Nations Unies A/CN.9/WG.IV/WP.155

Assemblée générale

Distr. limitée
13 septembre 2018
Français
Original : anglais

Commission des Nations Unies pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Cinquante-septième session
Vienne, 19-23 novembre 2018

Projet d'instrument relatif à la reconnaissance juridique transfrontière de la gestion de l'identité et des services de confiance – proposition de l'Allemagne

Note du Secrétariat

L'Allemagne a soumis au Secrétariat un document que le Groupe de travail examinera à sa cinquante-septième session. On trouvera en annexe à la présente note la traduction du texte tel qu'il a été reçu par le Secrétariat.

V.18-06085 (F) 021118 051118

Annexe

Projet d'instrument relatif à la reconnaissance juridique transfrontière de la gestion de l'identité et des services de confiance

Réaffirmant leur conviction que le développement des technologies de l'information et de la communication est une condition préalable à une croissance économique durable et une meilleure qualité de vie en général ;

Notant que les communications électroniques améliorent l'efficacité de la gouvernance publique et des activités commerciales, renforcent les relations économiques extérieures, offrent de nouveaux débouchés à des parties et des marchés auparavant isolés, jouant ainsi un rôle fondamental dans la promotion du commerce et du développement économique, aux niveaux tant national qu'international ;

Sachant que l'incertitude quant aux règles applicables, sur le plan technique et juridique, au flux de documents électroniques échangés entre les organismes publics et les administrations locales, les personnes physiques et morales des États parties au [projet d'instrument] [1] constitue un obstacle au développement des interactions électroniques ;

Convaincus qu'il est nécessaire d'instaurer la confiance entre tous les participants pour renforcer les interactions électroniques ;

Partant du principe que des règles uniformes accordent aux parties la liberté de choisir les supports, technologies, services d'identification et de confiance appropriés, en tenant compte des principes de la neutralité technologique et de l'équivalence fonctionnelle, dans la mesure où les moyens choisis par les parties sont pertinents aux fins de la législation existante ;

Reconnaissant que des systèmes de confiance centralisés et décentralisés sont possibles et faisables et qu'ils permettent d'accélérer les progrès et l'économie numérique, notamment de développer dans un environnement de confiance le commerce électronique et les transports, le règlement des litiges en ligne, l'administration en ligne et les services publics électroniques, la formation en ligne et les soins de santé en ligne, ainsi que divers registres électroniques et les services financiers électroniques;

Les parties sont convenues de ce qui suit :

Section I. Champ d'application

Article premier. Champ d'application

1. Le présent [projet d'instrument] définit les caractéristiques fondamentales d'un environnement transfrontière de confiance, à savoir un ensemble de conditions normatives, organisationnelles et techniques permettant d'instaurer la confiance dans l'échange transfrontière d'informations sous forme électronique entre autorités publiques, personnes physiques et personnes morales.

2. Pour déterminer le champ d'application du présent [projet d'instrument], l'appartenance à un État des participants à l'interaction électronique transfrontière, leur statut civil et juridique, ou encore la nature des documents et messages électroniques qu'ils échangent ne sont pas pertinents.

3. L'environnement transfrontière de confiance comprend les segments suivants :

[1] Le [projet d'instrument] est un texte provisoire en attendant le texte définitif dont la forme sera déterminée par la CNUDCI.

1) Un segment centralisé, qui définit les conditions réglementaires, organisationnelles et techniques pour instaurer la confiance dans l'échange de documents par voie électronique, en imposant des obligations contraignantes aux parties pour le contrôle des activités des prestataires de services de confiance, des logiciels et du matériel qu'ils utilisent dans les interactions électroniques transfrontières, des services de confiance et des procédures d'évaluation de la conformité des prestataires de services de confiance ainsi que des logiciels et du matériel qu'ils utilisent ;

2) Un segment autorégulé, qui définit les conditions réglementaires, organisationnelles et techniques pour instaurer la confiance dans l'échange de messages par voie électronique au moyen de bases de données distribuées et de la création d'unités de données qui reflètent la nature autorégulatrice des interactions électroniques transfrontières.

4. L'environnement transfrontière de confiance est utilisé par ses participants pour garantir le niveau de confiance nécessaire aux parties à l'interaction électronique. Le choix d'un segment particulier de l'environnement transfrontière de confiance, ou une combinaison de ces deux segments, conformément à l'article 1-3 du présent [projet d'instrument], est fonction de la nature des services numériques fournis, lesquels exigent que l'environnement transfrontière de confiance offre un certain niveau de confiance.

Section II. Dispositions générales

Article 2. Définitions

1. Aux fins du présent [projet d'instrument] :

1) Le terme « participants à l'environnement transfrontière de confiance » désigne les autorités publiques, le Conseil de coordination, les prestataires de services de confiance, les gestionnaires de bases de données distribuées, et les personnes physiques ou morales ;

2) Le terme « message électronique » désigne l'information créée, envoyée, reçue ou conservée à l'aide de réseaux d'information et de télécommunication ;

3) Le terme « document électronique » désigne un message électronique qui satisfait aux conditions nécessaires et suffisantes pour permettre la reconnaissance de son importance juridique, et dont la véracité et l'authenticité sont confirmées par le prestataire de services de confiance conformément au présent [projet d'instrument] ;

4) Le terme « enregistrements de données de transaction » désigne des messages électroniques authentifiés par des gestionnaires de bases de données distribuées et intégrés dans un bloc de données (valides) pertinent ;

5) Le terme « bloc de données (valides) pertinent » désigne un ensemble d'enregistrements de données de transaction créés conformément aux règles établies par les gestionnaires de bases de données distribuées ; ces blocs de données ne peuvent être modifiés ni complétés ;

6) Le terme « services de confiance » désigne les services qui confirment la véracité et l'authenticité des documents électroniques et/ou des informations qu'ils contiennent, notamment, mais pas uniquement, les services de création de signatures électroniques, d'application de cachets électroniques, d'horodatage électronique, ou de transmission électronique de documents et d'authentification des sites Internet ;

7) Le terme « interaction électronique transfrontière » désigne l'échange par l'intermédiaire de systèmes d'information de messages électroniques et/ou de documents électroniques entre les participants à l'environnement transfrontière de confiance ;

8) Le terme « Conseil de coordination » désigne l'organisme créé en application du présent [projet d'instrument] qui définit les prescriptions générales, contraignantes pour les Membres, régissant les activités des prestataires de services de confiance ainsi que les logiciels et le matériel qu'ils utilisent pour l'interaction électronique transfrontière, et les procédures d'évaluation de la conformité des prestataires de services de confiance et des logiciels et du matériel qu'ils utilisent ; le Conseil de coordination s'acquitte de toutes autres fonctions énoncées dans le présent [projet d'instrument] ;

9) Le terme « emplacement » désigne le lieu spécifié par une partie à l'environnement transfrontière de confiance comme lieu de résidence ; en l'absence de quoi, il désigne le lieu de résidence d'une personne ou le lieu de constitution d'une personne morale ;

10) Le terme « prestataire de services de confiance » désigne une personne physique ou morale qui satisfait aux exigences établies par le Conseil de coordination, qui a obtenu la confirmation de conformité à l'issue de la procédure établie par le Conseil de coordination et qui fournit des services de confiance au titre du segment centralisé de l'environnement transfrontière de confiance ;

11) Le terme « gestionnaires de bases de données distribuées (mineurs) » désigne les personnes physiques ou morales (y compris celles qui agissent de manière anonyme) qui utilisent les logiciels et le matériel nécessaires pour participer au segment autorégulé de l'environnement transfrontière de confiance en enregistrant les opérations et en vérifiant leur authenticité, en créant des blocs de données dans des bases de données distribuées et en vérifiant leur exhaustivité ;

12) Le terme « utilisateur » désigne une autorité publique, une personne physique ou morale qui est l'expéditeur ou le destinataire de messages électroniques et/ou de documents électroniques, y compris ceux envoyés par l'entremise des services fournis dans le cadre du segment autorégulé de l'environnement transfrontière de confiance ;

13) Le terme « systèmes d'information » désigne l'ensemble des technologies de l'information et du matériel conçus et utilisés pour créer, envoyer, recevoir, conserver ou autrement traiter les messages électroniques, y compris les documents électroniques, dans l'interaction électronique transfrontière ;

14) Le terme « signature ou cachet électronique » désigne des données électroniques, jointes physiquement ou associées logiquement à d'autres données électroniques, qui sont utilisées par le signataire pour signer des documents et qui attestent un lien entre le signataire et ces autres données électroniques de telle manière qu'un tiers peut vérifier son existence ultérieurement ;

15) Le terme « signataire » désigne la personne physique (dans le cas d'une signature électronique) ou la personne morale (dans le cas d'un cachet électronique) qui signe un document électronique en utilisant une signature ou un cachet électronique ;

16) Le terme « certificat qualifié de signature ou de cachet électronique » désigne une confirmation électronique qui permet d'associer des données à une personne physique (signature) ou morale (cachet) afin de vérifier la signature ou le cachet électronique et qui confirme au moins son identité ; ce certificat est délivré par un prestataire de services de confiance ayant satisfait à la procédure de conformité visée à l'article 8-6 du présent [projet d'instrument] et satisfaisant aux prescriptions du Conseil de coordination ;

17) Le terme « horodatage électronique » désigne des données sous forme électronique qui associent d'autres données électroniques à une date particulière et qui attestent l'existence de ces dernières à cette date, permettant ainsi aux participants à l'interaction électronique ou à un tiers de confirmer ultérieurement leur existence à une date précise ;

18) Le terme « service d'envoi recommandé électronique » désigne un service qui permet de transmettre par voie électronique des données entre des tiers et qui atteste le traitement des données transmises, y compris leur expédition et leur réception ; et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée ;

19) Le terme « certificat qualifié d'authentification de site Internet » désigne une confirmation électronique qui permet d'authentifier des sites Internet en les associant à une personne physique ou morale qui détient une confirmation délivrée par un prestataire de services de confiance ayant satisfait à la procédure de conformité visée à l'article 8-6 du présent [projet d'instrument] et satisfaisant aux prescriptions du Conseil de coordination ;

20) Le terme « identité » désigne des informations relatives à un sujet donné (en l'occurrence, l'utilisateur), qui, prenant la forme d'un ou plusieurs attributs, permettent au sujet d'être identifié de manière suffisante dans un contexte particulier ;

21) Le terme « moyen d'identification » désigne un élément matériel et/ou immatériel contenant l'identité d'un sujet donné (en l'occurrence, l'utilisateur) ;

22) Le terme « gestion de l'identité » désigne un ensemble de fonctions et de fonctionnalités (administration, gestion et tenue à jour, découverte, échanges de communication, corrélation et liens, application des politiques, authentification et assertions, par exemple) utilisées pour : i) garantir les informations d'identité (identificateurs, justificatifs d'identité et attributs, par exemple) ; ii) garantir l'identité d'une entité ; et iii) permettre des applications commerciales et sécuritaires.

23) Le terme « identification (fondamentale) primaire » désigne le processus consistant à réunir, vérifier et valider suffisamment d'attributs d'un sujet donné (en l'occurrence, l'utilisateur) pour définir et confirmer son identité sans contexte particulier.

L'identification primaire est généralement effectuée par l'autorité qui délivre le certificat d'identité primaire (par exemple, certificat de naissance, carte nationale d'identité, passeport, etc.) ;

24) Le terme « identification (transactionnelle) secondaire » désigne le processus consistant à réunir, vérifier et valider suffisamment d'attributs d'un sujet donné (en l'occurrence, l'utilisateur) pour définir et confirmer son identité dans un contexte particulier.

L'identification secondaire est généralement effectuée par un prestataire de services de confiance et peut être utilisée soit a) au moment de l'inscription pour identifier un sujet qui souhaite utiliser les services fournis par un prestataire de services de confiance, soit b) pour identifier un utilisateur qui souhaite utiliser un service de confiance en particulier.

a) Pour identifier le demandeur au moment de l'inscription, le prestataire de services de confiance utilise généralement un certificat primaire d'identité ou un résultat obtenu à l'issue d'une identification antérieure du demandeur. Après avoir identifié le demandeur, le prestataire de services de confiance établit/délivre son propre document secondaire d'identité de l'utilisateur (certificat secondaire d'identité) ;

b) Pour identifier un utilisateur souhaitant avoir recours à un service de confiance particulier, le prestataire de services de confiance demande à l'utilisateur, qui a déjà établi son identité conformément à l'alinéa a) de la présente définition, de s'identifier à l'aide de son certificat d'identité secondaire (par connaissance, par possession (y compris biométrique)).

25) Le terme « système d'identification » désigne un environnement (en ligne) pour les opérations liées à l'identification régi par un ensemble de règles, dans lequel des personnes physiques ou morales peuvent se faire mutuellement confiance parce que des sources faisant autorité établissent et authentifient leurs identités respectives.

Un système d'identification implique a) un ensemble de règles, de méthodes, de procédures et de routines, de technologies, de normes, de politiques et de processus, b) s'appliquant à un groupe d'entités participantes, c) régissant la collecte, la vérification, le stockage, l'échange, l'authentification et la fiabilité des attributs d'identité concernant une personne physique ou morale, d) dans le but de faciliter les opérations liées à l'identification.

26) Le terme « opération liée à l'identification » désigne toute opération impliquant deux ou plusieurs participants qui consiste à établir, vérifier, émettre, asserter, révoquer ou communiquer une identité, ou à s'y fier ;

27) Le terme « fournisseur d'identité » désigne a) une entité chargée d'identifier des personnes physiques ou morales, de fournir les moyens d'identification correspondants et de conserver et gérer ces informations pour le compte des sujets ;

28) Le terme « système d'identification notifié » désigne un système d'identification qui a) satisfait aux prescriptions du Conseil de coordination et b) a été notifié par le fournisseur d'identité qui exploite ce système d'identification au Conseil de coordination, conformément à l'article 5-2 du présent [projet d'instrument] ;

29) Le terme « niveau de garantie d'un système d'identification notifié » désigne un attribut (caractéristique) d'un système d'identification notifié qui a été défini par le fournisseur d'identité qui exploite ce système conformément aux prescriptions du Conseil de coordination visées à l'article 5-2 du présent [projet d'instrument] ;

30) Le terme « Membres » (du Conseil de coordination) désigne une personne morale i) ayant la capacité juridique et l'autorité en vertu de la législation interne de procéder à la reconnaissance juridique de la gestion de l'identité et des services de confiance, et ii) ayant officiellement reconnu toutes les dispositions du présent [projet d'instrument].

Article 3. Interprétation

1. Pour l'interprétation du présent [projet d'instrument], il sera tenu compte de son caractère international et de la nécessité de promouvoir l'uniformité de son application ainsi que d'assurer le respect de la bonne foi dans les interactions électroniques transfrontières et des autres principes visés à l'article 5 du présent [projet d'instrument].

2. Les questions concernant les matières régies par le présent [projet d'instrument] qui ne sont pas expressément tranchées par lui sont réglées selon les principes généraux dont il s'inspire ou, à défaut de ces principes, conformément à la loi applicable en vertu des règles du droit international privé.

Article 4. Principes

Les interactions électroniques transfrontières au sein de l'environnement transfrontière de confiance reposent sur les principes ci-après, qui s'appliquent aux deux segments de l'environnement transfrontière de confiance :

1) La neutralité technologique ;

2) L'équivalence fonctionnelle en ce qui concerne la gestion de l'identité et les services de confiance fournis ;

3) La protection des informations confidentielles, à savoir des informations protégées par le droit international et la législation interne des États parties, y compris le secret commercial et les données personnelles, dans les interactions électroniques transfrontières ;

4) L'utilisation des informations, documents et messages, y compris des blocs de données dans les bases de données distribuées, uniquement à des fins qui ne sont pas contraires au droit international et à la législation interne des États parties ;

5) La neutralité économique, qui se traduit par un bon rapport coût-efficacité et l'absence de distorsion en ce qui concerne la gestion de l'identité et les services de confiance fournis ;

6) La proportionnalité, à savoir que le contenu et les moyens employés doivent être conformes à l'objectif visé ;

7) L'autonomie des parties, à savoir la liberté accordée aux participants de choisir les supports, technologies, moyens d'identification et services de confiance appropriés à leurs besoins concrets ;

8) La non-discrimination.

Section III. Conseil de coordination

Article 5. Fonctions du Conseil de coordination

1. Le Conseil de coordination est l'organe chargé d'exercer les fonctions de direction dans le cadre du segment centralisé de l'environnement transfrontière de confiance, et les fonctions de facilitateur dans le cadre du segment autorégulé de l'environnement transfrontière de confiance.

2. Dans le segment centralisé de l'environnement transfrontière de confiance, le Conseil de coordination approuve au moins les prescriptions, procédures, politiques et conditions ci-après dont le respect manifeste par les participants permet la reconnaissance mutuelle des résultats de l'identification et des moyens d'identification ainsi que des résultats de l'utilisation de services de confiance :

A. Gestion de l'identité

1) Prescriptions concernant les propriétés et caractéristiques des systèmes d'identification utilisés pour procéder à une identification primaire remplissant les conditions de notification.

Ces prescriptions tiennent compte du fait que les systèmes d'identification sont établis et exploités dans le contexte national des États parties et qu'ils doivent respecter la législation interne applicable, notamment les dispositions nationales relatives à la certification des systèmes d'identification.

Ces prescriptions permettent de définir différents niveaux de garantie des systèmes d'identification notifiés ;

2) Responsabilité des fournisseurs d'identification des systèmes d'identification notifiés en cas de pertes ;

3) Procédures relatives à la reconnaissance mutuelle des résultats de l'identification obtenus et des moyens d'identification délivrés par les fournisseurs d'identification de systèmes d'identification notifiés ;

4) Détermination des effets juridiques – aux fins du présent [projet d'instrument] – sur la base de l'usage de systèmes d'identification notifiés, notamment la reconnaissance mutuelle des résultats de l'identification obtenus et des moyens d'identification délivrés par les fournisseurs d'identification de systèmes d'identification notifiés ; en tenant compte des différents niveaux de garantie des systèmes d'identification notifiés ;

5) Conditions fondamentales d'utilisation des systèmes d'identification notifiés ;

6) Prescriptions concernant les propriétés et caractéristiques des systèmes d'identification utilisés par des prestataires de services de confiance pour procéder à une identification secondaire des utilisateurs ;

7) Règles pour le règlement des litiges.

B. Services de confiance

1) Prescriptions relatives aux procédures de fonctionnement des prestataires de services de confiance, y compris en ce qui concerne leur responsabilité civile et leur audit ;

2) Prescriptions concernant les logiciels et le matériel utilisés dans les interactions électroniques transfrontières ;

3) Procédures d'évaluation de la conformité applicables aux prestataires de services de confiance, y compris d'évaluation de la conformité des systèmes d'identification utilisés pour procéder à l'identification secondaire des utilisateurs, ainsi que du matériel et des logiciels qu'ils utilisent (audit) ;

4) Responsabilité des prestataires de services de confiance en cas de pertes ;

5) Règles pour le règlement des litiges ;

6) Prescriptions pour les personnes morales et (ou) les personnes physiques intervenant dans la confirmation de la conformité des prestataires de services de confiance, y compris l'évaluation de la conformité des systèmes d'identification utilisés pour procéder à l'identification secondaire des utilisateurs, ainsi que du matériel et des logiciels qu'ils utilisent (audit) ;

7) Conditions fondamentales d'utilisation des services de confiance définies aux articles 15, 16, 17, 18, 19 et 20 du présent [projet d'instrument].

C. Autres documents prévus dans le présent [projet d'instrument]

3. En vertu du présent [projet d'instrument], les Membres conviennent d'exécuter ou de faire exécuter par les entités publiques et administrations autonomes locales, les utilisateurs, les prestataires de services et les services de confiance relevant de leur compétence les mesures prises par le Conseil de coordination conformément au paragraphe 2 du présent article.

4. Dans le segment autorégulé de l'environnement de confiance transfrontière, le Conseil de coordination :

1) Approuve la procédure recommandée pour confirmer le rattachement des gestionnaires de bases de données distribuées aux bases de données correspondantes ;

2) Approuve la procédure de notification au Conseil de coordination en cas d'incident dans une base de données distribuée, à savoir lorsque des messages électroniques, des enregistrements de données de transaction et des blocs de données dans les bases de données distribuées sont utilisés de manière contraire au droit international et à la législation interne des Membres ;

3) Organise la procédure à suivre par les prestataires de bases de données distribuées pour notifier au Conseil de coordination leur adhésion volontaire aux engagements de ce dernier de mettre en œuvre les dispositions du présent [projet d'instrument] en garantissant que les informations, documents et messages, y compris les blocs de données dans les bases de données distribuées, sont utilisés uniquement à des fins conformes au droit international et à la législation interne des Membres ; et pour informer le Conseil de coordination en cas d'incident concernant des informations contenues dans une base de données distribuée.

5. Les décisions et documents adoptés par le Conseil de coordination concernant le segment autorégulé de l'environnement transfrontière de confiance ont un caractère consultatif.

Article 6. Création et fonctionnement du Conseil de coordination

1. Le Conseil de coordination est composé de Membres qui siègent pour un mandat de quatre ans. Chaque Membre peut désigner un représentant autorisé.

2. Le Conseil de coordination peut créer les organes subsidiaires qu'il juge nécessaires à l'exercice de ses fonctions.

3. Chaque Membre du Conseil de coordination dispose d'une voix.

4. Les décisions du Conseil de coordination sur l'organisation de ses travaux sont prises par un vote affirmatif d'au moins deux tiers de ses Membres.

5. Les décisions du Conseil de coordination sur l'adoption des mesures visées à l'article 5-2 sont adoptées à l'unanimité.

6. Le Conseil de coordination établit son règlement intérieur et détermine notamment la procédure à suivre pour l'élection de son président, pour maintenir la confiance mutuelle entre les représentants responsables des Membres à l'égard de l'environnement transfrontière de confiance, et pour prendre des décisions concernant l'approbation des documents visés à l'article 5 du présent [projet d'instrument].

Section IV. Participants à l'environnement transfrontière de confiance

Article 7. Autorités publiques et administrations autonomes locales des États parties

1. Les autorités publiques participent à l'interaction électronique transfrontière pour s'acquitter des fonctions publiques qui leur incombent en vertu du droit interne des États parties, conformément aux règles établies par le présent [projet d'instrument] et aux mesures prises par le Conseil de coordination en conformité avec celui-ci.

2. Les autorités publiques sont habilitées à prendre leur propre décision concernant leur participation au segment autorégulé de l'environnement transfrontière de confiance.

3. Les autorités publiques sont habilitées à imposer des prescriptions supplémentaires pour l'interaction électronique en plus de celles établies par le présent [projet d'instrument] et des mesures prises par le Conseil de coordination en conformité avec celui-ci, pour autant qu'elles ne soient pas contraires à celles-ci, dans les cas prévus par le Conseil de coordination.

Article 8. Prestataires de services de confiance

1. Les prestataires de services de confiance participent au segment centralisé de l'environnement transfrontière de confiance.

2. Les prestataires de services de confiance peuvent fournir des services de confiance dans les limites fixées par un Membre particulier et/ou sur l'ensemble du territoire des États parties.

3. Les prestataires de services de confiance sont tenus de se conformer aux prescriptions établies par le Conseil de coordination, en fonction de leur champ d'action (l'ensemble du territoire des États parties ou certaines parties), et confirment leur conformité aux prescriptions selon les modalités établies par le Conseil de coordination.

4. Les prestataires de services de confiance sont tenus de publier sur Internet toute information sur l'acquisition ou la modification de leur statut de prestataire de services de confiance. Ils sont tenus d'informer les autorités compétentes du Membre responsable de toute modification touchant les services de confiance fournis et leur statut. Ils ont l'obligation d'informer les autorités compétentes et les membres du Conseil de coordination de tout incident concernant les échanges électroniques

transfrontières. Le Conseil de coordination établit la procédure à suivre pour fournir des informations et les conditions dans lesquelles celles-ci doivent être fournies.

5. Les prestataires de services de confiance sont tenus de souscrire une assurance couvrant la responsabilité civile ou doivent détenir une couverture financière suffisante selon les critères établis par le Conseil de coordination.

6. Les prestataires de services de confiance doivent faire l'objet d'une procédure d'évaluation (audit indépendant) de leur conformité ainsi que de la conformité des services qu'ils fournissent, notamment pour évaluer si les systèmes d'identification utilisés pour procéder à l'identification secondaire des utilisateurs et le matériel et les logiciels qu'ils utilisent sont conformes aux prescriptions du Conseil de coordination et selon les modalités définies par celui-ci.

Article 9. Audit indépendant de conformité. Assurance.

1. Seuls les prestataires de services de confiance ayant fait l'objet d'un audit indépendant de conformité ont le droit de fournir des services de confiance.

2. Les organismes ou institutions autorisés conformément à la procédure établie par le Conseil de coordination sont habilités à procéder à l'audit de conformité.

3. Les prestataires de services de confiance souscrivent une assurance couvrant la responsabilité civile conformément aux prescriptions établies par le Conseil de coordination.

Article 10. Gestionnaires de bases de données distribuées

1. Les gestionnaires de bases de données distribuées participent au segment autorégulé de l'environnement transfrontière de confiance.

2. Les gestionnaires de bases de données distribuées organisent l'interaction électronique transfrontière entre eux et avec les utilisateurs, sur la base des principes de l'autorégulation, et veillent au respect du présent [projet d'instrument] en ce qui concerne l'utilisation des informations, documents et messages, y compris des blocs de données dans les bases de données distribuées, uniquement à des fins qui ne sont pas contraires au droit international et à la législation interne des États parties, et en ce qui concerne la notification au Conseil de coordination d'incidents liés aux informations contenues dans des bases de données distribuées.

3. La notification volontaire au Conseil de coordination du respect volontaire de ces prescriptions permet au gestionnaire de bases de données d'être reconnu comme satisfaisant aux prescriptions du présent [projet d'instrument] en ce qui concerne l'utilisation des informations, documents et messages, y compris des blocs de données dans les bases de données distribuées, uniquement à des fins qui ne sont pas contraires au droit international et à la législation interne des Membres, et en ce qui concerne la notification au Conseil de coordination d'incidents liés aux informations contenues dans une base de données distribuée. La procédure de notification et la procédure à suivre pour établir une liste des gestionnaires de bases de données distribuées des Membres de l'environnement transfrontière de confiance sont définies par le Conseil de coordination.

Le Conseil de coordination a le droit de refuser de notifier au gestionnaire de bases de données distribuées figurant sur la liste s'il dispose d'informations sur des atteintes au droit international et à la législation interne des États parties commises par le gestionnaire.

4. L'interaction entre les gestionnaires de bases de données distribuées et le Conseil de coordination, ainsi qu'entre les gestionnaires de bases de données distribuées et les utilisateurs, peut avoir lieu sans identification des personnes physiques et morales qui gèrent des bases de données distribuées et les utilisent.

5. Lorsque le Conseil de coordination reçoit les informations concernant le non-respect des prescriptions du présent [projet d'instrument] visées au paragraphe 2 du

présent article par un gestionnaire de bases de données distribuées, ce dernier risque d'être exclu de la liste librement accessible de fournisseurs de bases de données distribuées parties à l'environnement transfrontière de confiance.

Article 11. Utilisateurs

1. Les utilisateurs sont les participants aux deux segments de l'environnement transfrontière de confiance.

2. En fonction du segment de l'environnement transfrontière de confiance, les utilisateurs échangent des messages électroniques et des documents électroniques, conformément aux règles établies par le Conseil de coordination et les prestataires de services de confiance, ou conformément aux règles établies par les gestionnaires de bases de données distribuées, respectivement.

Section V. Infrastructure de l'environnement transfrontière de confiance

Article 12. Matériel et logiciels utilisés par les prestataires de services de confiance

1. Les prestataires de services de confiance n'utilisent que des logiciels et du matériel satisfaisant aux procédures d'évaluation de la conformité prévues aux articles 8-6 et 9-1 pour fournir leurs services.

2. Les exigences fonctionnelles des logiciels et du matériel utilisé par les prestataires de services de confiance, et les prescriptions concernant les procédures à suivre pour évaluer la conformité des logiciels et du matériel aux exigences fonctionnelles, dans le respect du principe de la neutralité technologique, sont établies par le Conseil de coordination conformément aux articles 8-6, 9-1 et 9-2.

Article 13. Matériel et logiciels utilisés par les gestionnaires de bases de données distribuées

Les gestionnaires de bases de données distribuées déterminent de façon indépendante les logiciels et le matériel nécessaires à la vérification de l'authenticité et de l'exhaustivité des enregistrements de données de transaction, la création, l'entreposage et la vérification de l'exhaustivité des blocs de données.

Article 14. Logiciels et matériel utilisés par les utilisateurs

Les utilisateurs sont tenus de prendre leurs propres dispositions pour veiller à ce que les logiciels et le matériel utilisés dans les échanges électroniques transfrontières soient conformes aux exigences des prestataires de services de confiance.

Section VI. Services de confiance fournis dans le segment centralisé de l'environnement transfrontière de confiance

Article 15. Signature électronique

1. L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée.

2. Une signature électronique avancée satisfait aux exigences suivantes :

a) Être liée au signataire de manière univoque ;

b) Permettre d'identifier le signataire ;

c) Avoir été créée à l'aide de données de création de signature électronique que le signataire utilise sous son contrôle exclusif ;

d) Être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

3. Une signature électronique qualifiée est une signature électronique avancée qui repose sur un certificat qualifié de signature électronique et qui a été créée à l'aide de logiciels et de matériel certifiés conformément aux dispositions de l'article 8-6. L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite.

L'effet juridique d'une signature électronique avancée qui n'est pas une signature électronique qualifiée est équivalent à celui d'une signature manuscrite dans les cas convenus par les parties autorisant le recours à cette signature ou prévus dans la législation interne des États parties.

4. Une signature électronique qualifiée qui repose sur un certificat qualifié délivré dans le domaine de compétence d'un Membre est reconnue en tant que signature électronique qualifiée par tous les autres Membres.

Article 16. Cachet électronique

1. L'effet juridique et la recevabilité d'un cachet électronique comme preuve en justice ne peuvent être refusés au seul motif que ce cachet se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du cachet électronique qualifié.

2. Un cachet électronique avancé satisfait aux exigences suivantes :

a) Être lié au créateur du cachet de manière univoque ;

b) Permettre d'identifier le créateur du cachet ;

c) Avoir été créée à l'aide de données de création de cachet électronique que le créateur utilise sous son contrôle exclusif ;

d) Être lié aux données auxquelles il est associé de telle sorte que toute modification ultérieure des données soit détectable.

3. Un cachet électronique qualifié est un cachet électronique avancé qui repose sur un certificat qualifié de cachet électronique et qui a été créé à l'aide de logiciels et de matériel certifiés conformément aux dispositions de l'article 8-6. Un cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié.

Un cachet électronique avancé qui n'est pas un cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié dans les cas convenus par les parties autorisant le recours à ce cachet ou prévus dans la législation interne des États parties.

4. Un cachet électronique qualifié qui repose sur un certificat qualifié délivré dans le domaine de compétence d'un Membre est reconnu en tant que cachet électronique qualifié par tous les autres Membres.

Article 17. Horodatage électronique

1. L'effet juridique et la recevabilité d'un horodatage électronique comme preuve en justice ne peuvent être refusés au seul motif que cet horodatage se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences de l'horodatage électronique qualifié.

2. L'horodatage électronique qualifié crée une présomption d'exactitude quant à la date et l'heure précisée et d'intégrité des données, qui sont certifiées par l'horodatage électronique qualifié.

3. Un horodatage électronique qualifié satisfait aux exigences suivantes :

a) Lier la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données ;

b) Être fondé sur une horloge exacte liée au temps universel coordonné ;

c) Être signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié ayant satisfait à la procédure de conformité visée à l'article 8-6 du présent [projet d'instrument].

4. Un horodatage électronique qualifié délivré dans le domaine de compétence d'un Membre est reconnu en tant qu'horodatage électronique qualifié par tous les autres Membres.

Article 18. Service d'envoi recommandé électronique

1. L'effet juridique et la recevabilité des données envoyées et reçues à l'aide d'un service d'envoi recommandé électronique comme preuves en justice ne peuvent être refusés au seul motif que ce service se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du service d'envoi recommandé électronique qualifié.

2. Les données envoyées et reçues au moyen d'un service d'envoi recommandé électronique qualifié créent une présomption quant à l'intégrité des données, à l'envoi de ces données par un expéditeur identifié, à leur réception par un destinataire identifié, et à l'exactitude de la date et de l'heure de l'envoi et de la réception indiquées par le service d'envoi recommandé électronique qualifié.

3. Les services d'envoi recommandé électronique qualifiés satisfont aux exigences suivantes :

a) Être fournis par un ou plusieurs prestataires de services de confiance qualifiés ayant satisfait à la procédure de conformité prévue à l'article 8-6 du présent [projet d'instrument] ;

b) Garantir l'identification de l'expéditeur avec un degré de confiance élevé ;

c) Garantir l'identification du destinataire avant la fourniture des données ;

d) L'envoi et la réception de données sont sécurisés par une signature électronique avancée ou par un cachet électronique avancé d'un prestataire de services de confiance qualifié, de manière à exclure toute possibilité de modification indétectable des données ;

e) Toute modification des données nécessaire pour l'envoi ou la réception de celles-ci est clairement signalée à l'expéditeur et au destinataire des données ;

f) La date et l'heure d'envoi, de réception et toute modification des données sont indiquées par un horodatage électronique qualifié.

4. Les résultats de l'utilisation d'un service d'envoi recommandé électronique qualifié obtenus dans le domaine de compétence d'un Membre sont reconnus par tous les autres Membres comme les résultats de l'utilisation d'un service d'envoi recommandé électronique qualifié.

Article 19. Authentification de site Internet

1. Un certificat qualifié d'authentification de site Internet contient les renseignements suivants :

a) Une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié d'authentification de site Internet ;

b) Un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié ayant délivré le certificat qualifié ;

c) Pour les personnes physiques : au moins le nom de la personne à qui le certificat a été délivré, ou un pseudonyme ; pour les personnes morales : au moins le nom de la personne morale à laquelle le certificat est délivré et, le cas échéant, son numéro d'immatriculation, tels qu'ils figurent dans le registre officiel ;

d) Des éléments de l'adresse, dont au moins la ville et l'État, de la personne physique ou morale à laquelle le certificat est délivré et, le cas échéant, ces éléments tels qu'ils figurent dans les registres officiels ;

e) Le(s) nom(s) de domaine exploité(s) par la personne physique ou morale à laquelle le certificat est délivré ;

f) Des précisions sur le début et la fin de la période de validité du certificat ;

g) Le code d'identité du certificat, qui doit être unique pour le prestataire de services de confiance ;

h) La signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance délivrant le certificat ayant satisfait à la procédure de conformité visée à l'article 8-6 du présent [projet d'instrument] ;

i) L'emplacement des services de statut de validité des certificats qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié.

2. Les résultats de l'utilisation d'un service de confiance pour l'authentification de site Internet qui repose sur un certificat qualifié d'authentification de site Internet délivré dans le domaine de compétence d'un Membre est reconnu par tous les autres Membres comme les résultats de l'utilisation d'un service de confiance pour l'authentification de site Internet reposant sur un certificat qualifié d'authentification de site Internet.

Article 20. Autres services de confiance

1. Le Conseil de coordination pourrait inclure dans son champ de réglementation d'autres services de confiance non spécifiés aux articles 15 à 19 du présent [projet d'instrument].

2. Les règles applicables aux autres services de confiance devraient être analogues à celles applicables aux services de confiance mentionnés aux articles 15 à 19 du présent [projet d'instrument].

3. Afin de renforcer l'utilisation transfrontière des services de confiance, il devrait être possible de les utiliser comme éléments de preuve dans le cadre de procédures judiciaires dans tous les États parties. La législation interne doit préciser les effets juridiques des services de confiance, sauf disposition contraire dans le présent [projet d'instrument]

Article 21. Reconnaissance des services de confiance de pays tiers et d'organisations internationales

1. Les services de confiance fournis par des prestataires agréés conformément à la législation de pays tiers ou d'organisations internationales peuvent être reconnus comme équivalents, sur le plan juridique, à des services de confiance fournis par des prestataires ayant satisfait à la procédure de conformité prévue à l'article 8-6 du présent [projet d'instrument], à condition que le Conseil de coordination et un organisme agréé d'un pays tiers ou d'une organisation internationale en conviennent ainsi conformément au paragraphe 2 du présent article.

2. Les accords visées au paragraphe 1 du présent article prévoient notamment ce qui suit :

1) Les prescriptions imposées aux prestataires de services de confiance d'un pays tiers ou d'une organisation internationale ne sont pas inférieures à celles imposées aux prestataires de services de confiance qui fournissent des services de confiance conformément au présent [projet d'instrument] ;

2) Un pays tiers ou une organisation internationale partie à l'accord reconnaît dans son domaine de compétence l'équivalence juridique des services fournis par les prestataires de services de confiance ayant satisfait à la procédure de conformité prévue à l'article 8-6 du présent [projet d'instrument] et des services fournis par les

prestataires de services de confiance agréés conformément à la législation du pays tiers ou de l'organisation internationale ayant signé l'accord.

Section VII. Protection des droits et intérêts des participants aux échanges électroniques transfrontières

Article 22. Protection judiciaire

1. Les documents et les messages électroniques, y compris les résultats de l'utilisation de services de confiance décrits aux articles 15 à 20 du présent [projet d'instrument], sont acceptés comme éléments de preuve dans tous les tribunaux et tribunaux arbitraux des Membres.

2. Un droit légal certifié par un document électronique possède la même force exécutoire qu'un droit certifié par un document papier.

Article 23. Règlement des différends

1. Le Conseil de coordination adopte des règles pour le règlement administratif des différends découlant d'une interaction électronique transfrontière dans le segment centralisé de l'environnement transfrontière de confiance.

2. Les participants à une interaction électronique transfrontière ont le droit de conclure des accords bilatéraux et multilatéraux sur la procédure de règlement des différends découlant de l'interaction électronique transfrontière.