ORGANISATION MONDIALE DU COMMERCE

JOB/GC/115, JOB/CTG/3
JOB/SERV/247, JOB/IP/20
JOB/DEV/41

21 décembre 2016

(16-6995)

Original: anglais

Conseil général
Conseil du commerce des marchandises
Conseil du commerce des services
Conseil des aspects des droits de propriété intellectuelle qui touchent au commerce
Comité du commerce et du développement

PROGRAMME DE TRAVAIL SUR LE COMMERCE ÉLECTRONIQUE

SIGNATURE ÉLECTRONIQUE

Communication présentée par l'Argentine, le Brésil et le Paraguay

La communication ci-après, datée du 15 décembre 2016, est distribuée à la demande des délégations de l'Argentine, du Brésil et du Paraguay.

1.1 La signature électronique englobe un large éventail de solutions numériques visant à garantir l'authenticité, l'intégrité et la confidentialité des transactions et des communications intérieures et transfrontières effectuées en ligne. La signature électronique utilise des données électroniques pour vérifier l'identité de l'expéditeur d'un courriel ou de l'acheteur d'un service en ligne. Sous sa forme de base, elle ne nécessite pas d'être certifiée par une tierce partie officielle indépendante.

1.2 Dans sa version plus élaborée, la signature électronique, appelée signature électronique avancée ou signature numérique, est basée sur un fichier électronique (certificat numérique avancé) qui constitue une carte d'identité numérique complète, ce qui permet d'identifier de manière sûre et sans équivoque l'auteur d'un message électronique ou d'une transaction numérique. Le certificat numérique doit être délivré par une tierce partie de confiance – une autorité de certification officielle ou accréditée –, qui associera toute personne physique ou morale à une paire de clés cryptographiques. Non seulement il permet d'identifier clairement une personne sur le Web, mais il garantit aussi la validité juridique de toute action numérique qui l'utilise. Le certificat numérique est en train de devenir un outil fondamental pour le commerce électronique, les contrats électroniques, les opérations bancaires et les initiatives en matière d'administration électronique, entre autres usages. Par exemple, un certificat numérique associé à un courrier électronique garantit l'identité de l'expéditeur, l'intégrité du message et le fait que son contenu n'a pas été modifié de quelque manière que ce soit.

1.3 La question de la signature électronique et de l'authentification a déjà été identifiée comme une question pertinente dans le cadre des discussions menées au titre du Programme de travail sur le commerce électronique (documents JOB/GC/97/Rev.3 et JOB/GC/98).

1.4 Afin d'alimenter le débat, l'Argentine, le Brésil et le Paraguay souhaitent communiquer aux Membres la Résolution GMC n° 37/06, qui traite de cette question dans le cadre du MERCOSUR. Les coauteurs sont convaincus que la signature électronique sera un élément fondamental dans l'examen futur de toute question relative au commerce électronique à l'OMC.

MERCOSUR (Résolution GMC n° 37/06)

Article premier – Champ d'application

La présente résolution vise à reconnaître, sous réserve des conditions énoncées ci-après, la valeur juridique des documents électroniques, de la signature électronique et de la signature électronique avancée dans le cadre du MERCOSUR, et de contribuer ainsi à leur utilisation.

Les présentes dispositions ne s'appliquent pas aux autres aspects relatifs à la conclusion ou à la validité des instruments juridiques lorsque des prescriptions formelles sont établies dans la législation nationale, et elles n'affectent en rien les règles et les limites énoncées dans la législation nationale régissant l'utilisation de documents.

La présente résolution n'autorise pas la libre circulation des services de certification numérique au sein du MERCOSUR. Pour ce qui est de la prestation de services de certification numérique, les États Parties observeront les disciplines énoncées dans le Protocole de Montevideo sur le commerce des services dans le MERCOSUR et dans leurs listes d'engagements spécifiques.

Article 2 – Principes

Les États Parties observeront les principes suivants:

1. autonomie opérationnelle et coordination permanente entre les infrastructures nationales;

2. interopérabilité basée sur les normes internationales;

3. échange entre les États Parties, dans des conditions techniques sûres, de renseignements et de documents numériques ayant une validité juridique et une valeur probante;

4. transparence dans la gestion de la certification numérique;

5. traitement neutre, par les lois nationales, des différentes technologies utilisées pour les activités prévues dans la présente résolution afin de permettre l'adaptation au rythme du développement technologique inhérent à ces activités (neutralité technologique);

6. interprétation fonctionnelle des termes et concepts pour faire en sorte qu'un processus ou une technologie utilisé(e) par un État Partie ne soit pas privé d'effet juridique du seul fait qu'il lui a été attribué une nomenclature différente de celle qui figure dans la présente résolution.

Article 3 – Définitions

Aux fins de la présente résolution:

1) L'expression **"signature électronique"** s'entend des données sous forme électronique qui sont jointes ou logiquement associées à d'autres données électroniques et qui sont utilisées par le signataire comme moyen d'identification.

2) L'expression **"signature électronique avancée"** s'entend d'une signature électronique qui satisfait aux exigences suivantes:

   a) elle nécessite des renseignements que le signataire est seul à connaître, afin de permettre son identification;

   b) elle est créée par des moyens que le signataire peut garder sous son contrôle exclusif;

   c) elle est vérifiable par des tierces parties;

   d) elle est liée aux données signées de façon à ce que toute modification ultérieure des données soit détectable; et

e) elle est créée au moyen d'un dispositif de création de signatures techniquement sûr et fiable, et elle est basée sur un certificat qui est qualifié et valide au moment de la signature.

3) L'expression **"signature numérique"** s'emploie de manière interchangeable avec l'expression "signature électronique avancée".

4) Le terme **"signataire"** s'entend d'une personne physique ou morale qui utilise légalement un dispositif de création de signatures électroniques.

5) L'expression **"document électronique"** s'entend de la représentation numérique d'actes ou de faits, quel que soit le support sur lequel ils sont fixés enregistrés ou archivés.

6) L'expression **"document numérique"** s'emploie de manière interchangeable avec l'expression "document électronique".

7) L'expression **"certificat numérique"** s'entend d'un document électronique signé numériquement qui lie les données de vérification de la signature au signataire et qui confirme l'identité de ce dernier.

8) L'expression **"certificat qualifié"** s'entend d'un certificat numérique délivré par un prestataire de services accrédité qui satisfait aux exigences énoncées dans la législation nationale.

9) L'expression **"certificat avancé"** s'emploie de manière interchangeable avec l'expression "certificat qualifié".

10) L'expression **"prestataire de services de certification"** s'entend d'une personne physique ou morale qui, conformément à la législation nationale, délivre des certificats ou fournit d'autres services en rapport avec la signature électronique.

Article 4 – Effets juridiques des documents électroniques et des signatures électroniques

Les États Parties reconnaissent que les documents électroniques satisfont aux exigences applicables aux manuscrits. En conséquence, dans chaque État Partie, les documents électroniques auront les mêmes effets juridiques que les documents écrits, sous réserve des exceptions prévues dans la législation nationale.

Les États Parties reconnaîtront les effets juridiques des signatures électroniques quand celles-ci sont reconnues comme valables par les Parties qui les utilisent ou sont acceptées par le destinataire du document auquel elles sont liées.

Les États Parties feront en sorte que la valeur probante d'un document électronique ne soit pas niée du seul fait qu'il n'est pas lié à une signature électronique avancée, si l'authenticité et l'intégrité du document en question peuvent être démontrées sans équivoque.

Les Parties seront libres de convenir mutuellement des conditions dans lesquelles elles accepteront les signatures électroniques, conformément à leur législation nationale.

Dans le cas où l'une des Parties ne reconnaît pas une signature électronique, il appartiendra à l'autre Partie de prouver la validité de cette signature.

Article 5 – Signature électronique avancée: reconnaissance mutuelle

Afin d'assurer la reconnaissance mutuelle des signatures électroniques avancées et des certificats numériques, les États Parties pourront conclure entre eux des accords de reconnaissance mutuelle. Le Groupe du marché commun (GMC) adoptera des lignes directrices à cette fin. Ces lignes directrices refléteront la situation existant au moment de leur adoption et pourront être actualisées sur proposition du Sous-groupe de travail (SGT) n° 13, pour tenir compte des évolutions technologiques.

Dans le cadre des accords de reconnaissance mutuelle, les signatures électroniques avancées qui satisfont aux conditions énoncées dans ces accords auront la même valeur juridique et la même valeur probante que les signatures manuscrites.

Les États Parties reconnaîtront l'authenticité et l'intégrité d'un document électronique signé au moyen d'une signature électronique avancée et accepteront ce document comme preuve documentaire devant les tribunaux, conformément aux dispositions des accords de reconnaissance mutuelle.

Dans le cadre du SGT n° 13, les États Parties indiqueront quels organismes sont habilités à signer les accords de reconnaissance mutuelle.

Article 6 – Certificats numériques qualifiés

Les accords de reconnaissance mutuelle définiront les conditions dans lesquelles les certificats numériques délivrés par un État Partie à l'accord auront la même validité juridique dans les autres États Parties audit accord.

Ces conditions devront exiger, au moins, que les certificats numériques:

a) soient délivrés par un prestataire de services de certification accrédité conformément au système national d'accréditation et de contrôle prévu à l'article 7;

b) soient conformes aux formats normalisés internationalement reconnus, établis par l'autorité de mise en œuvre de chaque État Partie;

c) satisfassent aux critères minimaux énoncés dans les lignes directrices mentionnées à l'article 5;

d) contiennent, au moins, les données nécessaires pour:

   1. identifier de manière indubitable le titulaire et le prestataire de services de certification qui a délivré le certificat, en indiquant sa durée de validité et les données permettant l'identification unique du titulaire et du prestataire;

   2. vérifier leur état de révocation;

   3. distinguer clairement les renseignements vérifiés et les renseignements non vérifiés figurant dans le certificat numérique;

   4. pouvoir vérifier la signature;

   5. identifier la politique de certification en vertu de laquelle le certificat a été délivré.

Article 7 – Prestation de services de certification

Les États Parties ne soumettront pas à une accréditation préalable la prestation de services de certification, sauf dans le cas des services liés à une signature électronique avancée, conformément aux dispositions de la présente résolution.

Les États Parties créeront un système approprié d'accréditation et de contrôle des prestataires de services de certification établis sur leur territoire qui délivrent des certificats qualifiés permettant la vérification des signatures électroniques avancées.

Les États Parties pourront soumettre l'utilisation de la signature électronique et de la signature électronique avancée dans le secteur public à des prescriptions supplémentaires. Ces prescriptions seront objectives, transparentes, proportionnées et non discriminatoires, et se rapporteront uniquement aux caractéristiques spécifiques de l'application concernée. Elles ne constitueront pas un obstacle aux services transfrontières.

Article 8 – Responsabilité

Les États Parties feront , au moins, en sorte qu'un prestataire de services de certification accrédité conformément à l'article 7 soit responsable des dommages causés à une personne physique ou morale qui avait raisonnablement confiance dans le certificat numérique délivré par ledit prestataire eu égard à ce qui suit:

a) tous les champs et renseignements requis par les infrastructures nationales respectives sont inclus dans le certificat qualifié et sont exacts au moment de sa délivrance;

b) au moment où le certificat qualifié est délivré par le prestataire de services de certification accrédité, la signature identifiée dans ledit certificat reflète les données de création de signature correspondant aux données de vérification contenues dans le certificat qualifié du prestataire, afin de garantir la chaîne de confiance;

c) toute erreur ou omission dans les certificats qualifiés délivrés ou le non-respect des procédures de certification établies dans les accords de reconnaissance mutuelle;

d) l'enregistrement en bonne et due forme et en temps voulu de la révocation des certificats qualifiés délivrés, le cas échéant.

Il appartient au prestataire de services de certification accrédité de démontrer qu'il n'a pas agi par négligence ou intentionnellement.

Les États Parties feront en sorte que le prestataire de services de certification accrédité conformément à l'article 7 indique dans un certificat qualifié les limites de son utilisation, d'une manière identifiable par des tiers.

Le prestataire de services de certification accrédité conformément à l'article 7 ne sera pas tenu pour responsable d'un dommage résultant de l'utilisation d'un certificat qualifié qu'il a délivré si ladite utilisation sort du champ défini dans sa politique de certification. Il ne sera pas non plus tenu pour responsable des éventuelles inexactitudes dans le certificat qualifié, résultant des renseignements vérifiés fournis par le titulaire, à condition que le prestataire puisse démontrer qu'il a respecté toutes les conditions énoncées dans ses politiques et procédures de certification.

Article 9 – Protection des données personnelles

Les États Parties feront en sorte qu'un prestataire de services de certification qui délivre au public des certificats qualifiés puisse seulement recueillir des données personnelles directement auprès de la personne à laquelle ses données se rapportent, après avoir obtenu le consentement exprès de cette personne et uniquement dans la mesure où ces données sont nécessaires pour délivrer et maintenir le certificat. Les données ne seront pas obtenues ou utilisées à d'autres fins sans le consentement exprès du titulaire.

Les États Parties garantiront la confidentialité des autres données personnelles requises pour la délivrance du certificat qualifié qui ne figurent pas dans ce dernier, conformément aux dispositions du présent article.

_____