

**Conseil économique et social**

Distr. générale
25 janvier 2016
Français
Original : anglais

Commission économique pour l'Europe**Comité des transports intérieurs****Groupe de travail des problèmes douaniers
intéressant les transports****Groupe d'experts des aspects juridiques
de l'informatisation du régime TIR****Deuxième session**

Genève, 4 et 5 avril 2016

Point 4 de l'ordre du jour provisoire

**Compatibilité du cadre juridique du système eTIR
avec les dispositions juridiques nationales****Résultats des enquêtes menées par le Groupe spécial
informel d'experts des aspects théoriques et
techniques de l'informatisation du régime TIR****Note du secrétariat****I. Généralités**

1. À sa précédente session, le Groupe d'experts des aspects juridiques de l'informatisation du régime TIR a commencé d'examiner la question de savoir si les dispositions juridiques nationales de certains pays étaient compatibles avec les dispositions juridiques régissant la mise en place du système eTIR. À ce propos, il se rappellera peut-être que la délégation de la Fédération de Russie l'avait informé que la proposition actuelle de reconnaissance mutuelle des authentications effectuées dans le pays d'origine n'était pas compatible avec la législation de son pays. Dans ce contexte, il avait conclu qu'il serait peut-être justifié de mener une enquête pour obtenir des informations pertinentes à ce sujet auprès de toutes les Parties contractantes à la Convention TIR (voir ECE/TRANS/WP.30.GE.2/2, par. 8 a)). Dans un premier temps, il a demandé au secrétariat de communiquer à la session en cours les résultats des enquêtes pertinentes déjà réalisées, dans le cadre du projet eTIR, par le Groupe spécial informel d'experts des aspects théoriques et techniques de l'informatisation du régime TIR, afin de définir les prochaines étapes à suivre. Conformément à cette demande, le secrétariat a établi le présent résumé des résultats des enquêtes menées par le Groupe spécial informel d'experts.



II. Enquêtes du Groupe spécial informel d'experts des aspects théoriques et techniques de l'informatisation du régime TIR

2. À sa sixième session (octobre 2004), le Groupe d'experts s'était félicité d'une proposition du secrétariat d'entreprendre une étude visant à recueillir auprès des administrations douanières des informations sur les systèmes existants, ainsi que sur leurs besoins et leurs problèmes en ce qui concernait le système eTIR. À cette fin, le secrétariat a élaboré un questionnaire qui a été envoyé au directeur généraux des douanes (avec copie aux points de contact douaniers TIR). À sa septième session (mai 2005), le Groupe d'experts a utilisé les résultats préliminaires du questionnaire, figurant dans le document ExG/COMP/2005/3, pour finaliser le premier chapitre du modèle de référence eTIR et évaluer les besoins futurs du projet eTIR. Il a également demandé au secrétariat de continuer de demander aux pays qui n'avaient pas encore répondu au questionnaire, en particulier aux pays n'appartenant pas à l'Union européenne, de bien vouloir le faire. À sa huitième session (novembre 2005), le Groupe a pris note des dernières réponses au questionnaire eTIR, figurant dans le document TRANS/WP.30/GE.1/2005/4, et s'est félicité à l'idée de recevoir, à sa neuvième session, des résultats actualisés, notamment la réponse de la Fédération de Russie, éventuellement accompagnée des réponses d'autres pays que le secrétariat aurait reçues avant la mi-février 2006. Les résultats définitifs de l'enquête, publiés sous la cote ECE/TRANS/WP.30/GE.1/2006/2, ont été utilisés par le Groupe d'experts dans les chapitres 1.1.7 et 1.1.8 du modèle de référence eTIR.

3. À sa dix-neuvième session (septembre 2011), le Groupe d'experts a réexaminé la proposition visant à prévoir, dans le cadre du projet eTIR, des mécanismes de déclaration au niveau international, sur la base du document ECE/TRANS/WP.30/GE.1/2011/9, établi par le secrétariat en collaboration avec des experts des douanes de la République tchèque. Tout en soulignant l'absence d'accords internationaux mondiaux sur les signatures électroniques, le Groupe d'experts a pris note du fait que certains pays imposaient de recourir aux autorités nationales de certification quand il s'agissait de signer des documents électroniques destinés à des organismes publics. Il a estimé qu'il ne disposait pas d'assez de renseignements pour prendre une décision sur la question et demandé au secrétariat d'entreprendre une enquête auprès des points de contact TIR et eTIR pour recueillir des informations de la part de toutes les Parties contractantes à la Convention TIR sur les pratiques, règles et réglementations actuelles et prévues en matière de signatures électroniques (ECE/TRANS/WP.30/2012/1, par. 10). L'enquête s'est déroulée en mars 2012 et ses résultats, qui figuraient initialement dans le document informel n° 3 du Groupe d'experts (2012), sont présentés à l'annexe.

4. À sa vingtième session (avril 2012), le Groupe d'experts a conclu que l'enquête sur l'utilisation des signatures électroniques dans le cadre du projet eTIR confirmait que la plupart des pays exigeaient l'utilisation de signatures électroniques ou d'autres mécanismes d'authentification pour la communication d'informations anticipées sur les marchandises. Dans la plupart des pays, seules les signatures électroniques nationales (ou, dans les meilleurs cas, régionales) étaient acceptées et seul un petit nombre de pays reconnaissaient les autorités étrangères de certification pour la délivrance de signatures électroniques ayant force de loi. Le Groupe d'experts a confirmé que tant qu'il n'y aurait pas d'autorité de certification reconnue au niveau international, il serait extrêmement difficile de mettre en place un mécanisme d'utilisation transfrontière de documents signés électroniquement. Il a noté que 50 % des répondants avaient indiqué qu'une autorité internationale de certification pourrait être utilisée si elle était reconnue par un accord international, et que la moitié d'entre eux estimaient que l'on pourrait considérer que la Convention TIR pouvait être

utilisée à cette fin. En conséquence, le secrétariat a été prié de continuer à étudier la possibilité d'adopter des mécanismes de déclaration au niveau international, par exemple en faisant appel à des tiers de confiance ou directement dans le régime international eTIR, éventuellement en liaison avec la procédure d'autorisation des titulaires de carnets TIR. Enfin, le Groupe d'experts a prié le secrétariat de rédiger, pour sa prochaine réunion, une nouvelle version du modèle de référence eTIR afin d'y faire figurer divers mécanismes de déclaration au niveau international, en insistant sur le fait qu'une proposition réaliste devait être fondée sur des mécanismes d'authentification (par exemple nom d'utilisateur/mot de passe) et des mécanismes d'échanges d'informations entre systèmes sûrs (par exemple des réseaux privés virtuels), plutôt que sur des signatures électroniques (ECE/TRANS/WP.30/2012/7, par. 10).

III. Examen par le Groupe d'experts

5. Le Groupe d'experts des aspects juridiques de l'informatisation du régime TIR voudra peut-être examiner le présent document et déterminer s'il convient de mener une nouvelle enquête.

Annexe

Résultats de l'enquête sur l'utilisation des signatures électroniques dans le cadre du projet eTIR

I. Répondants

3. Le 10 avril 2012, les 30 pays ci-après avaient répondu au questionnaire :

Allemagne, Autriche, Belgique, Bulgarie, Chypre, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Italie, Lettonie, Lituanie, Monténégro, Mongolie, Norvège, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Serbie, Slovaquie, Slovénie, Suède, Turquie, Ukraine.

II. Synthèse des réponses à l'enquête

Question 1 : *Considérant que, dans le futur système eTIR, la déclaration en douane sera déposée et acceptée au moment où le titulaire (ou son représentant) présentera à la douane les marchandises, le véhicule et une référence aux informations anticipées sur les marchandises, estimez-vous qu'il est nécessaire, au moment de la soumission électronique des informations anticipées sur les marchandises, que le titulaire s'authentifie à l'aide d'une signature électronique ou de tout autre type de mécanisme d'authentification.*

Oui : 27 (90 %)

Allemagne, Autriche, Belgique, Bulgarie, Danemark, Espagne, Estonie, France, Grèce, Hongrie, Italie, Lettonie, Lituanie, Mongolie, Monténégro, Norvège, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Turquie, Ukraine

Non : 2 (7 %)

Finlande, Serbie

Pas de réponse : 1 (3 %)

Chypre

Question 2 : *Dans votre pays, les autorités douanières disposent-elles déjà d'un mécanisme juridique pour l'authentification de l'utilisateur ou l'utilisation des signatures électroniques?*

Oui : 25 (83 %)

Allemagne, Belgique, Bulgarie, Chypre, Danemark, Espagne, Estonie, Finlande, France, Hongrie, Italie, Lettonie, Lituanie, Monténégro, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Serbie, Slovaquie, Slovénie, Suède, Turquie, Ukraine

Non : 5 (17 %)

Autriche, Grèce, Mongolie, Norvège, Royaume-Uni

Sinon, savez-vous s'il est prévu dans votre pays de mettre en place, dans un proche avenir, un mécanisme de signatures électroniques ou tout autre type de mécanisme d'authentification à des fins douanières?

Oui : 3 (60 %)

Grèce, Mongolie, Royaume-Uni

Non : 2 (40 %)

Autriche, Norvège

Question 3 : Dans votre pays, les autorités douanières acceptent-elles l'utilisation de signatures certifiées par des autorités de certification étrangères?

Oui : 7 (24 %)

Belgique, Estonie, Lituanie, Portugal, République tchèque, Serbie, Turquie

Non : 22 (76 %)

Allemagne, Autriche, Bulgarie, Danemark, Espagne, Finlande, France, Grèce, Hongrie, Italie, Lettonie, Mongolie, Monténégro, Norvège, Pays-Bas, Pologne, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Ukraine

Sinon, savez-vous s'il est prévu, éventuellement, de modifier la situation dans un proche avenir?

Oui : 7 (33 %)

Bulgarie, Grèce, Italie, Mongolie, Monténégro, Pologne, Turquie

Non : 9 (43 %)

Allemagne, Autriche, Espagne, Lettonie, Norvège, Roumanie, Royaume-Uni, Slovénie, Ukraine

Sans objet : 5 (24 %)

Finlande, France, Hongrie, Slovaquie, Suède

Question 4 : Selon vous, serait-il possible qu'à l'avenir les autorités douanières de votre pays puissent accepter des signatures électroniques, si celles-ci étaient émises ou certifiées par une autorité de certification internationalement reconnue (à savoir une autorité de certification qui serait reconnue par un instrument juridique international, comme la Convention TIR)?

Oui : 15 (52 %)

Belgique, Estonie, Finlande, Grèce, Hongrie, Lituanie, Mongolie, Monténégro, Pologne, République tchèque, Serbie, Slovaquie, Slovénie, Suède, Turquie

Non : 3 (10 %)

Espagne, Italie, Ukraine

Pas de réponse/sans objet : 11 (38 %)

Allemagne, Autriche, Bulgarie, Chypre, Danemark, France, Lettonie, Pays-Bas, Norvège, Roumanie, Royaume-Uni

Dans l'affirmative, votre gouvernement souhaiterait-il que cette autorité de certification soit établie dans le cadre juridique de la Convention TIR?

Oui : 8 (53 %)

Finlande, Lituanie, Monténégro, Pologne, Serbie, Slovaquie, Slovénie, Turquie

Non : 3 (20 %)

Belgique, Mongolie, Suède

Pas de réponse/sans objet : 4 (27 %)

Estonie, Grèce, Hongrie, République tchèque

IV. Examen préliminaire par le secrétariat

Question 1 :

La plupart des répondants estiment qu'il est nécessaire que le titulaire s'authentifie au moment de la présentation des informations anticipées sur les marchandises. Certaines réponses renvoient à la législation européenne en vigueur et à l'application du Nouveau système de transit informatisé (NSTI), d'autres, à la législation nationale applicable. De l'avis général, l'authentification est nécessaire pour prévenir l'utilisation frauduleuse soit de l'identité du titulaire du carnet TIR, soit du carnet TIR. Comme c'est le cas de la signature dans le système sur papier, une authentification en bonne et due forme rend le titulaire responsable des données présentées dans le carnet TIR et engage entièrement sa responsabilité en ce qui concerne l'utilisation du régime TIR, y compris le paiement de la dette douanière en cas d'infraction.

Question 2 :

La plupart des pays disposent déjà, sous une forme ou une autre, de textes de loi nationaux précisant les conditions auxquelles doivent répondre les mécanismes d'authentification ou l'utilisation des signatures électroniques. Sur les cinq pays où cela n'est pas encore le cas, trois font savoir que l'adoption d'une telle législation est à l'étude.

Question 3 :

Seuls sept pays indiquent qu'ils reconnaissent les signatures électroniques certifiées par des autorités de certification étrangères. Les vingt-huit autres pays font observer qu'ils ne reconnaissent pas les signatures électroniques étrangères sauf, pour certains, si elles ont fait l'objet d'un enregistrement préalable auprès de leur système national.

Question 4 :

Quatorze pays font valoir qu'ils pourraient se prononcer en faveur de l'existence d'une certaine forme d'autorité de certification reconnue à l'échelle internationale, mais indiquent, dans le même temps, qu'un engagement plus ferme à cet égard devrait nécessairement s'appuyer sur une coordination plus étroite au niveau des gouvernements nationaux. Sept pays font savoir qu'ils souhaiteraient soutenir une telle évolution dans le cadre de la Convention TIR.

Appendice

A. Réponses par pays¹

Question 1 : Considérant que, dans le futur système eTIR, la déclaration en douane sera déposée et acceptée au moment où le titulaire (ou son représentant) présentera à la douane les marchandises, le véhicule et une référence aux informations anticipées sur les marchandises, estimez-vous qu'il est nécessaire, au moment de la soumission électronique des informations anticipées sur les marchandises, que le titulaire s'authentifie à l'aide d'une signature électronique ou de tout autre type de mécanisme d'authentification.

Danemark : Nous traitons les déclarations de transit (y compris les déclarations TIR) dans le NSTI. Les communications avec les commerçants se font par le biais du NSTI au moyen de déclarations adressées en format EDIFACT (Échange de données informatisé pour l'administration, le commerce et le transport).

Estonie : L'Estonie estime qu'il est nécessaire que le titulaire du carnet TIR s'authentifie au moment de la soumission électronique des informations anticipées sur les marchandises. Le représentant du titulaire du carnet TIR devait s'authentifier en tant que personne physique en accédant au système électronique de l'Administration fiscale et douanière estonienne à l'aide d'une pièce d'identité ou d'une carte d'identité numérique. Il n'est pas prévu dans un proche avenir de mettre en place un mécanisme d'authentification fondé sur les signatures électroniques.

Allemagne : Sur papier, le titulaire s'authentifie avec sa signature. Aussi, dans un environnement électronique, doit-il s'authentifier au moyen d'une signature électronique ou d'un autre mécanisme analogue.

Finlande : Il devrait appartenir à chaque Partie Contractante de procéder à une analyse des risques également pour les prédéclarations [= informations anticipées sur les marchandises], lesquelles ne seront jamais communiquées aux fins du transit. Ainsi, il pourrait être inapproprié d'identifier le titulaire à parti de la prédéclaration puisqu'effectivement celle-ci ne sera jamais communiquée aux fins du transit. En tout état de cause, le titulaire sera identifié lors du traitement de la déclaration de transit au bureau de douane. Le même principe vaut pour le régime commun de transit dans la Communauté européenne, bien que la pratique puisse varier selon les pays de l'UE.

France : Même si le projet eTIR prévoit que la déclaration ne sera considérée comme acceptée qu'au moment où le titulaire (ou son représentant) présentera à la douane les marchandises, le véhicule et une référence aux informations anticipées sur les marchandises, nous devons vérifier si un personne (physique) qui veut utiliser un carnet TIR en tant que déclaration en douane et qui dit représenter une entreprise, est effectivement autorisé à agir au nom du titulaire du carnet TIR. Plus précisément, le mécanisme d'authentification vise à empêcher l'utilisation frauduleuse de l'identité d'un titulaire ou du numéro du carnet TIR par un utilisateur auquel le titulaire ou son représentant n'a pas autorisé l'accès.

D'autre part, si une déclaration pouvait être déposée par une personne quelconque, sans aucune authentification, il semblerait alors possible que quelqu'un puisse déposer une déclaration, présenter le véhicule, les marchandises et la référence à la déclaration à un bureau de douane et effectuer un transport en utilisant le numéro d'identification d'un autre titulaire de carnet TIR ou la garantie TIR d'une autre société. La vérification de la concordance entre la déclaration et le véhicule ou le conducteur ne serait possible au bureau de douane que si la relation entre le titulaire,

¹ Les communications ont été revues par le secrétariat par souci de clarté et de cohérence.

le conducteur et le véhicule était bien établie, ce qui n'est pas toujours le cas, en particulier lorsqu'il y a sous-traitance.

Hongrie : La Hongrie considère que l'authentification ou l'identification d'un titulaire est essentielle et nécessaire lors de la transmission des données électroniques sur les marchandises, en particulier lorsque le carnet TIR est acceptée par les autorités douanières. Premièrement, le titulaire est responsable de toutes les données figurant dans le carnet TIR. Deuxièmement, le titulaire sera connu au moyen de l'identification ou sous réserve que son identité puisse être confirmée. Enfin et surtout, le titulaire est également responsable de l'opération TIR en ce qui concerne d'autres questions telles que les délais, l'itinéraire prescrit ou la dette douanière.

Italie : L'authentification du titulaire du carnet TIR est considérée comme une étape obligatoire dans la perspective d'un environnement dématérialisé.

Lettonie : En Lettonie, toute personne qui soumet une déclaration de transit TIR doit être enregistrée en tant qu'utilisateur auprès du système de déclaration nationale. Le titulaire se voit attribuer un nom d'utilisateur et un mot de passe qui lui permettent de s'authentifier. En dehors de cela, il n'existe pas d'autre moyen de soumettre des déclarations dans le pays. Le système national pourrait être relié à d'autres systèmes, y compris ceux d'autres pays. Dans ce cas, le commerçant ou l'organisme signe un accord avec l'Administration fiscale de la Lettonie concernant l'utilisation des signatures électroniques ainsi qu'un accord sur la présentation des carnets TIR électroniques au mécanisme de contrôle du transit et il obtient son nom d'utilisateur et son mot de passe. L'organisme pourrait partager ses données avec les utilisateurs de son système.

Lituanie : Règlement (CEE) n° 2454/93 de la Commission fixant certaines dispositions d'application du règlement (CEE) n° 2913/92 du Conseil établissant le code des douanes communautaire, article 184a (en cas de transport routier, la déclaration sommaire d'entrée est déposée au bureau de douane d'entrée au moins une heure avant l'arrivée au bureau de douane d'entrée dans le territoire douanier de la Communauté).

Mongolie : L'utilisation d'une signature électronique est exigée du fait de l'existence du Guichet électronique national unique.

Pays-Bas : Les douanes doivent connaître la personne qui utilise leur système de déclaration électronique et, par conséquent, l'authentification du déclarant est nécessaire.

Norvège : Notre système électronique national accepte uniquement les utilisateurs préenregistrés. Les réponses et messages sont renvoyés à une adresse centralement enregistrée.

Pologne : La Pologne estime que même si les données transmises par voie électronique sont considérés comme des « informations anticipées sur les marchandises » et non comme des « déclaration en douane », l'authentification du titulaire demeure nécessaire. Dans le régime du transit communautaire, il n'y a pas de distinction entre les deux : le message envoyé (IE15) est en fait considéré comme une déclaration en douane, même s'il n'est accepté qu'après la présentation des marchandises, avec la référence au document électronique.

Portugal : Toute personne, qu'il s'agisse du titulaire ou de son représentant, doit être dûment authentifiée et reconnue comme telle.

Serbie : La Serbie estime que l'authentification n'est pas nécessaire pour la présentation de la déclaration de chargement préalable. Une telle approche exigerait que soit accepté un grand nombre de certificats numériques délivrés par de nombreuses autorités de certification (ou entreprises) dans le monde entier. En outre,

cela pourrait compliquer la tâche du titulaire car il devrait probablement avoir en sa possession des dispositifs appropriés (jetons, cartes, lecteurs, etc.) qu'il lui faudrait bien sûr d'abord acheter.

Espagne : L'Espagne est d'avis que les systèmes de signature électronique sont nécessaires pour des raisons de sécurité.

Suède : les douanes suédoises ont adopté un mécanisme de sécurité fondé sur l'infrastructure à clef publique.

Turquie : En général, les carnets TIR sont présentés par les conducteurs aux bureaux des douanes, étant entendu que le titulaire ou son représentant ne sont pas physiquement présents sur les lieux. C'est pourquoi les carnets TIR sont signés par les conducteurs, bien qu'ils n'y soient pas autorisés. Si une signature électronique est utilisée, les carnets TIR peuvent être signés par le titulaire autorisé ou son représentant. Il importe également de savoir qui présente la déclaration et qui est responsable.

Ukraine : L'utilisation d'une signature électronique permet d'identifier clairement le document sous forme de document électronique ainsi que la personne qui a signé ce document électronique.

Royaume-Uni : Le système devrait pouvoir vérifier tous les messages et procéder à une vérification à rebours pour déterminer qui les a déposés.

Question 2 : Dans votre pays, les autorités douanières disposent-elles déjà d'un mécanisme juridique pour l'authentification de l'utilisateur ou l'utilisation des signatures électroniques? Sinon, savez-vous s'il est prévu de mettre en place, dans un proche avenir, un mécanisme de signatures électroniques ou tout autre type de mécanisme d'authentification à des fins douanières?

Danemark : Les citoyens et les entreprises du Danemark ont recours depuis des années à des services en ligne, y compris aux signatures électroniques, mais leur potentiel n'est pas encore complètement exploité.

Actuellement, le Gouvernement travaille sur une stratégie de cyberadministration pour les années 2011-2015. De plus en plus de procédures dans le secteur public seront automatisées et numérisées. Toutes les entreprises obtiendront une boîte à lettres numérique et seront autorisées à accéder aux informations des sociétés sur le portail de celles-ci. Le système de signatures électroniques, dénommé NemID, permet à tous les citoyens de se connecter et de communiquer électroniquement avec toutes les administrations publiques, les banques, etc. Il se fonde sur des registres personnels. En conséquence, des difficultés surgissent quand des entreprises étrangères ne sont pas enregistrées. Normalement, les entreprises peuvent être enregistrées par un représentant au Danemark. Pour qu'une entité (personne ou société) puisse acquérir les mêmes droits, il faudrait alors utiliser des certificats établis selon la norme X509. Ainsi, théoriquement, une telle procédure devrait être possible.

France : Les autorités douanières ont déjà mis en place un mécanisme juridique pour l'authentification des utilisateurs, mais il ne repose pas sur l'utilisation de signatures électroniques. En fait, lorsque des mécanismes de déclaration ont été élaborés, la possibilité d'utiliser des signatures électroniques a été évaluée et il a été conclu que l'utilisation de certificats électroniques pourrait représenter une très lourde charge pour les commerçants. Différents éléments justifient cette conclusion, non seulement les coûts financiers liés à l'achat de certificats, mais aussi la complexité de la gestion des certificats (nécessité pour chaque utilisateur d'une société d'obtenir un certificat distinct, etc.). En outre, la France a estimé qu'il était possible d'assurer l'authentification et de sécuriser l'accès au système par d'autres moyens, plus simples.

Tout d'abord, il convient de souligner qu'en France la plupart des déclarations en douane électroniques sont déposées dans l'EDI; dans ce cas, un échange entre systèmes intervient (chaque système reconnaît son partenaire) et aucune autre authentification, hormis l'authentification technique, n'est nécessaire. Dans le DTI, le processus d'authentification est pris en compte dans le portail des douanes: l'utilisateur est authentifié par son nom d'utilisateur et son mot de passe (qu'il choisit lui-même lors de l'inscription). Pour les applications douanières touchant à des questions plus sensibles, des exigences de sécurité plus strictes peuvent être ajoutées (l'inscription peut être « confirmée » par un dirigeant de la société). En outre, la plupart du temps, dans le DTI les droits de l'utilisateur sont attribués par les douanes, à la demande de la société, ce qui contribue à sécuriser le mécanisme de déclaration.

Grèce : Une équipe a été chargée d'étudier la possibilité d'adopter un mécanisme de signature électronique pour les douanes.

Pologne : Actuellement, la Pologne n'utilise pas le Nouveau système de transit informatisé (NSTI). Une vérification du déclarant est effectuée sur la base de l'adresse électronique et du numéro d'enregistrement et d'identification des opérateurs économiques (EORI); le déclarant doit être enregistré dans la base de données de référence pertinentes. S'agissant des autres procédures (importation, exportation), la Pologne a mis en place un mécanisme dénommé « clef pour la transmission sécurisée des données »; cette clef est délivrée/fournie par un service désigné au sein de l'Administration des douanes polonaises (Centre de transmission de données sécurisé).

Question 3 : Dans votre pays, les autorités douanières acceptent-elles l'utilisation de signatures certifiées par des autorités de certification étrangères? Sinon, savez-vous s'il est prévu, éventuellement, de modifier la situation dans un proche avenir?

République tchèque : Les autorités douanières acceptent l'utilisation de signatures certifiées par des autorités de certification étrangères. Cependant, étant donné que la méthode de certification de l'autorité de certification étrangère peut être différente de ce que prescrit la loi tchèque, l'acceptation de la signature est subordonnée à une évaluation au cas par cas.

Estonie : L'Administration fiscale et douanière estonienne ne peut accepter des signatures électroniques que des autorités de certification approuvées par l'Administration estonienne des systèmes d'information, laquelle coordonne la mise en place et la gestion des systèmes d'information nationaux, y compris l'infrastructure à clef publique, afin de permettre une authentification et des signatures numérique sécurisées.

France : Pas de réponse définitive (ni oui, ni non), car les signatures électroniques fondées sur des certificats électroniques ne sont pas utilisés par les douanes françaises dans le cadre des procédures douanières en ligne. Toutefois, si cela devait être le cas, on peut supposer que les certificats délivrés par des autorités de certification étrangères pourraient être acceptés, comme c'est le cas aujourd'hui pour les certificats utilisés à d'autres fins (certificats pour les serveurs, le cryptage de documents, etc. lorsque des certificats délivrés par des autorités étrangères peuvent être utilisés).

Monténégro : Récemment, un organe national agréé a été créé afin d'attribuer des clefs locales pour la soumission électronique de documents. Actuellement, il ne semble pas que des relations aient été établies entre notre pays et des organismes de certification étrangers, mais on pourrait envisager favorablement une telle éventualité.

Pays-Bas : Les Pays-Bas n'acceptent pas les signatures électroniques certifiées par des autorités de certification étrangères et n'envisagent pas de changement de la situation dans un proche avenir.

Pologne : Nous allons accepter les signatures/certificats électroniques émis par les autorités de certification de tous les autres États membres de l'UE, en se fondant sur ce qu'il est convenu d'appeler la Liste du statut des services de confiance, en application de la décision de la Commission européenne 2009/767/CE du 16 octobre 2009 établissant des mesures destinées à faciliter l'exécution de procédures par voie électronique par l'intermédiaire des « guichets uniques » conformément à la directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur. Une restriction : les certificats ainsi que les formats de signature devraient être conformes à un ensemble de spécifications techniques.

Roumanie : Selon la loi en vigueur, seules sont acceptées les signatures électroniques émises par des prestataires de certification qualifiés, accrédités auprès de l'Autorité spéciale de surveillance et de réglementation.

Serbie : Oui, certains organismes acceptent les signatures/certificats électronique émis par des autorités de certification étrangères. Nous utilisons le certificat numérique délivré par l'Union internationale des transports routiers (IRU) pour les prédéclarations TIR (informations anticipées sur les marchandises). Par ce moyen, indirectement, tous les titulaires qui utilisent le système de l'IRU pour l'envoi de prédéclarations sont authentifiés pour le système douanier. En outre, dans un proche avenir, nous échangerons très probablement des certificats délivrés en interne au sein de l'administration des douanes aux fins de l'échange de certificats d'origine.

Ukraine : Non, parce qu'il faudra préalablement modifier non seulement la législation douanière, mais aussi la législation régissant les signatures électroniques.

Question 4 : Selon vous, serait-il possible qu'à l'avenir les autorités douanières de votre pays puissent accepter les signatures électroniques, si celles-ci étaient émises ou certifiées par une autorité de certification internationalement reconnue (à savoir une autorité de certification qui serait reconnue par un instrument juridique international, comme la Convention TIR)? Dans l'affirmative, votre gouvernement souhaiterait-il que cette autorité de certification soit établie dans le cadre juridique de la Convention TIR?

République tchèque : À l'avenir, les autorités douanières tchèques pourraient accepter les signatures électroniques, si celles-ci étaient émises ou certifiées par une autorité de certification internationalement reconnue. Cependant, étant donné que la méthode de certification de l'autorité de certification étrangère peut être différente de ce que prescrit la loi tchèque, l'acceptation de la signature est subordonnée à une évaluation au cas par cas.

Il appartient au Ministère de l'intérieur de déterminer si une telle autorité de certification pourrait être mise en place dans le cadre juridique de la Convention TIR.

Estonie : À l'avenir, cela devrait être possible si l'Administration estonienne des systèmes d'information approuvait l'autorité de certification aux fins de la reconnaissance internationale des signatures électroniques.

L'Estonie participe à la politique de l'UE en matière de cyberadministration; dans ce contexte, la reconnaissance internationale des signatures électroniques est envisagée dans un certain nombre de projets en cours, financés par la Direction générale de la société de l'information ou le Programme d'innovation communautaire. Il est fondamental que les États membres de l'UE aient une politique commune concernant la création d'une autorité de certification dans le cadre de la convention TIR.

Allemagne : Une réponse à cette question exigerait une étude approfondie.

France : Comme indiqué ci-dessus, les douanes françaises ne sont pas opposées en principe aux signatures électroniques ni aux certificats électroniques, même lorsqu'ils sont émis par une autorité internationale. Mais, pour le moment, les douanes françaises ne sont pas convaincues que l'utilisation de signatures fondées sur des certificats électroniques offre une solution pratique et soit nécessaire pour authentifier les utilisateurs des systèmes douaniers.

À titre d'information, il convient de noter que, hormis les besoins spécifiques du projet eTIR, la France distingue deux besoins distincts en matière d'authentification :

a) Authentification d'un utilisateur dans un système géré par l'administration nationale; cette exigence peut être satisfaite par d'autres moyens que la signature fondée sur des certificats électroniques, car le système est placé sous le contrôle des douanes (ou un organisme partenaire).

Dans le DTI, un niveau plus simple d'authentification (nom d'utilisateur/mot de passe), associé à une gestion des profils d'utilisateurs, peut être suffisant.

Dans l'EDI, l'échange de système à système et la reconnaissance mutuelle des plates-formes suffisent pour accepter la validité et l'authenticité des données.

D'un point de vue théorique, on suppose que le mécanisme de déclaration internationale eTIR pourrait être considéré comme l'EDI (de même que les prédéclarations TIR qui permettent aux transporteurs d'envoyer des déclarations aux douanes par l'intermédiaire de l'IRU); ainsi, un système national accepterait la déclaration comme toute autre déclaration EDI et ne vérifierait pas l'identité ou le profil de l'utilisateur, puisque cette tâche serait effectuée en amont par le système international. Pour résumer, la France est d'avis que le DTI et l'EDI permettent l'authentification sans signature : dans le DTI, le système et son accès sont directement contrôlés par l'administration; dans l'EDI, l'accès et l'authentification sont contrôlés par la plate-forme EDI (qui peut être internationale). Par conséquent, la signature électronique n'est qu'une des diverses manières de répondre au besoin d'authentification. Même si elle était très sécurisée, elle pourrait imposer des contraintes et ralentir le déploiement de l'e-TIR.

b) Authentification des documents délivrés par un système tiers; cette exigence, qui semble sortir du champ d'application du projet eTIR, fait référence à des documents présentés aux douanes par l'intermédiaire d'un système (par exemple, des documents reçus par courriel) et qui doivent être vérifiés, comme un certificat d'origine signé par une chambre de commerce dans un pays tiers. À l'évidence, dans ce cas, le seul moyen de vérifier l'authenticité est de se fier à une signature fondée sur un certificat électronique. Pour le moment, ce scénario est le seul où l'utilisation de certificats électroniques est envisagée par les douanes françaises dans un avenir proche. Cependant, il semble possible que les Parties contractantes aient des pratiques et des points de vue différents en ce qui concerne l'authentification et la validation des déclarations. En conséquence, il serait peut-être préférable de ménager une certaine souplesse et d'accepter que certains pays exigent des certificats électroniques et d'autres pays utilisent des méthodes différentes.

Suite aux remarques ci-dessus, il est clair que la France n'est ni opposée ni favorable à la mise en place d'une autorité de certification dans le cadre juridique de la Convention eTIR.

Parallèlement, un point important devrait être examiné dans le cadre du document ECE/TRANS/WP.30/GE.1/2011/9, où il est dit au paragraphe 25 : « il serait facile de mettre en œuvre un mécanisme qui permettrait aux organismes nationaux ou aux administrations des douanes de délivrer des certificats électroniques internationalement reconnus avec le numéro d'identification du titulaire du carnet

TIR. Si elle était dûment reconnue dans la Convention TIR, une autorité de certification pourrait être créée sous contrôle international et elle pourrait délivrer des certificats aux sociétés de transport qui remplissent les conditions voulues pour utiliser le système TIR ». À notre avis, ce paragraphe laisse entendre qu'un certificat pourrait être accordé à une société de transport dès que l'autorisation serait accordée. Nous reconnaissons la simplicité de ce scénario. Cependant, les partisans des signatures électroniques doivent vérifier s'il suffit de délivrer des certificats aux « sociétés de transport ». À cet égard, la directive européenne 1999/93/CE établit une distinction entre la « signature électronique » (qui satisfait à des exigences minimales) et la « signature électronique avancée » (qui doit être liée à une personne physique, et qui est la seule qui puisse vraiment – et sans contestation possible – répondre aux exigences légales d'une signature). S'ils étaient délivrés à des « sociétés de transport », et non à des personnes physiques qui travaillent pour ces sociétés, ces certificats ne pourraient probablement pas constituer une base adéquate pour une signature électronique authentique. Les règles semblent assez claires : si un certificat est délivré à une société, il est impossible de savoir qui utilise effectivement le certificat ou de savoir si la personne en question a le pouvoir d'effectuer les formalités obligatoires au nom de la société.

Hongrie : Selon les informaticiens, l'utilisation de signature électronique pour les procédures douanières est possible mais elle entraînera des coûts élevés, tant pour les administrations douanières que pour les titulaires et clients. Il n'existe actuellement aucune base juridique.

Lituanie : Conformément à la loi sur les signatures électroniques de la République de Lituanie, les certificats qualifiés, délivrés par des prestataires de services de certification d'États étrangers, doivent être considérés comme juridiquement équivalents aux certificats qualifiés délivrés par les prestataires de services de certification de la République de Lituanie, si :

- a) Ils sont délivrés par un prestataire de services de certification qui est accrédité en République de Lituanie;
- b) Ils sont délivrés par un prestataire de services de certification qui est accrédité dans l'Union européenne;
- c) Le certificat est garanti par le prestataire de services de certification de la République de Lituanie, qui satisfait aux exigences fixées par le Gouvernement ou par un organisme autorisé par lui pour les prestataires de services de certification qui délivrent des certificats qualifiés;
- d) Le certificat est garanti par le prestataire de services de certification d'un État membre de l'Union européenne, qui satisfait aux exigences équivalentes fixées par le Gouvernement de la République de Lituanie ou un organisme autorisé par lui pour les prestataires de services de certification qui délivrent des certificats qualifiés.

Pays-Bas : La position n'est pas connue car les débats sur la question ont lieu au niveau gouvernemental.

Pologne : Notre loi dispose que les certificats délivrés par des autorités de certification implantées en dehors de la Pologne sont reconnus (et traités comme ceux établis en Pologne) sous réserve qu'une des conditions ci-après, par exemple, soit respectée :

- Le certificat ou l'autorité de certification est reconnu en vertu d'un accord entre l'UE et des pays tiers ou entre l'UE et des organisations internationales; ou
- L'autorité de certification est accréditée dans un système d'accréditation de l'un des pays de l'UE ou de l'EEE et satisfait aux exigences énoncées par la loi de ce pays.

Portugal : La réputation de l'organisme concerné n'est pas en tant que telle le vrai problème. Ce qui compte vraiment c'est la responsabilité de l'autorité de certification qui délivre le certificat.

Roumanie : Actuellement, nous ne savons pas s'il est possible de modifier la loi pour qu'elle définisse le cadre juridique régissant l'utilisation de signatures électroniques certifiées par des autorités de certification étrangères en Roumanie.

Ukraine : En cas de changement de la réglementation, cette évolution dans le cadre de la Convention TIR serait acceptable pour les autorités douanières ukrainiennes.

B. Législation applicable

Autriche : pas de législation nationale.

Belgique : L'utilisation des signatures électroniques repose sur une loi nationale du 9 juillet 2001 et est mise en pratique en vertu d'un « KB » (Koninklijk Besluit = Arrêté royal).

Bulgarie : Loi sur les documents électroniques et les signatures électroniques, en vigueur depuis 2011 et modifiée en décembre 2010.

Chypre : En vertu de lois locales spécifiques ou par conventions ou traités internationaux que Chypre a signés et ratifiés, la législation chypriote reconnaît la certification des signatures comme suit :

À Chypre : certification effectuée par des agents certificateurs autorisés.

Dans tout autre pays : certification effectuée par :

Tout fonctionnaire consulaire de la République de Chypre ou

Les autorités d'autres États qui, en vertu des conventions et traités internationaux dont Chypre est signataire, sont compétentes en la matière. Ces traités sont les suivants :

a) Convention de La Haye supprimant l'exigence de la légalisation des actes publics étrangers, en date du 5 octobre 1961 – lois 50/72 et 91/72. À Chypre, l'autorité compétente pour les questions relatives à cette Convention est le Ministère de la justice. Cette certification est de type « apostille »;

b) Traité sur la coopération juridique entre la République de Chypre et la République hellénique en matière civile, familiale, commerciale et pénale – loi 55/84. En vertu de ce traité, la République de Chypre accepte toutes les signatures certifiées par un agent public d'un service de police grec. Sont également acceptables les certifications des centres de services aux citoyens du Ministère grec de l'intérieur;

c) Convention européenne relative à la suppression de la légalisation des actes établis par les agents diplomatiques ou consulaires. Loi 6/69. En vertu de cette Convention, la République de Chypre accepte toutes les signatures certifiées dans tout pays par des agents consulaires de tout État membre de l'Union européenne.

République tchèque : Loi sur les signatures électroniques n° 227/2000.

Estonie : Loi sur les signatures numériques, entrée en vigueur en 2000.

Allemagne : Loi sur les douanes et la fiscalité et loi sur les signatures électroniques.

Finlande : Règlement (CEE) n° 2452/93 de la Commission (dispositions d'application), article 199.2.

France : Même si, actuellement, les signatures électroniques ne sont pas utilisées par les douanes françaises pour l'authentification de l'utilisateur, nous confirmons que les signatures électroniques sont conformes à la législation française qui se fonde sur le droit communautaire (directive 1999/93/CE du 13 décembre 1999 portant sur un cadre communautaire pour les signatures électroniques). En ce qui concerne le domaine particulier des formalités douanières, le Code des douanes français prévoit que « la transmission d'une déclaration électronique dans les conditions arrêtées par le ministre chargé du budget emporte les mêmes effets juridiques que le dépôt d'une déclaration faite par écrit, signée et ayant le même objet. Cette transmission vaut engagement en ce qui concerne l'exactitude des énonciations de la déclaration et l'authenticité des documents y annexés ou archivés ». Cet article indique clairement que, pour les douanes françaises, la valeur d'une déclaration électronique en douane peut être reconnue indépendamment de l'utilisation d'un certificat électronique, puisque les conditions énoncées par l'administration sont remplies.

Hongrie : Selon le Règlement (CEE) n° 2452/93 de la Commission (dispositions d'application), un processus d'identification est défini à l'article 4.

Italie : Dans leur ensemble, les aspects juridiques concernant toutes les administrations publiques italiennes sont déterminés par Digit PA, l'organisme national chargé de la numérisation des administrations publiques.

Lettonie : L'utilisation des signatures électroniques est applicable en vertu de la loi sur les documents électroniques. Les utilisateurs doivent signer un accord avec l'Administration fiscale de la Lettonie concernant l'utilisation des signatures électroniques. Pour présenter les déclarations en douane (y compris les déclarations de transit et les déclarations TIR), l'identifiant et le mot de passe de l'utilisateur font fonction de signature électronique. Il est inutile de joindre des fichiers particuliers.

Lituanie : Loi sur les signatures électroniques de la République de Lituanie et réglementation de la Direction des douanes qui relève du Ministère lituanien des finances.

Monténégro : Loi sur les signatures électroniques (2003).

Mongolie : La loi sur les signatures électroniques a été approuvée en 2011. Elle entrera en vigueur le 1^{er} janvier 2013. En conséquence, les règles et règlements qui l'accompagnent ainsi que la mise en place d'un cadre juridique en sont à différents stades d'élaboration. L'Administration mongole de l'information, des communications, de la technologie et des postes est chargée de cette question.

Pologne : Loi sur les signatures électroniques et loi sur l'informatisation des organismes qui assurent des services publics.

Des changements sont prévus dans le cadre d'un projet visant à mettre en place, dans un délai de trois ans (application intégrale), un mécanisme de vérification des signatures électroniques pour toutes les procédures, y compris en ce qui concerne le NSTI.

Trois options sont en fait disponibles :

- Utilisation d'une clef pour une transmission sûre des données;
- Utilisation de signatures/certificats électroniques émis par des autorités de certification;
- Utilisation d'un profil de confiance (e-PUAP) pour les communications avec les administrations publiques.

Portugal : Décret-loi n° 290-D/99, du 2 août 1999, modifié par le décret-loi n° 62/2003 du 3 avril 2003 et ordonnance n° 767/2007 du 9 juillet 2007.

Roumanie : Loi n° 455/2001.

Serbie : Loi sur les signatures électroniques, loi sur les documents électroniques, règlement sur la cyberadministration (administration publique), règlement sur le traitement des marchandises approuvé par l'administration douanière, loi sur les procédures administratives générales et loi sur les litiges administratifs.

Slovaquie : Loi nationale sur les signatures électroniques.

Slovénie : Loi sur le commerce électronique et les signatures électroniques.

Espagne : Loi 11/2007 du 22 juin, accès électronique des citoyens aux services publics; mentionne les différentes formes d'identification et d'authentification et présente les systèmes de signature électronique que le public peut utiliser dans ses relations avec les pouvoirs publics (y compris l'administration douanière) conformément à ce que chaque administration décide.

Suède : Lois nationales.

Turquie : Loi sur les signatures électroniques, n° 5070. Cette loi porte sur le statut juridique des signatures électroniques, les activités des prestataires de services de certification électronique et les procédures régissant l'utilisation des signatures électroniques dans tous les domaines.

Ukraine : Loi ukrainienne sur les signatures électroniques numériques du 22 mai 2003, n° 852-IV.

Loi ukrainienne sur les documents électroniques et la circulation électronique des documents du 31 mai 2005, n° 2599-IV; Décret du Conseil des ministres ukrainien du 28 octobre 2004, n° 1452, sur l'approbation de l'application d'un mécanisme de signatures numériques par les pouvoirs publics, les collectivités locales, les entreprises, les institutions et les organismes d'État; Décret du Conseil des ministres ukrainien du 28 octobre 2004, n° 1453, sur l'approbation des procédures opérationnelles permanentes relative à la circulation électronique des documents dans les organes du pouvoir exécutif; Décret du Conseil des ministres ukrainien du 28 octobre 2004, n° 1451, sur l'approbation de l'organe central de certification; Décret du Conseil des ministres ukrainien du 28 mai 2010, n° 680, sur l'approbation de la certification de la disponibilité des documents électroniques (données électroniques) à un moment donné.

Royaume-Uni : Le régime de la TVA, qui relève de l'Administration fiscale et douanière [Her Majesty's Revenue and Customs (HMRC)] ne dispose pas d'un mécanisme de signatures électroniques. Pour les déclarations en douane, le numéro de matricule (authentification de l'utilisateur) pourrait être utilisé, mais plusieurs personnes pourraient intervenir. À des fins douanières, l'utilisation, dans un proche avenir, de signatures électroniques ou de toute autre type de mécanisme d'authentification est envisagée.