen et approbation à la vingtième session plénière du CEFACT-ONU.

Table des matières

I. Introduction

1. L'échange d'informations précises, complètes et récentes joue un rôle fondamental dans la conduite efficace des opérations commerciales nationales et internationales. Jusqu'à présent, cet échange se faisait au moyen de documents sur papier. De plus en plus, les équivalents du papier, y compris les services en ligne, ont permis aux partenaires commerciaux, aux fournisseurs de services commerciaux, aux pouvoirs publics et aux autres organismes de réglementation d'échanger des données plus rapidement et plus efficacement.

2. Le Centre des Nations Unies pour la facilitation du commerce et les transactions électroniques (CEFACT-ONU) a constamment pour objectif de réduire le nombre de documents utilisés dans la chaîne d'approvisionnement entre les partenaires commerciaux tant nationaux qu'internationaux. Lorsqu'une obligation légale, une prescription réglementaire ou une nécessité commerciale empêche de supprimer un document, l'objectif du CEFACT-ONU est que ce document n'ait pas besoin de comporter une signature pour signifier l'intention de la partie dont il émane ou pour que la partie qui le reçoit donne suite aux informations qu'il contient.

3. Le CEFACT-ONU reconnaît qu'il est probablement impossible de parvenir à supprimer tout les documents commerciaux utilisés dans la chaîne d'approvisionnement. Certains de ces documents continueront, pour des raisons juridiques, de nécessiter une signature. Cette obligation est liée à l'utilisation des documents sur papier. Le recours de plus en plus fréquent à des moyens électroniques ou à d'autres moyens automatiques de transmission des données rend souhaitable la mise au point d'autres méthodes d'authentification, dont certaines pourront éliminer complètement l'obligation de comporter une signature ou constituer l'équivalent électronique d'une signature manuelle. Depuis la publication de la première version de la présente Recommandation, en 1979, un certain nombre de méthodes d'authentification autres que la signature ont fait leur apparition et d'autres méthodes de substitution verront probablement le jour dans les prochaines années.

Première partie
Recommandation n° 14 relative à l'authentification des documents commerciaux

I. Portée

4. La présente recommandation a pour but d'encourager l'utilisation des moyens électroniques de transmission des données dans le cadre du commerce international en recommandant que les gouvernements examinent les dispositions nationales et internationales exigeant que les documents établis dans le contexte du commerce international soient signés, afin de supprimer l'obligation d'établir des documents sur papier et de remplacer la signature manuelle obligatoire par des méthodes d'authentification applicables dans le cadre d'une transmission électronique[2].

[2] Pour le passage des documents sur papier aux équivalents électroniques dans les diverses fonctions d'une transaction commerciale internationale, voir Lauri Railas, «The Rise of the Lex Electronica and the International Sale of Goods, Facilitating Electronic Transactions Involving Documentary Credit Operations», Forum Iuris, Université d'Helsinki, 2004, en particulier le chapitre VIII.

5. En outre, cette recommandation vise à encourager les milieux d'affaires et les fournisseurs de services commerciaux à examiner les processus commerciaux afin de recenser les cas dans lesquels les signatures (de tout type) peuvent être éliminées et, lorsque cela n'est pas possible, à s'efforcer de transmettre les données commerciales par voie électronique et d'adopter des méthodes d'authentification autres que la signature manuelle.

II. Utilisation de normes internationales

6. L'utilisation de normes internationales peut contribuer de façon décisive à faire accepter plus largement les solutions choisies et, finalement, à permettre l'interopérabilité. Dans la mesure du possible, les acteurs publics et privés qui ont l'intention d'échanger des données par voie électronique au moyen d'une méthode d'authentification doivent essayer d'utiliser les normes internationales existantes.

7. Le présent document fait partie d'un ensemble de recommandations relatives à la normalisation et à la facilitation des échanges commerciaux (voir l'annexe A.3). L'échange de données électroniques présente de nombreux aspects, dont beaucoup font l'objet de plusieurs recommandations actuelles et futures de la Commission économique des Nations Unies pour l'Europe (CEE).

8. Les travaux de codification juridique entrepris par la Commission pour le droit commercial international (CNUDCI) dans le domaine du commerce électronique et de la signature électronique doivent être pris en considération et exploités chaque fois que possible comme base de la mise en place de l'infrastructure juridique de l'authentification électronique, aussi bien pour les transactions nationales que pour les transactions internationales.

III. Recommandation

9. Le CEFACT-ONU recommande que les pouvoirs publics et les participants au commerce international et au mouvement des marchandises:

- Envisagent activement de supprimer l'obligation de signer les documents commerciaux (manuellement ou par un moyen électronique équivalent), sauf lorsque la fonction du document ou l'activité l'exigent, et s'abstiennent d'inscrire cette obligation dans les nouvelles règles et pratiques.

10. En outre, le CEFACT-ONU, reconnaissant l'importance des méthodes d'authentification dans l'échange électronique de documents commerciaux, recommande que les pouvoirs publics et les participants au commerce international et au mouvement des marchandises:

- Envisagent d'adopter des méthodes électroniques pour authentifier les documents commerciaux;
- Créent un cadre juridique ou contractuel autorisant ces méthodes d'authentification et leur accordant un statut égal.

11. Pour atteindre cet objectif, le CEFACT-ONU recommande:

- Qu'un groupe de travail conjoint des secteurs public et privé (ou des groupes de travail sectoriels) examine(nt) régulièrement la documentation utilisée pour les échanges commerciaux nationaux et internationaux. L'objectif de ce(s) groupe(s) de travail serait d'éliminer l'obligation de comporter une signature manuelle et, lorsque cela n'est pas possible, de remplacer la signature manuelle par d'autres méthodes d'authentification.

Deuxième partie
Lignes directrices concernant la mise en œuvre de la Recommandation n° 14

I. Introduction

12. Les présentes lignes directrices concernant la mise en œuvre de la Recommandation n° 14 du CEFACT-ONU relative à l'authentification des documents commerciaux sont destinées à aider les pouvoirs publics et les milieux d'affaires à définir la fonction et l'utilisation de la signature. Elles donnent un aperçu des principales questions à examiner, de certains des outils disponibles et des mesures à prendre pour mettre en place des méthodes électroniques d'authentification.

13. La présente recommandation s'accompagnera de deux annexes destinées à aider les pouvoirs publics et les milieux d'affaires à bien comprendre comment des méthodes électroniques d'authentification ont été mises en place ou sont actuellement appliquées.

II. Signature

A. Définition d'une signature

14. Dans le vocabulaire d'aujourd'hui, le mot «signature» désigne à la fois une signature manuelle et son équivalent électronique[3].

15. Au sens le plus large, une signature (manuelle ou son équivalent électronique) crée un lien entre une personne (physique ou morale) et un contenu (document, transaction, procédure ou autre). Ce lien peut être considéré comme ayant trois fonctions intrinsèques: une fonction d'identification, une fonction de preuve et une fonction d'attribution[4].

16. La confiance est l'un des fondements essentiels des relations commerciales internationales; il est très probable que dans de nombreux cas, le fait d'exiger une signature participe de cette confiance.

B. Fonctions d'une signature

- La fonction d'identification d'une signature consiste à permettre d'établir l'identité du signataire ou à confirmer cette identité; l'identification peut recouvrir: l'identité déclarée/affirmée de la personne, la véracité de la déclaration d'identité, l'attestation de tout organisme de vérification, la preuve de l'origine, l'heure et la date, ainsi que tout autre aspect permettant d'identifier les personnes concernées ou le contenu;

[3] La version originale de 1979 de la présente recommandation ne fait pas de distinction dans son titre parce qu'à cette époque, une signature était toujours considérée comme manuelle. Par conséquent, ce terme doit être précisé dans le titre actuel de la Recommandation et dans l'ensemble du présent document.

[4] Ces réflexions sur les fonctions sont développées au paragraphe 7, p. 5, du document de la CNUDCI intitulé «Promouvoir la confiance dans le commerce électronique: questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques», Nations Unies, Vienne, 2009. Document disponible à partir de mars 2013 à l'adresse suivante: http://www.uncitral.org/pdf/french/texts/electcom/08-55699_Ebook.pdf. Voir aussi «Review of Definitions of "«Writing", "Signature» and «Document" employed in multinational conventions and agreements relating to international trade», document présenté par le Groupe de travail juridique (révision du document Trade/WP.4/R.1096 daté du 22 juillet 1994), Genève, octobre 2001, ECE/TRADE/240.

- La fonction de preuve d'une signature aura des conséquences juridiques et pourra se rapporter aux éléments suivants: intégrité, consentement, reconnaissance et détection de toute modification apportée au document après sa signature. Elle peut consister à témoigner du niveau d'engagement que l'action de signer pourrait avoir indiqué;
- La fonction d'attribution d'une signature est le lien entre le signataire et le document qui est signé. Cela peut inclure le pouvoir accordé dans le cadre des fonctions du signataire (c'est-à-dire à l'intérieur d'une entreprise, d'un organisme public, du secteur marchand…).

17. Ces trois fonctions peuvent être considérées comme se situant à des niveaux variables. Il peut y avoir plus ou moins de chacune de ces fonctions dans toute signature.

C. Méthodes d'authentification

18. Une signature ou son équivalent fonctionnel est une méthode courante d'authentification des documents commerciaux. Dans les présentes lignes directrices, les termes «signer» et «authentifier» ont la même acception.

19. L'usage qui consiste à apposer une signature manuelle ou l'obligation d'apposer une telle signature posent d'importants problèmes de transmission des données par les moyens technologiques modernes dans les cas où ces données sont transmises au pays de destination (finale) et où la signature manuelle doit pouvoir être présentée au moment du dédouanement des marchandises. La législation nationale et les conventions internationales devront être modifiées chaque fois qu'elles imposent une signature manuelle comme garantie de l'authenticité des informations transmises de cette manière.

20. Les termes présentés ici au chapitre II (signature, fonction de la signature et authentification) sont à considérer avec prudence. Ils sont souvent compris différemment selon l'environnement (juridique ou technique). Il peut y avoir d'autres différences selon la région du monde où ils sont employés[5].

III. Obligation de signer les documents commerciaux

21. En général, il y a diverses utilisations de la signature dans la documentation commerciale. Pour examiner une transaction selon que la procédure suivie est celle de la signature manuelle ou de son équivalent électronique, il est nécessaire d'examiner le contexte de la transaction elle-même.

A. Examen du contexte juridique de la transaction

22. Généralement, pour les transactions d'entreprise à entreprise, les prescriptions légales peuvent s'inscrire dans le cadre du droit commercial. Ces prescriptions ou les pratiques commerciales peuvent être précisées ou définies par les organisations

[5] En général, dans le domaine des technologies de l'information, signature et authentification ont souvent des fonctions intrinsèques qui peuvent avoir trait à l'intégrité, l'authenticité, la preuve, la sécurité, etc. Là encore, tous ces termes peuvent être interprétés différemment selon l'environnement et la géographie. La présente recommandation a été élaborée en conformité avec les travaux de la CNUDCI et compte tenu de l'emploi de ces termes dans d'autres recommandations de la CEE. Lors de la lecture ou de la rédaction de tout texte sur le sujet, il est recommandé d'indiquer clairement quelle est l'interprétation donnée. Il est recommandé aux législateurs, qui utiliseront probablement une définition juridique, de se référer aux documents de la CNUDCI sur le sujet afin de préciser clairement l'utilisation juridique de ces termes.

commerciales pour leurs membres. Enfin, de nombreuses prescriptions relatives aux transactions entre deux partenaires commerciaux indépendants seront définies explicitement dans des accords bilatéraux ou multilatéraux.

23. Pour les transactions avec des organismes publics ou entre organismes publics, les prescriptions légales sont définies presque exclusivement dans le cadre du droit public.

24. Il peut y avoir plusieurs niveaux de droit public et de droit privé à prendre en considération: les niveaux fédéral, national, ministériel, institutionnel, régional, international, etc. Il peut aussi être nécessaire de tenir compte de plusieurs types de règlements publics: règlements commerciaux, relatifs au transport, sanitaires, douaniers, etc.

25. En outre, un même document peut être utilisé par plusieurs organismes d'un même gouvernement, voire de différents gouvernements. Cela peut se produire par exemple dans le cadre de mécanismes de guichet unique ou d'une gestion coordonnée des frontières. Dans ces cas, les prescriptions relatives à l'authentification devront être harmonisées de façon à ne pas remettre en doute la validité des données qui sont communiquées.

26. La législation ne doit pas imposer des prescriptions rigoureuses qui remettraient en doute la validité et la force exécutoire de transactions autrement légitimes.

B. Documents commerciaux

27. Le choix d'une méthode d'authentification peut aller à l'encontre de plusieurs intérêts, dont les intérêts commerciaux, relatifs au transport, financiers et officiels. Les documents qui traversent une frontière peuvent poser des problèmes du fait qu'ils doivent être utilisés dans deux pays ou régions différents. Il est à noter en outre que les informations qui figurent dans certains documents peuvent intéresser d'autres parties que l'expéditeur et le destinataire de ces documents.

28. Les documents commerciaux peuvent être des factures, des certificats de qualité ou de quantité, des avis d'expédition, des notifications ou des notes de crédit. Un principe fondamental du droit commercial international est qu'il n'existe pas d'obligation formelle en matière de signature. À moins que la législation nationale ne l'exige à titre exceptionnel, les documents requis pour l'exécution pratique d'un contrat n'ont pas besoin d'être signés.

29. Les documents de transport font souvent intervenir un certain nombre de parties autres que le transporteur lui-même: exportateurs, importateurs, bailleurs de fonds, assureurs et autorités. Ces documents sont entre autres l'ordre d'expédition de marchandises à l'exportation, la lettre de transport maritime ou aérien, le connaissement ou le certificat d'expédition. Nombre de ces documents sont visés par des conventions internationales qui imposent des obligations et des conditions juridiquement contraignantes souvent transposées dans les lois et les règlements nationaux. Certaines de ces conventions imposent encore de présenter un document signé pour effectuer certaines opérations liées au transport, au transit ou à la chaîne logistique. Cependant, beaucoup plus nombreuses sont les conventions qui ont adopté une approche plus moderne et plus simple en supprimant cette obligation et en la remplaçant par l'emploi d'un équivalent électronique ou d'une autre méthode d'authentification[6]. En conséquence, la signature est de moins en moins exigée dans les chaînes de transport nationales et internationales.

[6] La CNUDCI mène actuellement des travaux sur ce sujet. Voir, entre autres références, le rapport du Groupe de travail IV sur les travaux de sa quarante-septième session, à l'adresse suivante: http://www.uncitral.org/uncitral/fr/commission/working_groups/4Electronic_Commerce.html (au 1er juillet 2013) et le projet de dispositions types dans le document A/CN.9/WG.IV/WP.122.

30. Les documents financiers peuvent être une police ou un certificat d'assurance, un ordre de virement bancaire, des documents bancaires concernant le crédit ou le recouvrement ou des lettres de change. Les mêmes considérations que celles qui s'appliquent aux documents de transport peuvent être faites à leur sujet. Un grand nombre de ces documents ont déjà été remplacés par des processus automatisés mis en place entre les institutions financières. Certains documents financiers, en particulier les lettres de change, sont des instruments négociables pour lesquels il existe des prescriptions bien établies en ce qui concerne la forme et la signature. Cependant, cela n'empêche pas de prendre des mesures pour supprimer ces prescriptions et les remplacer par des méthodes d'authentification plus modernes et plus simples.

31. Les documents officiels comprennent les déclarations en douane, les déclarations et certificats d'importation, les certificats agricoles, les certificats de la CITES (Convention sur le commerce international des espèces de faune et de flore sauvages menacées d'extinction) et les autres documents requis pour établir l'admissibilité et la responsabilité. L'acceptation et l'engagement de la responsabilité quant au respect des obligations officielles et réglementaires ont souvent lieu au moment de l'importation dans le pays de destination finale. Cependant, le respect de ces obligations est souvent directement lié aux mesures prises dans le pays d'exportation avant ou au moment de l'expédition, ou ultérieurement.

C. Détermination des besoins d'authentification dans le contexte d'une transaction

32. Pour les transactions avec des organismes publics, il est recommandé de créer un groupe de travail conjoint des secteurs public et privé (ou des groupes de travail sectoriels) afin d'examiner régulièrement la documentation utilisée pour les échanges commerciaux nationaux et internationaux. L'objectif de ce(s) groupe(s) de travail serait d'éliminer la signature manuelle chaque fois que possible et soit d'éliminer sa nécessité complètement, s'il est sûr et raisonnable de le faire dans le contexte de la transaction, soit de la remplacer par d'autres méthodes d'authentification. Une liste de considérations est proposée dans l'annexe B.1.

33. Pour les transactions d'entreprise à entreprise, les deux parties peuvent de la même façon étudier les besoins d'authentification dans le contexte de chaque transaction ou faire référence à un accord transversal. La liste de considérations proposée dans l'annexe B.1 devrait aussi donner des indications dans ce contexte.

IV. Utilisation de méthodes électroniques d'authentification

34. Le choix d'autres méthodes d'authentification dépendra du processus commercial et d'une évaluation des risques inhérents aux nécessités de ce processus. Une liste de considérations relatives au choix d'une méthode électronique d'authentification est proposée dans l'annexe B.1.

A. Neutralité de la technologie

35. Dans la mesure du possible, la législation doit rester technologiquement neutre; elle ne doit établir aucune discrimination entre les formes de technologie. Les informations techniques, lorsqu'elles sont fournies, doivent être fondées sur des prescriptions minimales et s'accompagner éventuellement d'exemples, tout en laissant la possibilité de satisfaire à ces prescriptions au moyen d'autres solutions fonctionnellement équivalentes.

B. Niveaux de fiabilité

36. Comme on l'a vu plus haut, selon la relation entre les parties et en fonction du contexte juridique, certains processus peuvent exiger une sécurité plus ou moins grande. Toutes les transactions ne requièrent pas le niveau de sécurité le plus élevé. De même, les techniques varient et peuvent assurer une sécurité plus ou moins grande selon les besoins.

37. La fiabilité de la méthode d'authentification choisie doit être «suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière»[7].

38. Des efforts doivent être faits pour éviter de créer des solutions électroniques qui soient plus difficiles d'emploi ou plus coûteuses que le processus manuel. La technologie peut générer des applications dont le niveau de fiabilité est très élevé. Le choix d'une application doit être fonction du niveau de fiabilité requis par le processus et des contraintes juridiques existantes.

C. Typologie des méthodes électroniques d'authentification

39. Il existe un certain nombre de méthodes qui peuvent remplacer une signature manuelle. La technologie évolue en permanence. L'activité illicite ou frauduleuse évolue aussi constamment, trouvant des moyens de réduire le niveau de fiabilité de certains éléments d'une méthode donnée. Pour cette raison, les normes et applications techniques sont examinées de façon plus approfondie dans l'annexe B.2 de la présente recommandation, afin d'en faciliter la mise à jour en fonction des meilleures pratiques et des normes actuelles.

40. Selon les risques, les besoins de sécurité et d'autres considérations, une méthode d'authentification utilisée seule («authentification unifactorielle») peut suffire. Cependant, dans des situations de risque élevé, une combinaison appropriée de méthodes d'authentification et d'autres techniques peut s'avérer nécessaire («authentification multifactorielle»). Par exemple, un processus d'enregistrement et de vérification peut être fondé sur une identification par un nom d'utilisateur et un mot de passe, à laquelle vient s'ajouter un réseau privé virtuel ou une autre méthode électronique.

D. Signature électronique

41. Toutes ces méthodes peuvent, presque sans exception, être qualifiées de signature électronique. Une signature électronique peut être définie comme «des données sous forme électronique contenues dans un message de données ou jointes ou logiquement associées audit message, pouvant être utilisées pour identifier le signataire dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue»[8].

[7] Art. 7.1, «Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation 1996 avec le nouvel article 5 *bis* tel qu'adopté en 1998», Nations Unies, New York, 1999, p. 5 et 6. Document disponible à partir de mars 2013 à l'adresse suivante: http://www.uncitral.org/uncitral/fr/uncitral_texts/electronic_commerce/1996Model.html.

[8] Voir l'article 2a de la «Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation 2001», Nations Unies, New York, 2002, p. 6. Document disponible à partir de mars 2013 à l'adresse suivante: http://www.uncitral.org/uncitral/fr/uncitral_texts/electronic_commerce/ 2001Model_signatures.html. Il convient de noter que la définition originale qui figure dans ce document de 2002 mentionne l'«approbation» du signataire. Les travaux ultérieurs de la CNUDCI ont conduit à parler plutôt de l'«intention» du signataire.

42. Il est à noter qu'une signature électronique au sens large n'appelle pas en soi une forme spécifique de technologie. Une signature électronique remplira les mêmes fonctions qu'une signature manuelle, là encore à un degré variable selon la fonction (à savoir l'identification, la preuve ou l'attribution).

43. Une signature électronique ne doit pas faire l'objet d'une discrimination à cause de son origine, ni du simple fait qu'il s'agit d'une méthode électronique d'authentification. Cependant, elle peut faire l'objet d'une discrimination à cause de ses qualités intrinsèques. Les gouvernements et les organismes de réglementation de divers pays doivent s'efforcer de mettre en œuvre des arrangements comme des mémorandums d'accord, des accords, etc. afin d'assurer une reconnaissance juridique des signatures électroniques d'origine étrangère et l'interopérabilité des signatures électroniques.

44. Une distinction doit être faite entre l'expression «signature électronique» telle qu'elle est employée dans les présentes lignes directrices et les textes pertinents de la CNUDCI sur le commerce électronique et l'expression «signature numérique», examinée dans l'annexe B de la présente recommandation. Par souci de clarté, il faut souligner que ces deux termes ne sont pas interchangeables. Le terme générique, qui ne fait référence à aucun choix technologique et est employé dans les textes de la CNUDCI sur le commerce électronique, est «signature électronique». Le terme «signature numérique», tel qu'il est examiné dans les documents de la CNUDCI, implique qu'un choix technologique a été fait (en faveur de solutions s'accompagnant d'un chiffrement asymétrique, dont l'«infrastructure à clef publique» (ICP) est le principal exemple)[9]. Les organismes de régulation et les rédacteurs de contrats ou de documents techniques devraient garder cette distinction présente à l'esprit et n'employer le terme «signature électronique» que s'ils ont l'intention de faire savoir qu'un tel choix technologique a été fait.

V. Aspects des méthodes électroniques d'authentification à prendre en considération

45. Selon la méthode d'authentification choisie, les aspects ci-après doivent être pris en considération.

A. Recours aux services d'une tierce partie

46. Les parties peuvent préférer ou avoir besoin de faire appel à un tiers pour se charger d'un aspect de la méthode d'authentification relatif à la transmission, l'archivage, la récupération, la vérification, etc. Dans certains cas, les services d'une tierce partie sont mandatés ou validés par un organisme public (qui émet par exemple les clefs de codage). Dans certains cas également, les partenaires commerciaux peuvent choisir de recourir aux services d'une tierce partie pour la mise en place de solutions prêtes à l'emploi, la compilation et la transmission des données, le renforcement de la sécurité, l'archivage ou la récupération, etc.

47. En règle générale, l'autorisation de recourir aux services d'une tierce partie doit être accordée par l'un ou l'autre des partenaires commerciaux. Dans ce cas, ces services sont considérés comme ceux d'une partie concernée/autorisée. Toute limitation de cette

[9] Voir par exemple le paragraphe 21, p. 15, du document de la CNUDCI intitulé «Promouvoir la confiance dans le commerce électronique: questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques», Nations Unies, Vienne, 2009. Document disponible à partir de mars 2013 à l'adresse suivante: http://www.uncitral.org/pdf/french/texts/electcom/08-55699_Ebook.pdf.

autorisation ou de la possibilité de recourir aux services d'une tierce partie doit être clairement indiquée dans le texte juridique approprié, l'accord bilatéral entre les partenaires commerciaux ou l'accord avec la tierce partie.

48. Lorsque les services d'une tierce partie sont mandatés ou validés par un organisme public, les critères d'attribution d'un tel mandat doivent être transparents et le processus ouvert à tous.

B. Sécurité des données

49. L'accès des parties concernées (parties autorisées) aux données ne doit pas être limité, ce qui peut être déterminé dans une certaine mesure par les responsabilités juridiques des parties.

50. Les prescriptions relatives à la sécurité des données correspondront au niveau de fiabilité exigé par la transaction, qui devra avoir été fixé par une évaluation du risque compte tenu du processus, des contraintes opérationnelles, des contraintes juridiques et du rapport de confiance entre les parties. Si une tierce partie autorisée intervient dans le processus, elle devra assurer un même niveau de fiabilité. Selon le niveau de fiabilité fixé, les intérêts des parties devront être protégés en cas de litige.

51. Selon le niveau de fiabilité, la sécurité des données peut impliquer leur protection et le fait de veiller à ce qu'elles ne soient pas supprimées ni détruites.

C. Transmission des données

52. Les aspects de la transmission effective des données dépendront de la méthode électronique choisie. Ils sont présentés dans l'annexe B de la présente recommandation.

53. Pour les échanges privés d'entreprise à entreprise, les deux parties doivent convenir explicitement d'une méthode de communication et d'une méthode d'authentification. Elles doivent envisager le niveau de fiabilité requis lors de l'établissement de cet accord. Cela pourrait par exemple faire partie d'un accord d'échange entre les deux parties, selon le modèle qui figure dans la Recommandation n° 26 du CEFACT-ONU, ou encore d'un accord transversal établi par un expert.

54. Selon le niveau de fiabilité, une piste d'audit pourra être nécessaire. Dans certains cas, il pourra être utile ou juridiquement nécessaire d'obtenir une confirmation de la transmission ou de la réception, de déterminer l'ordre des messages, l'horodatage, les diverses en-têtes, etc. Ces obligations pourront figurer dans certains accords entre les partenaires commerciaux ou résulter d'un contexte juridique particulier[10].

D. Archivage/récupération

55. Dans la plupart des cas, les documents commerciaux devront être archivés soit pour un usage ultérieur dans le cadre d'autres processus, pour garder une trace des opérations, etc., soit pour répondre à des obligations légales ou réglementaires (par exemple l'obligation légale d'archiver les factures électroniques ou les déclarations en douane). Lorsqu'une partie envisage d'archiver des documents commerciaux, elle doit envisager la période et le lieu d'archivage, ainsi que la question du contrôle de l'accès.

[10] À cet égard, référence peut être faite à l'article 15 de la Loi type de la CNUDCI sur le commerce électronique et à l'article 10 de la Convention sur l'utilisation de communications électroniques, qui fixe des règles relatives au moment et au lieu de l'expédition et de la réception des messages de données.

La méthode d'authentification employée pour l'archivage des documents peut être très différente selon qu'il s'agit d'un archivage à long terme ou à court terme. Les documents archivés pour de longues périodes peuvent demander une attention spéciale, étant donné que les méthodes d'authentification existantes perdent souvent de l'efficacité au fil du temps, voire deviennent obsolètes, du fait de l'évolution technologique. Les gouvernements ou les signataires d'accords bilatéraux peuvent vouloir prévoir le passage d'une technologie à une autre pendant l'archivage.

56. Selon les impératifs de la transaction, il peut être attendu des méthodes d'archivage qu'elles correspondent au moins à un niveau de fiabilité équivalent à celui de la méthode d'authentification ou de signature utilisée. La méthode d'archivage doit être vérifiable; autrement dit, il doit être possible de vérifier sa fiabilité afin de constater s'il elle fonctionne ou non, de vérifier l'exactitude et la lisibilité des données récupérées (format utilisé) et de vérifier que la portée de la méthode s'étend aux aspects fonctionnels de l'authentification acceptée par les parties et les autorités.

57. Les partenaires commerciaux pourront souhaiter recourir aux services d'une tierce partie pour les aider à archiver et récupérer les données, ce qui pourra dépendre de nombreux facteurs, y compris les capacités techniques et les coûts. Dans ce cas, les services en question devront être fournis compte tenu des points mentionnés plus haut. La tierce partie pourra en outre avoir la possibilité de délivrer un certificat prouvant juridiquement qu'une partie autorisée aura récupéré les données et indiquant la date à laquelle ces données auront été récupérées, si de telles dispositions sont requises par le niveau de fiabilité[11].

VI. Processus d'examen de la recommandation

58. La présente recommandation se compose du texte même de la recommandation, de lignes directrices et d'annexes (qui comprennent des référentiels). Il est proposé de mettre à jour les annexes et les référentiels tous les trois à cinq ans, ce qui supposera de contacter chaque coauteur initial pour vérifier que les informations sont toujours pertinentes/actuelles (faute de réponse, la communication sera éliminée de l'annexe). Une fois reçue la réponse du coauteur, les informations figurant dans l'annexe seront confirmées, révisées ou éliminées selon le cas. Ce sera également l'occasion de demander de nouvelles communications à intégrer dans les annexes et de compléter celles-ci par d'autres apports.

59. Il est proposé qu'une fois mis à jour l'ensemble des annexes et des référentiels, le contenu de la recommandation et de ses lignes directrices soit vérifié par rapport aux annexes révisées. S'il n'y a pas de modifications ou si celles-ci sont minimes, il sera peut-être préférable de ne pas mettre à jour la recommandation afin d'essayer de garder une version stable. Si des éléments des annexes ou des référentiels contredisent le texte de la recommandation ou rendent celui-ci obsolète/erroné, la recommandation devra être modifiée.

60. En outre, si des gouvernements ou des représentants du secteur commercial soulèvent des problèmes de fond quant à la pertinence du texte de la recommandation, ces problèmes seront examinés et le texte pourra être révisé même en dehors des périodes de mise à jour.

[11] Dans ce contexte, référence peut être faite à l'article 10 de la Loi type de la CNUDCI sur le commerce électronique, qui énonce une règle relative à la conservation des messages de données.

VII. Options autres que la signature manuelle

61. Le présent chapitre a pour objet d'apporter des précisions supplémentaires aux trois principales recommandations du présent document.

A. Supprimer les signatures manuelles et leur équivalent électronique lorsque cela est possible

62. Il est recommandé aux gouvernements et à toutes les organisations concernées par la facilitation des procédures du commerce international d'examiner les documents commerciaux en usage courant, de recenser ceux dans lesquels les signatures manuelles et leur équivalent électronique pourraient être éliminés sans inconvénient et de mettre sur pied un vaste programme d'enseignement et de formation en vue d'introduire les changements nécessaires dans les pratiques commerciales.

63. Cette suppression de l'obligation de signer les documents devra être étudiée au cas par cas pour chaque document commercial. Lorsque la signature n'est pas un élément essentiel de la fonction du document ou de la transaction, il est recommandé de supprimer cette obligation.

64. Il est recommandé en outre, lors de la création de nouveaux environnements ou documents commerciaux, de s'abstenir naturellement d'imposer l'usage de la signature dans les nouveaux règlements, nouvelles règles, nouveaux contrats ou nouvelles pratiques.

B. Faciliter le remplacement de la signature manuelle par des méthodes électroniques

65. Il est recommandé aux gouvernements et aux organisations internationales s'occupant des accords intergouvernementaux pertinents d'étudier les textes nationaux et internationaux qui comportent des dispositions exigeant que les documents à utiliser dans le commerce international soient signés et d'envisager le cas échéant de modifier ces dispositions afin de permettre la préparation et la transmission par voie électronique des renseignements figurant dans ces documents.

66. Il n'est pas possible, étant donné leur nombre très élevé, de modifier les dispositions pertinentes de chaque texte juridique dans lequel une signature est mentionnée. Pour résoudre ce problème à l'échelle nationale, il est recommandé d'adopter une législation établissant l'équivalence fonctionnelle de la signature électronique et de la signature sur papier, à l'image des lois types de la CNUDCI sur le commerce électronique et sur les signatures électroniques. Cette disposition d'ensemble donnerait aux références à la signature ou à l'authentification une nouvelle interprétation qui permettrait de tenir compte de l'équivalent électronique fonctionnel de ces deux pratiques. À l'échelle internationale, le même résultat peut être obtenu par l'adoption de la Convention des Nations Unies de 2005 sur l'utilisation de communications électroniques dans les contrats internationaux (art. 9.3)[12]. Étant donné que cette convention ne s'applique qu'aux transactions internationales, il est recommandé en outre de créer pour les transactions nationales un texte juridique parallèle comportant une disposition d'ensemble qui donnerait de même aux références à la signature ou à l'authentification une nouvelle interprétation englobant l'équivalent électronique fonctionnel de ces deux pratiques.

[12] «Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux» (Convention sur l'utilisation de communications électroniques), Nations Unies, New York, 2007. Convention en vigueur depuis mars 2013. Document disponible à partir de mars 2013 à l'adresse suivante: http://www.uncitral.org/pdf/french/texts/electcom/06-57453_Ebook.pdf.

67. Il est proposé de localiser le processus sur papier et de le détailler étape par étape. L'évaluation du risque doit être un principe directeur, compte tenu du contexte de la transaction/du service, des contraintes juridiques, des contraintes opérationnelles, etc. Les parties doivent être autorisées et encouragées à satisfaire aux prescriptions fonctionnelles d'une signature manuelle en employant d'autres méthodes.

C. Créer un cadre juridique

68. Des exemples d'environnement juridique propice sont présentés dans l'annexe A. La capacité opérationnelle de remplacer une signature manuelle par une méthode électronique devra s'accompagner d'une législation appropriée accordant un statut égal à ces méthodes d'authentification. Ce cadre juridique devra prévoir l'acceptabilité des méthodes de transmission et des processus d'archivage de substitution par les tribunaux. Il faudra peut-être examiner ensemble ou séparément deux aspects importants: le cadre juridique des opérations du secteur privé et celui des opérations entre le secteur privé et les organismes publics.

69. En ce qui concerne les opérations entre les entreprises privées et entre les entreprises et les consommateurs, les gouvernements devront entreprendre une étude (y compris des études de comparaison juridique et d'analyse des lacunes du commerce électronique) afin de définir un ensemble approprié de mesures qu'il y aura peut-être lieu de prendre pour régler les questions juridiques relatives à l'authentification des échanges nationaux et internationaux de données commerciales.

70. En ce qui concerne les opérations entre les entreprises et les organismes publics, le gouvernement, au plus haut niveau, devra d'abord faire adopter par les organes délibérants le texte autorisant les organismes publics à proposer l'option de la mise à jour, de la présentation ou de la divulgation des informations par voie électronique, lorsque cette option peut remplacer le support papier. Dans le cadre de ce mandat, le gouvernement devra, en concertation avec d'autres organismes et le secteur privé, formuler des recommandations pratiques concernant les aspects juridiques liés à l'utilisation de méthodes électroniques de classement et d'enregistrement par les organismes publics, de façon à ce que ceux-ci puissent quant à eux faire une évaluation appropriée de leur mission. Ces organismes devront prêter attention à la manière de concevoir le processus afin de protéger leurs droits, ainsi qu'à la meilleure manière de réduire au minimum leurs risques d'ordre juridique.

71. Les pouvoirs publics devront, lorsque c'est possible, donner aux entreprises privées des indications à ce sujet. Toute indication fournie par le gouvernement et/ou l'organisme concerné devra en outre tenir compte des prescriptions légales en cours en ce qui concerne l'utilisation, le stockage et la divulgation des informations, ainsi que leur utilisation en tant que preuve auprès des tribunaux ou des organes administratifs.

72. Les cadres législatifs devront être examinés régulièrement pour correspondre aux pratiques commerciales en vigueur. Le droit public doit s'efforcer, chaque fois que possible, d'être en harmonie avec les pratiques économiques, meilleures pratiques et normes en vigueur.

Annexe A.1

Environnement juridique propice

Liste de contrôle recommandée pour l'examen de leur environnement juridique par les organismes publics

- ✓ Conformité avec les lois et règlements applicables?
- ✓ Conformité avec les lois sur la confidentialité?
- ✓ Plan détaillé visant à examiner toutes les questions soulevées par le passage à un système électronique?
- ✓ Concertation avec les parties concernées, y compris les autres administrations et organismes pertinents?
- ✓ Y a-t-il une loi ou un règlement imposant que les informations utilisées au cours du processus soient présentées sous une forme particulière, sur papier ou autre? Si une partie du processus est sur papier, comment satisfaire à ces prescriptions?
- ✓ Y a-t-il une obligation légale ou une nécessité administrative de conserver les informations? Et dans l'affirmative, pendant combien de temps?
- ✓ Les informations sont-elles importantes pour la sécurité nationale, la santé ou la sécurité publique, l'intérêt général, la protection de l'environnement ou d'autres objectifs publics essentiels?
- ✓ Le fait que ces informations ne soient pas disponibles a-t-il des répercussions sur le public?
- ✓ Quelle est l'importance des informations pour la mission/les programmes de l'organisme?
- ✓ Y a-t-il des répercussions sur les revenus de l'organisme?
- ✓ Pourrait-il être nécessaire d'utiliser les informations dans une procédure pénale ou une autre procédure judiciaire?

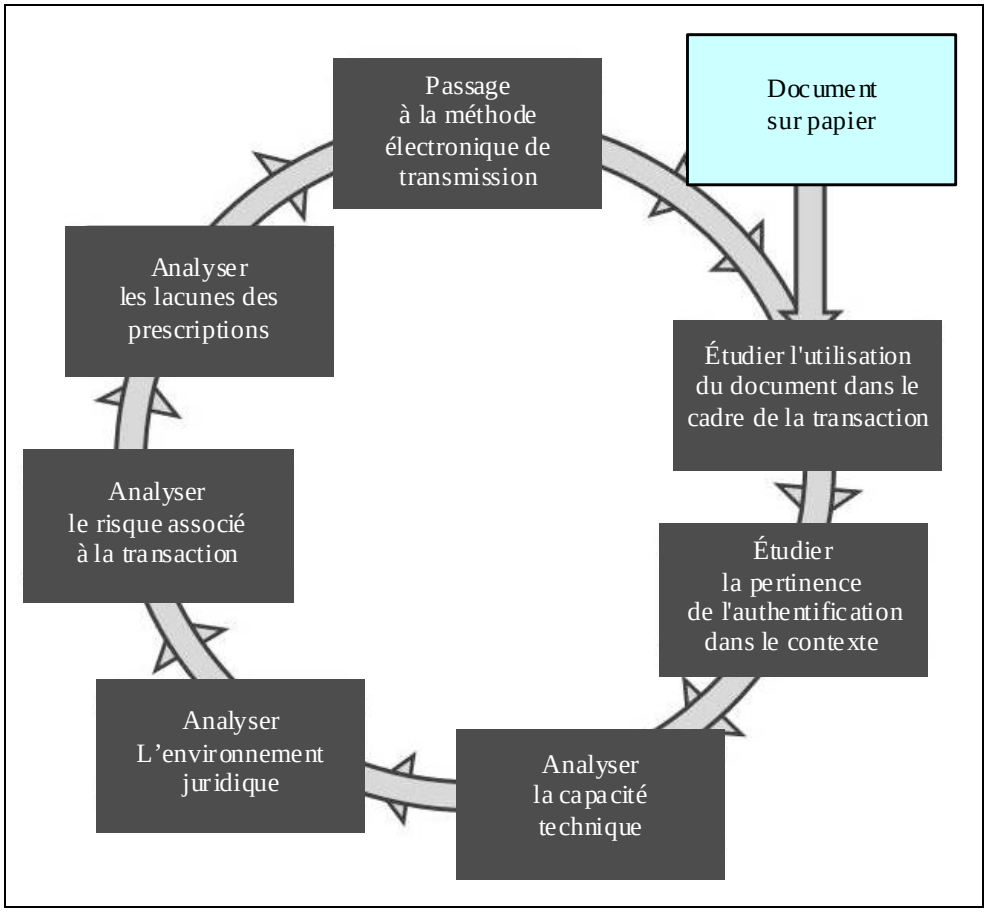
Annexe A.2

Cercle vertueux applicable à l'examen des documents commerciaux

1. Pour atteindre l'objectif qui consiste à supprimer l'obligation de signer les documents commerciaux ou, lorsque cela n'est pas possible immédiatement, à envisager d'autres méthodes d'authentification, la Recommandation n° 14 préconise d'examiner régulièrement les documents utilisés dans les échanges commerciaux nationaux et internationaux. Cet examen serait effectué par un groupe de travail conjoint des secteurs public et privé afin que les prescriptions réglementaires et officielles et les besoins des milieux d'affaires soient pris pleinement en considération d'une manière ouverte, transparente et dépourvue d'exclusive.

2. Il est proposé que le groupe de travail applique la méthode indiquée dans la figure ci-dessous:

Figure 1



3. Le diagramme en forme de cercle vertueux décrit un programme d'examen régulier, tous les trois à cinq ans, de tous les documents utilisés dans les échanges commerciaux nationaux et internationaux. Pour faciliter l'application de ce programme et utiliser l'expertise des participants au groupe de travail, il faudrait répartir les documents en groupes fonctionnels spécifiques concernant par exemple le commerce, le transport, les questions financières (y compris les paiements internationaux) et les documents officiels. Cette répartition est proposée à titre indicatif et n'est pas exhaustive.

4. Un comité de contrôle ou de surveillance conviendrait d'un programme ou d'un calendrier des groupes d'examen afin d'assurer la cohérence des méthodes et des résultats de ces différents groupes. Adopter cette approche devrait faciliter la réalisation et assurer l'efficacité du programme. Le fait que celui-ci soit structuré devrait en outre épargner du temps et du travail aux participants aux différents groupes d'examen.

5. Le programme d'examen régulier déboucherait sur un plan d'action visant à supprimer l'obligation de signer un grand nombre de documents commerciaux. Lorsque cela ne sera pas possible immédiatement, le plan d'action devra offrir des moyens imaginatifs et innovants de remplacement par des méthodes d'authentification. À cet égard, les membres des groupes d'examen devraient adopter le principe d'une simplification et d'une facilitation des processus commerciaux au moyen de solutions qui, tout en étant solidement étayées et mûrement pesées, seraient radicales.

6. S'il adopte, ou quand il adoptera le principe d'un programme d'examen conçu comme un cercle vertueux, le groupe de travail devra, pour assurer le succès de cet examen, tenir compte de certaines conditions préalables, d'abord et surtout de la capacité technique du gouvernement et des milieux d'affaires de mettre en œuvre le plan d'action proposé. Il devra s'assurer de la capacité du gouvernement de recueillir, de partager (entre les différents services administratifs et les organismes de réglementation), de stocker et de récupérer les données, ainsi que d'accepter et de traiter d'autres formes d'authentification.

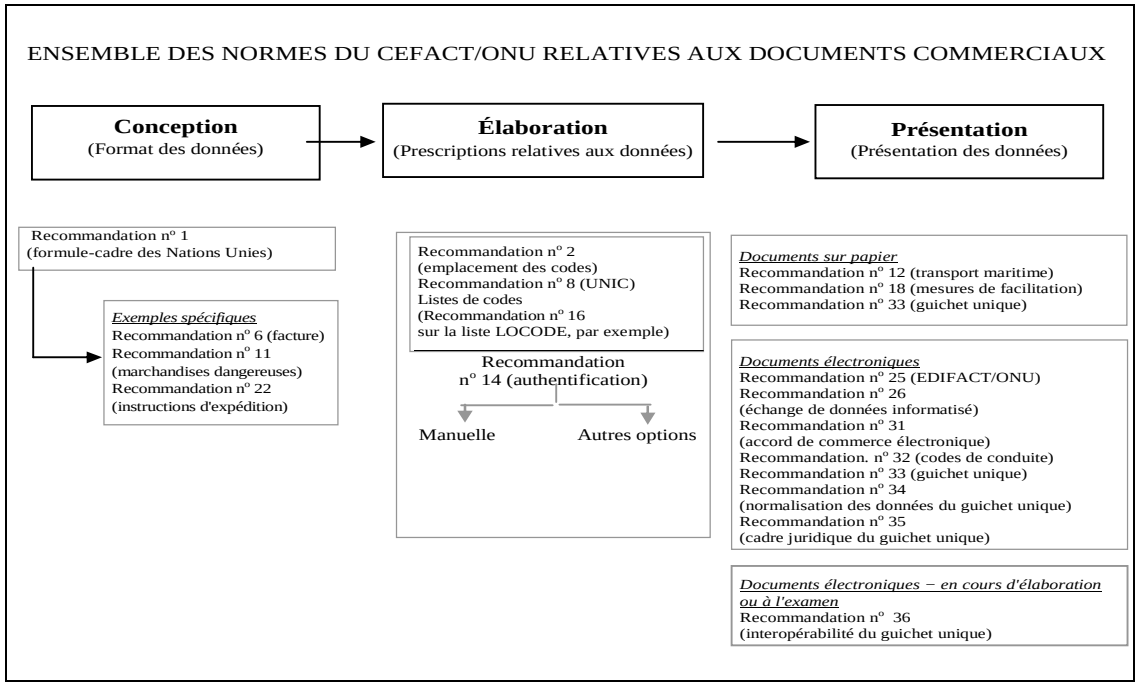
7. En ce qui concerne les milieux d'affaires, en particulier le secteur des petites et moyennes entreprises, le groupe de travail devra déterminer si les négociants ont la capacité de créer, de recevoir et de traiter les messages de données électroniques types. Les entreprises devront aussi démontrer qu'elles sont en mesure, au moyen de leurs propres systèmes et fichiers commerciaux, de conserver les données électroniques, dans l'éventualité de contrôles administratifs par audit. Pour évaluer la capacité, il est également important de veiller à ce que le droit commercial permette que dans une transaction commerciale, des formules d'authentification autres que la signature engagent les partenaires à exécuter les contrats.

Annexe A.3

Ensemble de normes relatives aux documents commerciaux

Le CEFACT-ONU propose un ensemble de recommandations, de lignes directrices, de conseils et de bonnes pratiques en matière de conception, d'élaboration et de présentation (y compris la transmission électronique) des documents commerciaux utilisés dans le commerce national et international. La Recommandation n° 14 fait partie de cet ensemble et le diagramme ci-dessous (fig. 2) est une représentation graphique de la place qu'elle occupe dans l'ensemble intégré de normes relatives aux documents commerciaux.

Figure 2



Annexe B.1

Mise en œuvre technique

Liste de considérations relatives à la détermination des besoins d'authentification dans le contexte d'une transaction donnée

Les points essentiels ci-après doivent être pris en considération pour déterminer les besoins d'authentification. Cette liste doit être applicable aux transactions avec les organismes publics comme aux transactions d'entreprise à entreprise.

Considérations relatives au contexte

- ✓ Une signature est-elle seulement nécessaire pour authentifier le document commercial?
- ✓ Une transmission électronique du document est-elle appropriée?
- ✓ Type de transaction;
- ✓ Volume des transactions (nombre de transactions différentes);
- ✓ Valeur de la transaction;
- ✓ Nombre de signataires par transaction;
- ✓ Fréquence des transactions commerciales;
- ✓ Nature de l'activité commerciale (qui sont les parties, quel est le secteur d'activité?);
- ✓ Coût et avantages;
- ✓ Conformité aux pratiques et usages commerciaux.

Considérations techniques

- ✓ Capacités du système et de l'équipement et leur éventuelle interaction (matériel/logiciel);
- ✓ Lorsqu'il est fait appel à un intermédiaire, procédures d'authentification mises en place par celui-ci (procédure d'audit?);
- ✓ Quels sont les dangers/vulnérabilités/risques face aux attaques?
- ✓ Quels sont les atouts de chaque méthode d'authentification de remplacement?
- ✓ Problèmes de compatibilité des méthodes d'authentification;
- ✓ Analyse des techniques existantes et viabilité de ces techniques à des fins de conservation des données et/ou d'accès futur à ces données.

Considérations juridiques

- ✓ Contexte juridique (national [local, fédéral…], régional, international, sectoriel, jurisprudence, droit privé … comme décrit ci-dessus au point 3a));
- ✓ Adhésion aux modèles de lois de la CNUDCI sur le commerce électronique ou la signature électronique, qui permettent la reconnaissance mutuelle des méthodes d'authentification;
- ✓ Accords internationaux/reconnaissance mutuelle bilatérale ou multilatérale (reconnaissance de normes, arrangements financiers, problèmes d'interopérabilité, etc., par exemple);

- ✓ Connaissance des problèmes juridiques et/ou des restrictions réglementaires dans l'environnement de chaque partenaire commercial;
- ✓ La transaction doit-elle avoir une validité en droit ou l'authentification a-t-elle uniquement pour objet de renforcer la sécurité?
- ✓ Existence de mécanismes d'assurance contre les communications non autorisées.

Considérations d'ordre relationnel

- ✓ Détermination du niveau de protection nécessaire et du risque potentiel de responsabilité de l'organisme/du partenaire commercial;
- ✓ Importance et valeur des informations contenues dans la communication électronique;
- ✓ Degré d'acceptation ou de non-acceptation de la méthode d'identification dans le secteur ou le domaine considéré au moment où la méthode a été convenue et à celui où le message électronique a été communiqué;
- ✓ Relation entre les partenaires commerciaux (confiance, etc.).

Annexe B.2

Typologie des moyens d'authentification électronique

Les différents types d'équivalents électroniques de la signature manuelle sont entre autres les suivants (liste non exhaustive présentée par ordre alphabétique afin de souligner qu'aucune de ces méthodes n'est favorisée):

Accord structurel permettant un échange électronique de données sans authentification

- Signature d'un contrat ponctuel sur papier permettant un échange électronique de données (lettre électronique de transport aérien de l'IATA).

Appareils (authentification à l'aide d'un téléphone mobile, par exemple)

- Identification de l'appareil au moyen d'une technique comme le message textuel (recevoir un code de validation ou envoyer un message au passage de la frontière);
- La personne devra être associée d'une manière ou d'une autre à l'appareil.

Case «Oui» ou «J'accepte» sur laquelle cliquer

- Cliquer sur une case «Oui» ou «J'accepte»;
- Cela ira souvent de pair avec une autre procédure d'identification, comme un paiement par carte de crédit (pour un paiement) et un nom d'utilisateur/mot de passe. Même le fait d'accepter une licence en cliquant sur une case «J'accepte» sera suivi par l'installation d'un logiciel (par exemple).

Image d'une signature

- Une signature manuelle est numérisée et envoyée par télécopie. Il peut s'agir d'un document complet qui a été signé à la main et qui est numérisé/transmis par télécopie. Il peut s'agir aussi de l'image d'une signature ou d'une signature numérisée qui est jointe par la suite au document.

Méthodes biométriques

- «Un identificateur biométrique est une mesure servant à identifier une personne par ses caractéristiques physiques ou comportementales. Les caractéristiques susceptibles d'être utilisées pour la reconnaissance biométrique sont l'ADN; les empreintes digitales; l'iris; la rétine; la forme de la main ou du visage; la thermographie faciale; la forme de l'oreille; la voix; l'odeur corporelle; le dessin des vaisseaux sanguins; l'écriture; la démarche et la dynamique de frappe» (CNUDCI, Promouvoir la confiance, op. cit., par. 53);
- La mesure biométrique peut être unique en son genre, mais il peut y avoir d'autres formes de problème systémique, comme la garantie qu'une empreinte digitale donnée (par exemple) appartient à une personne donnée.

Nom d'utilisateur/mot de passe

- Mots de passe et codes sont utilisés à la fois pour contrôler l'accès à des informations ou à des services et pour «signer» des communications électroniques. Dans la pratique, cette deuxième utilisation est moins fréquente que la première, en raison du risque de compromettre le code s'il est transmis dans un message non codé. Toutefois, les mots de passe et les codes sont la méthode d'«authentification» la plus utilisée pour les contrôles d'accès et la vérification de l'identité, dans de nombreuses opérations, y compris pour la plupart des opérations bancaires en ligne, les retraits d'espèces aux guichets automatiques et les transactions par carte de crédit. (CNUDCI, Promouvoir la confiance, op.cit., par. 63).

PGP (Pretty Good Privacy)

- «Pretty Good Privacy» (PGP) est un logiciel de protection des données fondé sur deux clefs. La première est un système de chiffrement à clef publique destiné à chiffrer les informations recueillies sans identification personnelle. La deuxième est la clef de déchiffrement, qui est un code privé connu uniquement par le propriétaire et qui permet de récupérer les données chiffrées.

Question personnelle

- Vérification de l'identité au moyen d'une question dont la réponse n'est connue que de la personne concernée.

Réseau de communication

- Identification par la participation à un réseau. Il peut s'agir d'un vaste réseau multipartite (comme ODETTE dans l'industrie automobile ou SWIFT). Il peut aussi s'agir d'une liaison de point à point (comme un réseau privé virtuel entre deux points d'accès);
- Cela va souvent de pair avec un autre moyen comme le nom d'utilisateur/mot de passe.

Sceau (sceau de la société)

- Signature numérique qui s'applique une société par opposition à une signature personnelle.

Signature dactylographiée

- Insérée dans la signature de la partie émettrice, à la fin d'un document − un message électronique par exemple (ce qui est souvent vérifié dans le contexte de la transaction − dans cet exemple, une deuxième vérification peut être faite par l'expéditeur du message électronique).

Signature numérique

- La «signature numérique» désigne des applications technologiques qui utilisent la cryptographie asymétrique, autrement dit un système de chiffrement à clef publique, pour garantir l'authenticité des messages électroniques et l'intégrité de leur contenu. La signature numérique peut prendre de multiples formes, telles que la signature avec arrêt sur défaillance, la signature aveugle et la signature indéniable.
- La création de l'infrastructure permettant de mettre en place et de gérer le processus de certification sera prise en considération.

Signature sur fichier

- Signature d'un accord avec un partenaire (par exemple une agence de voyages) qui permet de téléphoner ou d'envoyer un message électronique à ce partenaire pour acheter des produits/services à l'aide de la méthode de paiement stipulée dans les dossiers dudit partenaire.

Signature sur tablette

- Signature manuelle sur un appareil à écran tactile.

Validation par une tierce partie

- Identification de l'auteur d'un document validée par une tierce partie, par exemple.