Nations Unies ECE/TRADE/C/CEFACT/2018/7

Conseil économique et social

Distr. générale
13 février 2018
Français
Original : anglais

Commission économique pour l'Europe

Comité exécutif de la CEE

Centre pour la facilitation du commerce et les transactions électroniques

Vingt-quatrième session
Genève, 30 avril-1er mai 2018
Point 7 b) de l'ordre du jour provisoire
Recommandations et normes : autres produits à noter

Livre blanc sur un environnement transfrontière de confiance

Garantir la fiabilité et la valeur juridique des interactions électroniques internationales

Résumé

Dans le cadre d'échanges d'informations par voie électronique, la question peut parfois se poser de la portée juridique des données ou, en d'autres termes, de savoir si l'information reçue est juridiquement contraignante. Le présent livre blanc s'appuie sur les travaux de la Recommandation nº 14 de la CEE concernant l'authentification des documents commerciaux pour donner des orientations relatives à la création d'un cadre de reconnaissance mutuelle entre les pays visant à garantir la portée juridique des informations, lorsque des niveaux de fiabilité plus élevés sont requis ou souhaités. Ce cadre de référence mutuelle constitue l'environnement transfrontière de confiance. Ce document pourrait éventuellement servir de base aux futurs travaux sur le sujet.

Le présent document est soumis à la vingt-quatrième session plénière pour qu'il en soit pris note.

GE.18-02195 (F) 130318 140318
1802195

I. Introduction

1. Le présent document a pour objet de faciliter et d'encourager la création d'un environnement transfrontière de confiance en vue de garantir la valeur juridique des échanges internationaux de documents et de données électroniques entre des autorités publiques et des personnes physiques ou morales. Il est destiné aux parties intéressées par la création, l'exploitation et l'utilisation concrète de telles infrastructures transfrontières.

2. Internet est devenu un outil et un environnement familiers pour les services électroniques aux particuliers et aux personnes morales de différents pays. Ces services présentent des avantages évidents, mais un certain nombre de problèmes organisationnels et juridiques entravent la généralisation de leur utilisation, notamment dans les cas où les parties ont besoin d'un certain degré de confiance mutuelle et dans les services électroniques qu'elles utilisent. Un des principaux défis est d'assurer la validité légale des documents électroniques et de garantir la portée juridique des interactions électroniques en général. Il s'agit d'un problème pressant aux niveaux national (au sein d'un pays donné) et international (interactions de participants relevant de la compétence de différents États).

3. On trouvera ci-après quelques cas de figure dans lesquels un certain *degré de confiance* est requis :

- Procédures d'appel d'offres électroniques, en particulier dans les cas où l'autorité contractante est un organisme public ou une grande entreprise. Ceux-ci exigent généralement un degré de fiabilité plus élevé en ce qui concerne les documents commerciaux de leurs opérateurs économiques.
- Certains documents commerciaux et de transport échangés dans le cadre de procédures commerciales transfrontières.
- Procédures de règlement des litiges, notamment en ligne. Elles exigent l'identification et l'authentification sans équivoque du demandeur et du défendeur.
- Assurance électronique. Il devrait y avoir un mécanisme permettant de vérifier de façon fiable les certificats d'assurance.

4. La nécessité impérieuse de créer des environnements nationaux propices au commerce sans papier est soulignée dans certains arrangements régionaux pour la facilitation du commerce transfrontière sans papier, comme l'Accord-cadre sur la facilitation du commerce transfrontière sans papier en Asie et dans le Pacifique, adopté par la Commission économique et sociale pour l'Asie et le Pacifique (CESAP). Le présent livre blanc a notamment pour objet d'aider les gouvernements et les organisations régionales et internationales à mettre en place et à gérer ces environnements d'une manière interopérable.

5. Comme il l'a fait savoir dans sa Recommandation n° 14, le CEFACT-ONU préconise la suppression (si possible) des règles, pratiques ou contrats excessifs pour faciliter les procédures du commerce international. Il reste néanmoins des cas de transactions commerciales dans lesquelles les participants aspirent à un *degré de confiance* mutuelle élevé. Ce livre blanc a précisément pour objet de faciliter ce type de cas.

6. Le présent livre blanc examine les principes relatifs à la création et à la gestion d'organisations régionales et mondiales de coordination visant à renforcer la confiance dans l'échange international de données et de documents électroniques entre des participants (autorités publiques et personnes physiques et morales) qui interagissent dans le cadre d'une structure électronique.

7. Ce livre blanc comporte essentiellement des dispositions d'ordre organisationnel et, en partie, technologique, concernant les services de confiance dans le domaine des technologies de l'information et de la communication (TIC). Des dispositions relatives à l'instauration de régimes juridiques appropriés pourront être élaborées par d'autres organismes.

8. Ce livre blanc a généralement pour objet de contribuer à garantir les droits et les intérêts juridiques des citoyens et des organisations dans le cadre d'opérations électroniques concernant des informations, opérations à *valeur juridique*[1] effectuées via Internet et d'autres systèmes de TIC ouverts d'utilisation de masse.

9. Pour atteindre un *degré de confiance* plus élevé dans les interactions électroniques, le présent livre blanc étudie la possibilité de mettre en place une *infrastructure de confiance commune* − plateforme de base aisément extensible qui offre des services de TIC spécialisés et de confiance ainsi qu'un accès unifié à ces services.

10. Le CEFACT-ONU reconnaît le principe de la neutralité technologique et ne propose donc aucune technologie en particulier pour servir de base aux *infrastructures de confiance commune*. Il appartient aux gouvernements de choisir les technologies qui leur assureront le *degré de confiance* voulu dans les interactions électroniques. Ce livre blanc est axé sur les aspects relatifs à l'organisation de l'*infrastructure de confiance commune* et aborde des questions techniques uniquement dans la mesure nécessaire pour permettre l'application dans la pratique des méthodes préconisées.

II. Principe de base de l'infrastructure de confiance commune

11. Quiconque participe à des interactions électroniques a généralement recours à certains types de services de TIC (courrier électronique, stockage en ligne, portails Web ou autres). Si le *degré de confiance* entre les participants et dans les services de TIC qu'ils utilisent est suffisant, aucune modification n'est nécessaire. En revanche, si le degré de confiance mutuelle entre les participants n'est pas suffisant ou si les participants ne font pas suffisamment confiance aux services qu'ils utilisent, il pourrait alors être utile d'avoir recours à une tierce partie de confiance pour contribuer à renforcer le *degré de confiance* dans les interactions électroniques. Les services fournis par ces tierces parties sont appelés des *services de confiance*.

12. Dans ce livre blanc, les *services de confiance* peuvent être de différents types (remplissant des fonctions différentes) et présenter des *niveaux de qualification* différents. Les *services de confiance* ayant un *niveau de qualification élevé* relèvent d'un ou plusieurs accords internationaux ; ils satisfont aux conditions et respectent les règles établies par les coordonnateurs internationaux. Les *services de confiance* ayant un *niveau de qualification de base* relèvent d'un ou plusieurs accords commerciaux et peuvent être établis, par exemple, dans le cadre de grands projets internationaux et appliquer les pratiques optimales reconnues pour les prestataires de services de confiance. L'audit auquel il convient de soumettre les *services de confiance* devraient être fonction de leur *niveau de qualification*.

13. L'ensemble des *services de confiance* qui relèvent du cadre juridique, organisationnel et technique constitue l'*infrastructure de confiance commune*. Cette infrastructure est une plate-forme de base aisément extensible qui fournit un accès unifié à des *services de confiance*.

14. Les particularités naturelles (notamment historiques, culturelles, politiques, économiques et techniques) propres aux différentes régions du monde peuvent susciter, à l'intérieur de ces régions, différents *degrés de confiance* dans les interactions électroniques.

15. L'objectif principal d'une *infrastructure de confiance commune* est de garantir la *valeur juridique* des interactions électroniques entre usagers en fournissant des *services de confiance* offrant différents *niveaux de qualification* (nul, de base et élevé) aux participants à une interaction électronique.

[1] L'association de l'attribut « valeur juridique » à une interaction électronique nécessitera un cadre juridique qui sort du champ du présent livre blanc.

16. Cette garantie institutionnelle doit être fournie dans le cadre des activités commerciales de prestataires spécialisés, qui :

- Fournissent aux usagers un ensemble de services de TIC de confiance ;
- Respectent des régimes juridiques établis, lesquels comportent entre autres des limites au traitement des données à caractère personnel ; et
- Exercent leur activité dans le cadre d'une infrastructure de confiance commune.

III. Principes relatifs à la création d'une *infrastructure de confiance commune*

- **Extensibilité** : l'infrastructure de confiance commune devrait être conçue de telle sorte qu'elle soit aisément extensible. Il serait ainsi possible d'y intégrer de nouveaux participants, notamment des pays, des participants supranationaux, des prestataires de services de confiance et des systèmes de registre.
- **Traçabilité** : si des participants à une interaction électronique le demandent, toute interaction électronique effectuée dans le cadre de l'infrastructure devrait être enregistrée et mise à disposition pour le règlement d'un litige, le cas échéant.
- **Rentabilité** : l'évaluation des risques devrait être prise en compte dans la détermination de la variante concrète de l'architecture de l'infrastructure. Les coûts liés à la création et au fonctionnement de l'infrastructure devraient être inférieurs aux pertes que pourraient induire les dysfonctionnements ou les actes de malveillance dont les TIC seraient éventuellement l'objet.
- **Complexité** : les aspects juridiques, organisationnels et technologiques devraient être décrits de manière cohérente lors de la création de l'infrastructure. Une description détaillée est garante du bon fonctionnement du système tout entier et de chacun de ces éléments.

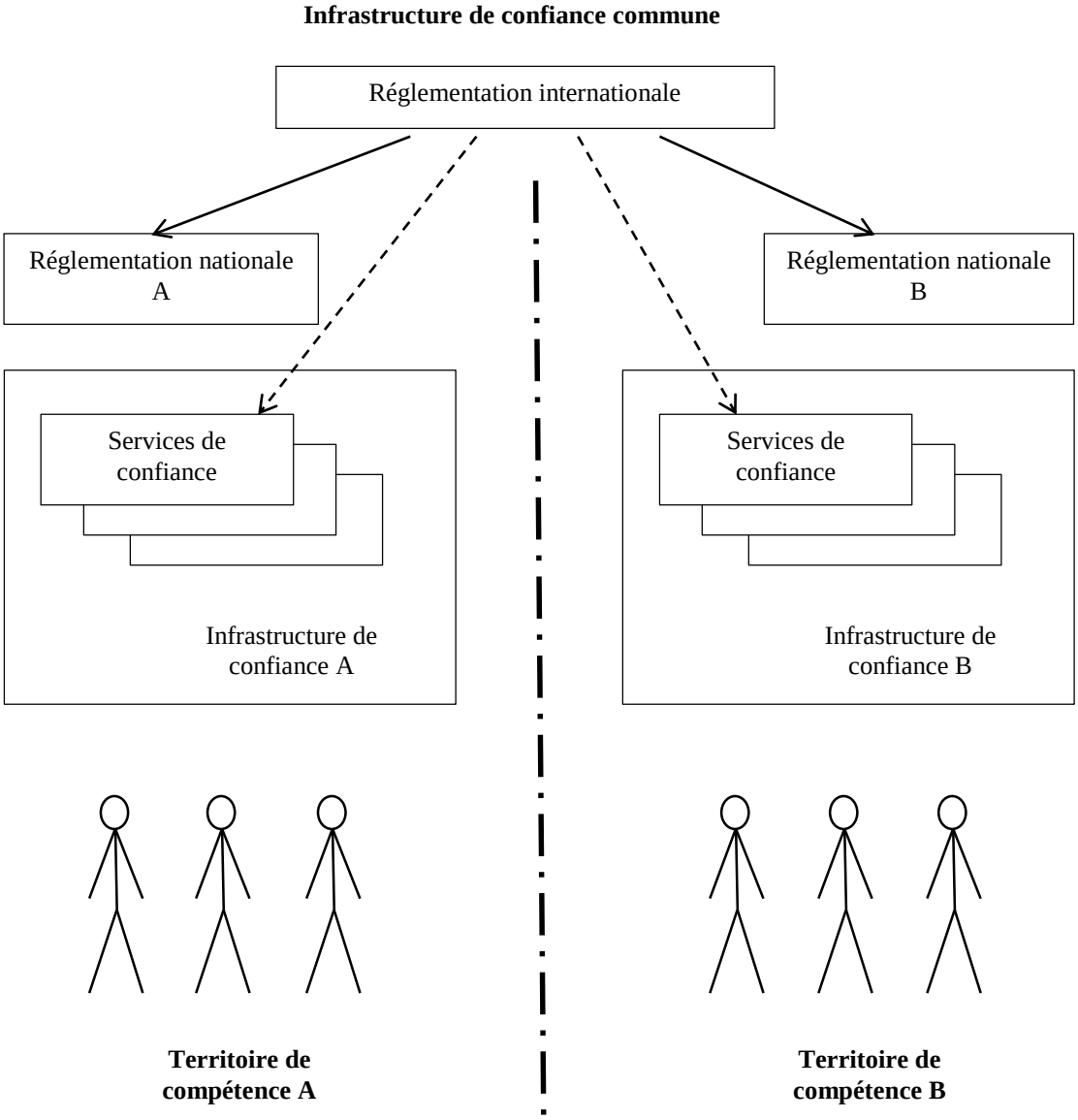
IV. Méthodes de coordination de l'*infrastructure de confiance commune*

17. L'architecture de l'*infrastructure de confiance commune* est déterminée conformément aux principes énoncés dans la section précédente. La coordination de l'infrastructure s'effectue à trois niveaux : juridique, organisationnel et technologique.

A. Niveau juridique

18. L'*infrastructure de confiance commune* peut s'élaborer sur une base à domaine unique ou multidomaine. Dans le contexte de la réglementation juridique et organisationnelle, la base multidomaine est la variante la plus compliquée. La figure 1 présente le schéma général d'une approche envisageable de la réglementation juridique. Les flèches en pointillés indiquent les cas dans lesquels aucune réglementation n'est appliquée, ou ne peut être appliquée, à l'échelle nationale.

Figure 1
Niveau juridique



19. La réglementation juridique des interactions réalisées dans le cadre de l'*infrastructure de confiance commune* s'articule en deux volets : l'un international, l'autre national. La réglementation juridique internationale se fonde sur les types de documents suivants :

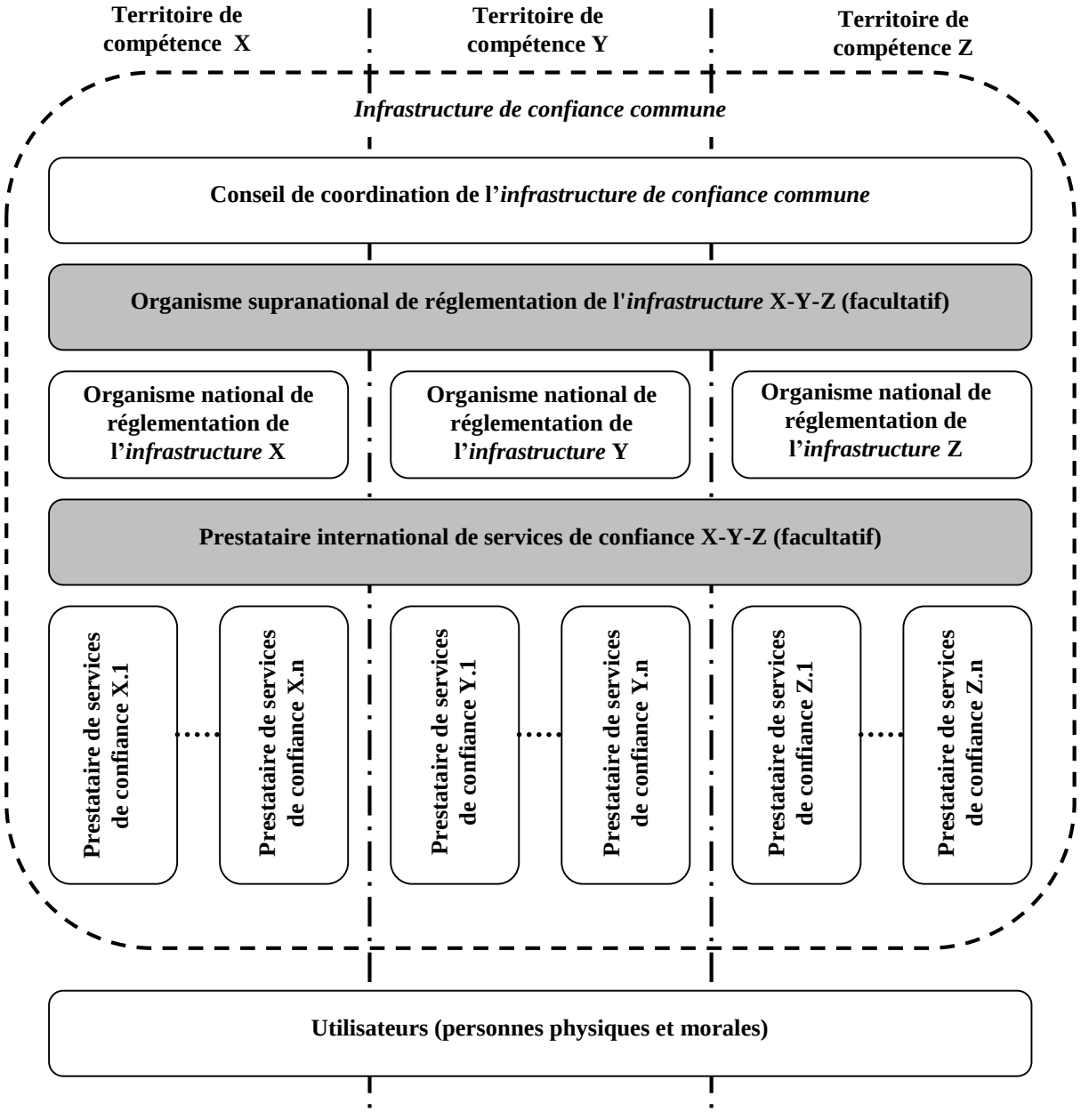
- Traités/accords internationaux ;
- Documents législatifs des différentes organisations internationales ;
- Normes et règlements internationaux ;
- Accords entre participants aux interactions électroniques transfrontières sur des questions données ;
- Lois types.

20. La réglementation juridique nationale se fonde sur un ensemble de documents prescriptifs qui établissent des normes dans chaque territoire de compétence.

B. Niveau organisationnel

21. La reconnaissance mutuelle de la *portée juridique* des documents et des données électroniques traités par des *services de confiance* fournis dans différents territoires de compétence pourrait être assurée avec la création et la mise en œuvre d'un organe spécialisé (appelé, dans cet exemple, « Conseil de coordination de l'*infrastructure de confiance commune* »), englobant des organismes nationaux de réglementation qui auraient intégré cet organe de leur plein gré. Les activités du Conseil de coordination pourraient être régies par une charte qui devrait être reconnue et signée par tous les membres agréés, à savoir les organismes de réglementation de l'échange de données électroniques représentés principalement par les organismes nationaux de réglementation de l'*infrastructure de confiance commune*. La figure 2 présente un cadre général de coordination au niveau organisationnel. Les éléments facultatifs sont signalés par des cadres grisés.

Figure 2
Niveau organisationnel



22. Le Conseil de coordination de l'*infrastructure de confiance commune* publie un certain nombre de documents liés à sa charte, notamment sur :

- **Les conditions** que les membres du Conseil de coordination doivent respecter pour être membres à part entière ;
- **Des lignes directrices** en matière de supervision « parallèle » en vue de l'admission au Conseil, et de vérification mutuelle périodique pour maintenir la participation volontaire au Conseil ;
- **Les critères de conformité** que doivent respecter les prestataires de services de confiance et les méthodes d'application de ces critères ;
- **Les mécanismes d'évaluation ou de vérification** des prestataires de services de confiance en ce qui concerne le respect des critères ci-dessus.

23. Chaque pays est représenté au sein de l'*infrastructure de confiance commune* par son organisme national de réglementation de l'infrastructure (voir fig. 2), qui réglemente les activités des prestataires de *services de confiance* dans son territoire de compétence.

24. Pour les groupements d'États à forte intégration (par exemple, l'Union économique eurasienne ou l'Union européenne), il existe la possibilité de créer un organisme supranational de réglementation de l'*infrastructure de confiance commune* (fig. 2, organisme supranational de réglementation de l'infrastructure X-Y-Z). Un seul organisme supranational de réglementation X-Y-Z remplace alors un groupe d'organismes nationaux de réglementation X, Y et Z.

25. L'extension naturelle de l'*infrastructure de confiance commune* se traduit dans la pratique par la procédure d'admission de nouveaux membres au Conseil de coordination de l'infrastructure (nouveaux participants nationaux et supranationaux) et par le mécanisme permettant de vérifier que les prestataires de *services de confiance* satisfont aux *critères de conformité* définis par le Conseil de coordination (nouveaux prestataires de *services de confiance*).

26. Les prestataires internationaux de *services de confiance* peuvent fournir, entre autres, un type spécifique de services de confiance, à savoir des passerelles interdomaines neutres. La principale fonction de ces passerelles consiste à assurer la reconnaissance mutuelle (légalisation) des documents et données électroniques. Ces passerelles reliant différents *domaines* les uns aux autres sont les éléments qui permettent d'établir une *infrastructure de confiance commune*.

27. Les passerelles interdomaines peuvent être établies simplement aux niveaux juridique et organisationnel ; ou à un niveau plus complexe (juridique, organisationnel et technique).

28. Dans le premier cas, les *domaines* mis en rapport créent une base juridique commune qui leur permet de coopérer les uns avec les autres (voir la section sur le niveau juridique ci-dessus). Cette base juridique définit un ensemble complet d'exigences, de critères et de conditions préalables qui assure, voire garantit, la reconnaissance juridique mutuelle (légalisation) des documents électroniques ayant une *portée juridique*.

29. Sur le plan organisationnel, les procédures et processus d'interaction entre différents *domaines* doivent maintenir un *degré de confiance* suffisant entre ces *domaines* pour assurer la reconnaissance mutuelle (légalisation) des documents et données électroniques provenant de *domaines* ou de territoires de compétence différents.

30. Pour atteindre le *degré de confiance* requis, cet ensemble d'exigences, de critères et de conditions préalables doit réglementer, entre autres, la création et l'exploitation d'un environnement international neutre, c'est-à-dire d'un environnement extérieur à tout *domaine* (indépendant). Le Conseil de coordination de l'*infrastructure de confiance commune* et les prestataires internationaux de services de confiance sont des composantes de cet environnement international neutre, lequel pourrait être exploité dans un cadre juridique neutre, défini par un organisme international.

31. Lorsque des passerelles interdomaines sont établies uniquement aux niveaux juridique et organisationnel, elles sont mises en œuvre simplement au moyen de traités, d'accords et de procédures organisationnelles. Une telle infrastructure juridique et organisationnelle peut être prise en charge par des *services de confiance* distincts (vérification de la signature électronique, vérification des droits, horodatage, etc.), sans qu'il soit nécessaire de consacrer un *service de confiance* spécifique à la fonction de passerelle.

32. Dans le deuxième cas (plus complexe), lorsque des passerelles interdomaines sont établies aux niveaux juridique, organisationnel et technique, celles-ci transforment en outre un document de manière à le rendre conforme aux exigences (attributs, format, structure et autres) applicables aux documents électroniques du *domaine*[2] (territoire de compétence) du destinataire qui ont une *portée juridique*. Ainsi, le *service de confiance* offrant une passerelle interdomaines peut se substituer à plusieurs *services de confiance* remplissant une seule fonction spécifique (vérification de la signature électronique, vérification des droits, horodatage ou autre). Comme toujours, lorsqu'ils sont mis en œuvre sur le plan technique, les *services de confiance* offrant une passerelle interdomaines doivent également fonctionner dans le cadre d'un environnement international neutre.

33. Les méthodes de création de passerelles interdomaines devraient prendre en considération l'utilisation de profils de transition dans lesquels le passage d'un *domaine* à l'autre serait décrit et défini. Ces profils devraient tenir compte, entre autres, des fondements juridiques de la coopération entre les *domaines* reliés ainsi que des *niveaux de qualification* des mécanismes d'identification utilisés dans les *domaines* concernés.

34. Pour pouvoir devenir un prestataire national de services de confiance, tout prestataire de ce type de services devrait être accrédité par l'organisme national de réglementation de l'*infrastructure de confiance commune* du territoire de compétence dont il relève. Les prestataires internationaux de services de confiance devraient être accrédités par le Conseil de coordination de l'*infrastructure de confiance commune*. Les conditions d'accréditation des prestataires de *services de confiance* , ainsi que les conditions régissant leurs activités devraient être établies par les critères de conformité définis par le Conseil de coordination ainsi que par d'éventuels additifs émis par les différents organismes nationaux de réglementation de l'*infrastructure de confiance commune*.

35. Les utilisateurs de services électroniques au sein du Conseil de coordination de l'*infrastructure de confiance commune* peuvent être aussi bien des particuliers que des entités juridiques. Le choix du *niveau de qualification* voulu du *service de confiance* est laissé à leur appréciation ou déterminé par un accord.

36. Les services devraient être fournis par les prestataires respectifs, à savoir les prestataires de *services de confiance*, lesquels devraient être intégrés dans l'*infrastructure de confiance commune*.

37. Les *services de confiance*, éléments de l'*infrastructure de confiance commune*, pourraient se présenter différemment, selon le *degré de confiance* entre les *domaines* (territoires de compétence). À titre d'exemple, si le degré de confiance entre les membres de l'*infrastructure de confiance commune* est « élevé » ou « moyen », il est utile d'utiliser des *services de confiance* internationaux centralisés, mis en œuvre conformément aux normes convenues. Si le *degré de confiance* est « faible », les *services de confiance* sont établis selon le principe de la décentralisation, c'est-à-dire que l'on crée des *services de confiance* nationaux dans chaque territoire de compétence.

C. Niveau technologique

38. Il peut y avoir un grand nombre de possibilités sur le plan technologique pour la mise en place de *services de confiance*. L'interopérabilité est la caractéristique primordiale de l'*infrastructure de confiance commune*. À ce niveau, la réglementation dépend de

[2] Les « domaines » ou « domaines de confiance » peuvent correspondre à un seul ou à plusieurs territoires de compétence.

l'application de différentes normes et instructions énoncées dans les documents du Conseil de coordination de l'infrastructure.

39. Le présent livre blanc préconise la coopération étroite avec les principales organisations de normalisation technique, comme l'ISO, l'ETSI, le W3C et le CEN, en vue d'atteindre le niveau de coordination nécessaire sur le plan technologique[3].

V. Services des infrastructures de confiance : méthodes pour garantir l'interopérabilité technique

40. Pour déterminer les types de *services de confiance* à fournir, il est conseillé de se poser la question de savoir si des attributs de base sont requis pour permettre au document de remplir sa fonction juridique.

Tableau 1
Attributs requis pour que le document puisse remplir sa fonction juridique

N°	*Type d'attribut*	*Obligatoire Oui/non*	*Description/observations*
1.	Contenu	oui	Au moins un des attributs suivants donne le contenu, à savoir les informations contenues dans le document, indépendamment de sa forme (sur papier ou sous forme électronique) : 1) Type de document 2) Degré de confidentialité du document 3) Intitulé du document 4) Table des matières 5) Corps du document (obligatoire) 6) Annexes Ainsi, l'intégrité et l'authenticité des informations doivent être garanties lors du traitement, de la conservation et du transfert des données.
2.	Statut juridique de l'émetteur du document	oui	Les attributs suivants constituent le statut juridique de l'émetteur : 1) Type de logo 2) Nom de l'émetteur 3) Données de référence de l'émetteur (adresse, coordonnées, etc.) 4) Cachet apposé sur le document
3.	Statut ou attributions (droits) du signataire	non	Description succincte des droits du signataire et indication de leur durée de validité.
4.	Signature	oui	Les attributs suivants constituent la signature : 1) Signature de l'émetteur 2) Cachet de signature de confirmation 3) Cachet de signature d'approbation

[3] Organisation internationale de normalisation (ISO), Institut européen des normes de télécommunication (ETSI), World Wide Web Consortium (W3C), Comité européen de normalisation (CEN).

N°	*Type d'attribut*	*Obligatoire Oui/non*	*Description/observations*
			4) Visa (autorisation/cachet de confirmation) 5) Cachet « copie certifiée conforme » 6) Cachet de l'Organisation émettrice 7) Etc.
5.	Heure	oui	Indication de l'heure de signature, sur la base d'une source d'horodatage fiable (aspect lié à la validité).
6.	Lieu	non	L'indication du lieu de signature (lieu où le signataire a exprimé sa volonté de signer en cliquant sur « signature ») est facultative. Si ce type de service n'est pas disponible, l'attribut caractéristique du lieu peut être considéré comme faisant partie des attributs du contenu.

41. Les types de *services de confiance* de base (fonctions disponibles sur demande expresse) sont les suivants :

a. Création, vérification et confirmation des signatures et des cachets ;

b. Contrôle du statut juridique ;

c. Création, vérification et confirmation des horodatages ;

d. Fourniture de passerelles interdomaines neutres ;

Note : s'il existe une passerelle entre différents domaines (territoires de compétence), un profil devrait être créé pour cette passerelle sur la base d'un accord entre les domaines concernés. Chaque profil de passerelle interdomaines devrait « connaître » les attributs requis pour chaque domaine. Sur le plan technologique, la passerelle interdomaines devrait donner lieu à une certaine conversion de protocoles ou à la conversion de différents protocoles ou normes, d'un domaine à l'autre. On trouvera une description mathématique des fonctions des passerelles interdomaines à l'annexe 2. Les services de confiance (y compris les passerelles interdomaines) fonctionnent avec les mécanismes nationaux d'identification, d'une part, et une infrastructure de confiance internationale (autres services de confiance), d'autre part.

e. Identification des personnes physiques et morales.

42. Les types d'attributs ci-après (voir tableau 1) supposent l'identification préalable des personnes physiques ou morales concernées :

- Statut juridique de l'émetteur du document ;
- Statut ou attributions (droits) du signataire ;
- Signature.

43. Les types de *services de confiance* a) et b) s'appuient sur ce type d'attribut et supposent donc également l'identification préalable des personnes physiques ou morales concernées. Les services d'identification sont fournis par des prestataires spécialisés en la matière et peuvent être fournis à différents *niveaux de qualification* : nul, de base et élevé. Le Conseil de coordination de l'*infrastructure de confiance commune* doit décider ou convenir des mécanismes d'identification pouvant entrer en ligne de compte, ainsi que des conditions minimales qui leur sont applicables. Il peut y avoir des mécanismes d'identification spécifiques du Conseil de coordination et/ou des renvois à des normes internationales et/ou à des mécanismes d'identification notifiés à l'intérieur d'un *domaine* spécifique.

44. La définition des *niveaux de qualification* des mécanismes d'identification peut se fonder sur les procédures d'identification et les ensembles d'attributs d'identification eux-mêmes. Les *niveaux de qualification* des mécanismes d'identification peuvent être essentiels pour la réglementation des interactions entre différents *domaines*. Les régimes juridiques peuvent définir des ensembles d'attributs d'identification aux fins des activités commerciales des prestataires spécialisés dans l'identification et des prestataires fonctionnels, ensembles dont la maintenance peut être assurée par les *services de confiance* (service d'identification). L'activité des prestataires spécialisés dans l'identification peut être réglementée au moyen d'exigences organisationnelles et techniques spéciales visant à garantir la protection des données personnelles.

45. Note : les services d'archivage à long terme et de vérification en la matière peuvent faire partie des fonctions du service de TIC ou d'un type spécial de service de confiance.

46. Note : les systèmes électroniques existants devraient être pris en compte de manière à réduire au minimum les exigences relatives à leur mise à jour et à leur connexion à l'*infrastructure de confiance de base*.

VI. Niveaux de qualification des services de l'infrastructure de confiance commune

47. Le *niveau de qualification* d'un *service de confiance* traduit la capacité manifeste du service concerné à satisfaire à un ensemble préétabli d'exigences.

48. Un *service de confiance* peut avoir différents *niveaux de qualification* progressifs. Plus bas est le degré de confiance mutuelle entre les participants et dans les services de TIC traitant les interactions électroniques (création, accès, transformation, transmission, destruction, etc.), plus haut est le *niveau de qualification* des *services de confiance* demandé.

49. Les caractéristiques des *niveaux de qualification* des *services de confiance* sont décrites dans le tableau ci-après.

Tableau 2
Caractéristiques des niveaux de qualification des services de confiance

	Degré de confiance des participants entre eux et dans les services de TIC		
	Degré de confiance élevé	*Degré de confiance non négligeable*	*Degré de confiance limité*
Niveaux de qualification des services de confiance	Aucun service de confiance requis (niveau de qualification « nul »)	Niveau de qualification de base	Niveau de qualification élevé
Régime juridique régissant le fonctionnement des services de confiance	s.o.	Fondé sur des accords commerciaux et/ou des pratiques commerciales courantes	Fondé sur des accords internationaux (conventions) et/ou une réglementation internationale applicable directement[4]
Architecture organisationnelle des services de confiance	s.o.	Projets de grande envergure de tous types	Conseil de coordination de l'infrastructure de confiance commune (voir partie IV *supra*)

[4] Par exemple, les *services de confiance* fonctionnant conformément au règlement eIDAS de l'Union européenne, à l'Accord de l'Union économique eurasienne ou à d'autres documents.

	Degré de confiance des participants entre eux et dans les services de TIC		
	Degré de confiance élevé	*Degré de confiance non négligeable*	*Degré de confiance limité*
Exigences technologiques relatives aux services de confiance	s.o.	Satisfaire aux pratiques optimales reconnues pour les prestataires de services de confiance	- Répondre aux critères de conformité définis par le Conseil de coordination de l'infrastructure de confiance commune ET - Satisfaire aux exigences énoncées dans la réglementation nationale applicable (aux prestataires nationaux de services de confiance)

50. Lorsque les *services de confiance* qui participent au cycle de vie du document (notamment à la chaîne de passerelles interdomaines établies entre l'émetteur et le destinataire du document) n'ont pas le même *niveau de qualification*, le *niveau de qualification* global est égal au niveau le plus bas.

VII. Communication avec des organisations dans différents cadres de normalisation

51. Le présent livre blanc préconise la description de différents régimes juridiques possibles :

- Fondés sur des accords internationaux (conventions) et/ou sur la réglementation internationale directement applicable ;
- Fondés sur des accords commerciaux et/ou sur les pratiques commerciales courantes ;
- Sans aucune réglementation internationale spéciale.

52. Les régimes juridiques peuvent aussi être appuyés par des organismes traditionnels (autorités gouvernementales, institutions de règlement judiciaire, institutions d'assurance contre les risques, institutions notariales et autres), par le biais de la reconnaissance mutuelle des documents électroniques sécurisés par des *services de confiance*.

53. Les régimes juridiques établis peuvent aussi prévoir la mise en place d'exigences spéciales applicables au soutien matériel et financier des activités commerciales des prestataires spécialisés dans l'éventualité de préjudices causés à leurs clients, notamment en cas d'atteinte à l'intégrité des données à caractère personnel.

54. Les garanties institutionnelles et les régimes juridiques pour la création et l'exploitation d'environnements transfrontières de confiance régionaux et mondiaux devraient être pris en compte dans un document distinct établi par un organisme spécialisé.

55. Le présent document recommande de décrire les mécanismes d'interaction entre, d'une part, les États et leurs institutions internationales et, d'autre part, d'autres structures internationales dans le cadre de la création d'un environnement transfrontière de confiance commun.

a. Par l'adhésion complète ou partielle d'un État à un régime juridique existant sur la base des traités internationaux et/ou des normes internationales directement applicables, dans le cadre desquels la mise en place d'un environnement transfrontière de confiance régional a déjà été engagée ou menée à bonne fin. Ce régime juridique existant offre des garanties institutionnelles aux sujets d'interactions électroniques.

b. Dans le cadre d'une interaction entre différentes institutions internationales :

- Dans un premier temps, un groupe d'États crée un domaine régional qui assure des garanties institutionnelles aux sujets d'interactions électroniques au sein du régime juridique déterminé par ces États ;
- Dans un deuxième temps, les protocoles d'interactions de confiance avec d'autres institutions internationales sont spécifiés dans le cadre de la reconnaissance mutuelle de différents régimes juridiques. Cette reconnaissance mutuelle devrait prendre en compte les garanties institutionnelles et les exigences en matière de sécurité des informations relatives à chacune des institutions internationales, éventuellement sur la base de passerelles interdomaines fonctionnant dans le cadre d'un régime juridique international.

c. Dans le cadre d'une interaction entre un État et d'autres d'États ou avec des institutions internationales :

- Dans un premier temps, un État crée son propre domaine, lequel fonctionne dans le cadre d'un régime juridique national spécifié par cet État ;
- Dans un deuxième temps, les protocoles d'interactions de confiance avec d'autres États et/ou des institutions internationales sont spécifiés dans le cadre de la reconnaissance mutuelle de différents régimes juridiques. Cette reconnaissance mutuelle devrait prendre en compte les garanties institutionnelles et les exigences en matière de sécurité des informations relatives à ces États et institutions internationales, éventuellement sur la base de passerelles interdomaines fonctionnant dans le cadre d'un régime juridique international.

VIII. Communication avec des organisations internationales dans différents cadres de normalisation sur les aspects techniques et organisationnels relatifs à la création et à l'exploitation d'un environnement transfrontière de confiance

56. Ce livre blanc préconise la prise en compte des aspects relatifs à la normalisation ci-après :

Aspects technologiques

57. Dans ce contexte, la normalisation a principalement pour objet de faciliter l'interopérabilité technique au sein de l'environnement transfrontière de confiance. Elle devrait s'intéresser à tous les aspects techniques qui se répercutent inévitablement sur l'interopérabilité fonctionnelle et l'interopérabilité relative à la sécurité, notamment les formats des documents et des données, les protocoles de communication, la conversion de formats et de protocoles, les interfaces techniques et l'équivalence des niveaux d'assurance (sécurité) des composantes techniques.

Aspects organisationnels

58. Sur le plan organisationnel, la normalisation a principalement pour objet de maintenir un *degré de confiance* suffisant entre les domaines pour assurer la reconnaissance mutuelle (légalisation) des documents et données électroniques provenant de *domaines* (territoires de compétence) différents. À cet égard, on peut citer, notamment, les procédures d'audit de conformité des prestataires de *services de confiance* engagées par des organismes indépendants d'évaluation de la conformité ; les procédures d'accréditation des organismes d'évaluation de la conformité ; et les procédures d'audits mutuels « pair à pair »

entre membres du Conseil de Coordination de l'*infrastructure de confiance commune*, ainsi que les objets et domaines soumis à ces audits et les critères de vérification applicables.

59. Les aspects spécifiés devraient être pris en considération dans la mesure où ils s'appliquent à différents *niveaux de qualification* de *services de confiance*. De fait, lorsqu'un *service de confiance* dont le *niveau de qualification* est faible interagit avec un *service de confiance* dont le *niveau de qualification* est élevé, le *niveau de qualification* global de l'interaction entre ces deux services sera, au mieux, égal au *niveau de qualification* le plus bas.

Annexe I

Glossaire

Les termes qui apparaissent en *italique* sont définis aux fins du présent livre blanc.

Aux fins du présent document, on entend par :

- ***Infrastructure de confiance commune***
    - Une infrastructure conçue pour contribuer à garantir la *valeur juridique* des interactions électroniques transfrontières. L'*infrastructure de confiance commune* fournit un ensemble de *services de confiance* harmonisés sur les plans juridique, organisationnel et technologique.
- ***Degré de confiance*** (confiance mutuelle entre les participants à des interactions électroniques et confiance dans les services de TIC qui rendent ces interactions possibles)
    - Fonction sociétale d'un degré de confiance attestée ou ressentie des participants à une interaction électronique les uns envers les autres et dans les services de TIC qui la rendent possible
- ***Portée juridique*** (d'une opération)
    - Propriété d'une opération (processus) autorisant la création (production) de documents (unités de données) ayant une *valeur juridique*.
- ***Portée juridique*** (d'un document)
    - Propriété d'un document (unité de données) en vertu de quoi il est possible de modifier le statut juridique d'un sujet de droit (personne physique ou morale ayant, en droit, la capacité d'exercer des droits et d'accomplir des devoirs juridiques).
    - Un document qui a une *portée juridique* revêt automatiquement une *valeur juridique* assortie d'un contenu concret.
- ***Validité légale (également appelée « valeur légale »)*** (d'un document)
    - Propriété d'un document (unité de données) utilisé par les autorités judiciaires (jugé conforme aux dispositions du droit applicable. La *validité légale* d'un document lui est conférée par la législation en vigueur, par l'autorité de l'émetteur et par l'ordre d'émission donné (il faut notamment qu'il puisse y être fait référence ultérieurement pour consultation).
- ***Niveau de qualification*** (d'un service)
    - Caractéristique d'un service qui satisfait manifestement à un ensemble préétabli d'exigences.
- ***Degrés de confiance*** (entre domaines)
    - Fonction sociétale qui détermine le degré de confiance entre *domaines*.
    - Selon un *degré de confiance* établi, les *domaines* sont prêts à échanger une certaine quantité de ressources et à utiliser conjointement certaines infrastructures ; en d'autres termes, les *domaines* sont prêts à déléguer une partie de leurs propres pouvoirs, fonctions et ressources à une *infrastructure de confiance commune*, dans laquelle chacun d'eux a confiance. Plus le *degré de confiance* dans cette infrastructure est élevé, plus nombreux sont les pouvoirs que les *domaines* seront disposés à lui déléguer.

- ***Domaine*** (domaine de confiance)
    - Espace juridique et d'information utilisant la même *infrastructure de confiance commune*. Un *domaine* peut coïncider avec un ou plusieurs territoires de compétence.
- ***Service de confiance***
    - (Définition de haut niveau) − service électronique ayant pour ambition de garantir un certain *degré de confiance* entre les participants à une interaction électronique.
- ***Interaction électronique de confiance***
    - L'échange électronique de données, quelles qu'elles soient, effectué de telle sorte qu'il soit accepté sans conteste par l'utilisateur de ces données, selon sa propre politique opérationnelle. C'est la politique opérationnelle de chaque utilisateur qui détermine si l'interaction électronique peut être considérée comme une interaction de confiance. Par conséquent, la détermination de la fiabilité des données reçues dans le cadre d'un échange électronique varie d'un utilisateur à l'autre. Toute interaction électronique passe par des services de TIC (fournisseur d'accès à Internet, fournisseur de services de messagerie électronique, services d'échange de messages de toutes sortes, stockage en ligne, etc.), mais l'*interaction électronique de confiance* suppose l'utilisation de *services de confiance*.

Annexe II

Description mathématique des fonctions des passerelles interdomaines

L'ensemble de règles permettant de convertir les exigences à satisfaire entre deux domaines A et B devrait être défini à l'intérieur d'une passerelle interdomaines.

$A=\{a_1, a_2,..., a_N\}$

$B=\{b_1, b_2,..., b_M\}$

$E(a)=A \rightarrow B$

A est l'ensemble des exigences (attributs) applicables au domaine A, B est l'ensemble des exigences applicables au domaine B, et E(a) est l'ensemble de règles de conversion de A à B. Gardant à l'esprit que, dans une situation réelle, le poids (c'est-à-dire la quantité d'exigences) de l'ensemble A peut ne pas être égal à celui de l'ensemble B ($N \neq M$), des règles devraient être définies pour faire en sorte que les deux ensembles aient un poids égal K ($K=MAX(N, M)$).

Le degré de confiance dans cet ensemble de règles de conversion peut être défini comme une conversion en un surensemble universel d'exigences opérée à l'intérieur de chaque domaine.

$E(a)=A \rightarrow X$

$E(x)=X \rightarrow B$

X étant un surensemble universel d'exigences applicables à A et B.