Nations Unies ECE/TRANS/SC.1/2023/3

Conseil économique et social

Distr. générale
4 août 2023
Français
Original : anglais

Commission économique pour l'Europe

Comité des transports intérieurs

Groupe de travail des transports routiers

118e session
Genève, 17-19 octobre 2023
Point 2 c) iv) de l'ordre du jour provisoire
Instruments relatifs aux transports intérieurs :
Convention relative au contrat de transport international de marchandises par route (CMR)
Groupe d'experts de la mise en œuvre de l'eCMR

Deuxième partie du rapport du Groupe d'experts de la mise en œuvre de l'eCMR : procédures opérationnelles prévues dans le Protocole additionnel eCMR − environnement numérique

Communication du Groupe d'experts

I. Contexte

1. Le présent document constitue la deuxième partie du rapport établi par le Groupe d'experts de la mise en œuvre de l'eCMR (GE.22) pour la 118e session du Groupe de travail des transports routiers (SC.1). Fondé sur le document ECE/TRANS/SC.1/GE.22/2023/4/Rev.1, il comprend les modifications apportées à la sixième session du GE.22 ainsi que certaines observations formulées par divers participants (notamment les préoccupations exprimées par l'Union internationale des transports routiers (IRU) et ses membres), qui sont présentées en retrait.

2. Le SC.1 est invité à examiner le rapport du Groupe d'experts, qui se compose de quatre parties (ECE/TRANS/SC.1/2023/2 à 5), et à répondre à la demande formulée par le Groupe d'experts (à l'exception de la République islamique d'Iran) visant à ce que son mandat soit prorogé, sans que ses missions et son plan de travail actuels soient modifiés, pour qu'il puisse achever ses travaux et faire rapport au SC.1 à sa 119e session, en octobre 2024. En outre, l'IRU a demandé que la solution hybride (qui consiste à donner à l'exploitant ou au conducteur du véhicule routier la possibilité de présenter les données eCMR de différentes manières afin qu'elles puissent être lues par un humain) soit étudiée dans le cadre des futurs travaux du GE.22, dans le cas où le mandat de celui-ci serait prorogé.

II. Procédures opérationnelles prévues dans le Protocole additionnel eCMR − environnement numérique

3. Le Protocole additionnel à la Convention relative au contrat de transport international de marchandises par route (CMR) concernant la lettre de voiture électronique (Protocole eCMR) et l'environnement numérique imposent la mise en place d'une série de nouvelles prescriptions, qui doivent être examinées et adoptées par les parties concernées, afin d'établir un cadre international durable pour les lettres de voiture électroniques. Il convient de rappeler qu'il ne s'agit pas de concevoir un système de diffusion des données figurant dans la lettre de voiture électronique mais de mettre au point un mécanisme de validation grâce auquel la lettre de voiture électronique constituera l'équivalent juridique de la lettre de voiture papier. C'est pourquoi il est nécessaire d'examiner et d'adopter une série de processus pour adapter cet outil à l'environnement numérique.

Observations relatives au paragraphe 3 que l'IRU et ses associations membres (Azerbaijan International Road Carriers Association (ABADA), Bundesverband Güterkraftverkehr Logistik und Entsorgung) (BGL) et Latvjas Auto Association (LAA)) ont formulées à la sixième session et qui ont recueilli l'adhésion de la République islamique d'Iran : la lettre de voiture sur papier et l'eCMR ayant la même valeur juridique selon l'article 2.1 du Protocole, il n'est pas nécessaire de créer un nouveau mécanisme de validation qui pourrait être lourd et coûteux pour le secteur privé et les pouvoirs publics.

L'International Federation of Freight Forwarders Associations (FIATA), l'Association slovène de logistique et la British International Freight Association (BIFA), qui représentent une partie du secteur privé, ainsi que les autorités suédoises ont dit qu'elles ne souscrivaient pas aux observations formulées par l'IRU, ses associations membres et les autorités iraniennes.

A. Authentification des utilisateurs

Observations relatives aux sur paragraphes 4 à 8 que l'IRU et ses associations membres (ABADA, BGL et LAA) ont formulées à la sixième session et qui ont recueilli l'adhésion de la République islamique d'Iran : le Protocole eCMR n'exige que l'authentification d'une lettre de voiture et non de ses utilisateurs. La Convention CMR définit clairement les utilisateurs d'une lettre de voiture, à savoir l'expéditeur, le transporteur et le destinataire. Les douanes, la police, les garde-frontières, les cours et tribunaux et les autres entités publiques ne sont pas des utilisateurs au sens de la Convention CMR et du Protocole eCMR. Ils n'ont généralement pas besoin d'une authentification distincte, mais utilisent l'accès pour pouvoir lire une lettre de voiture et suivre les modifications qui y sont apportées par les utilisateurs. L'IRU a proposé une solution hybride qui comprend l'impression de la CMR, comme indiqué dans sa déclaration.

La FIATA, l'Association slovène de logistique et la BIFA, qui représentent une partie du secteur privé, ainsi que les autorités suédoises ont dit qu'elles ne souscrivaient pas aux observations formulées par l'IRU, ses associations membres et les autorités iraniennes.

Le GE.22 a indiqué qu'il ne partageait pas la position de l'IRU, de ses associations et du Gouvernement iranien, car elle est contraire au mandat actuel du groupe, au contenu du Protocole eCMR et aux objectifs de développement durable 12 sur la consommation et la production responsables et 13 sur la lutte contre les changements climatiques.

4. L'article 3 du Protocole additionnel eCMR est consacré à l'authentification de la lettre de voiture électronique. Toutefois, sur la base du mandat du Groupe, qui porte sur la mise en œuvre de l'eCMR et sur l'architecture de haut niveau du futur système eCMR, les experts ont relevé deux éléments indispensables en matière d'authentification :

a) L'authentification des utilisateurs ;

b) L'authentification de la version finale de la lettre de voiture.

5. Afin de susciter la confiance dans le système et de garantir que tous les utilisateurs reconnaissent sa validité, ceux-ci devraient être authentifiés lorsqu'ils y accèdent. L'authentification des utilisateurs vaut automatiquement acceptation par ceux-ci des droits et obligations énoncés dans la Convention CMR. Les entités définies comme utilisateurs sont les suivantes :

a) L'expéditeur/l'envoyeur ;

b) Le transporteur/les transporteurs successifs/le transitaire/le sous-traitant ;

c) Le destinataire/le réceptionnaire ;

d) Les autorités douanières ;

e) La police/les garde-frontières ;

f) Les tribunaux et autres entités publiques.

6. Les mécanismes à utiliser pour authentifier les utilisateurs et les lettres de voiture électroniques doivent être ceux qui sont déjà utilisés et qui sont prévus dans la législation nationale des Parties contractantes au Protocole eCMR.

7. Pour des raisons de transparence et d'efficacité, chaque Partie contractante au Protocole eCMR pourrait souhaiter déclarer quels mécanismes d'authentification sont utilisés sur son territoire afin de s'assurer que tous les acteurs sont bien informés des mécanismes officiels utilisés dans chaque pays. Chacun de ces mécanismes génère un numéro d'identification unique pour ses utilisateurs.

8. Il est bien sûr très utile de connaître l'identifiant national unique de chaque utilisateur lors de l'établissement d'une lettre de voiture électronique, dans la mesure où cela permet de gagner du temps et facilite l'utilisation du système. Toutefois, il sera presque impossible de connaître l'identifiant national de chaque utilisateur lorsque des milliers d'importateurs, d'exportateurs et de transporteurs utiliseront les systèmes. Il pourrait être proposé d'établir des directives générales en vue de l'élaboration d'une liste internationale de numéros d'identification, qui serait alimentée par les mécanismes d'authentification nationaux et utilisée par tous les fournisseurs de solutions informatiques au plan international, ce qui encouragerait l'utilisation du système. Ces numéros d'identification établis selon les directives générales, s'ils sont approuvés, seront automatiquement créés par les fournisseurs de solutions informatiques chaque fois qu'un nouvel utilisateur sera enregistré dans un système. Toutefois, par la suite, ce numéro unique pourra être utilisé par l'utilisateur dans le cadre de toute solution certifiée permettant d'établir des lettres de voiture électroniques. Ces directives générales pourraient par exemple être celles indiquées dans le tableau ci-après. En outre, le Groupe d'experts pourrait évaluer les solutions existantes en matière d'identification numérique unique si son mandat est prorogé.

Système international de numéros d'identification	Numéro d'identification national produit par le mécanisme d'authentification
Pays − identifiant du fournisseur de solutions informatiques − numéro d'identification	xxxxxx
SW − 03 − 00001	

B. Signatures électroniques

Observations relatives aux paragraphes 9 à 11 que l'IRU et ses associations membres (ABADA, BGL et LAA) ont formulées à la sixième session et qui ont recueilli l'adhésion de la République islamique d'Iran : conformément aux dispositions du Protocole eCMR, il n'est pas nécessaire d'authentifier l'un quelconque des processus décrits dans le document. Le concept proposé ne peut ni imposer une approche harmonisée ni se fonder sur la loi type de la Commission des Nations Unies pour le

droit commercial international (CNUDCI) sur les signatures électroniques pour créer une telle harmonisation. L'utilisation des signatures électroniques et des mécanismes d'authentification est réglementée au niveau national et peut varier d'un pays à l'autre.

La FIATA, l'Association slovène de logistique et la BIFA, qui représentent une partie du secteur privé, ainsi que les autorités suédoises ont dit qu'elles ne souscrivaient pas aux observations formulées par l'IRU, ses associations membres et les autorités iraniennes.

9. L'article 3 du Protocole additionnel eCMR dispose expressément que la signature électronique est utilisée pour l'authentification des lettres de voiture électroniques, même si le paragraphe 2 de cet article indique que la lettre de voiture peut aussi être authentifiée par tout autre procédé d'authentification électronique permis par la législation du pays. Quel que soit le mécanisme utilisé (signature électronique ou autre), il ne s'agit pas de « noms d'utilisateur » et de « mots de passe ».

10. Les signatures électroniques ou tout autre mécanisme national d'authentification seront utilisés pour authentifier notamment les processus suivants :

a) Authentification en ligne de la version finale de la lettre de voiture par les parties (expéditeur ou transporteur) ;

b) Authentification des réserves du transporteur lors du chargement des marchandises et de l'acceptation de l'expéditeur ou de l'envoyeur ;

c) Authentification du transfert du droit de disposer des marchandises. L'une des principales fonctions qu'un futur système eCMR devrait prendre en charge est de déterminer qui a le droit de disposer des marchandises à certaines étapes du voyage en l'absence de deuxième exemplaire sur papier de la lettre de voiture attestant de ce fait. Une authentification devrait être requise chaque fois que cette situation se produit (voir ECE/TRANS/SC.1/GE.22/2023/3) ;

d) Authentification des modifications apportées par l'expéditeur ou l'envoyeur concernant le destinataire ou le réceptionnaire ou des nouvelles instructions établies par l'expéditeur ou l'envoyeur. Cette action est directement liée à la responsabilité du transporteur et il convient de déterminer de manière sûre qui établit ces nouvelles instructions ;

e) Authentification de l'attestation d'acceptation ou de non-acceptation des marchandises par le destinataire avec ou sans réserves. Comme indiqué dans le document ECE/TRANS/SC.1/GE.22/2023/3, le destinataire doit effectuer deux opérations à réception des marchandises : a) attester de la livraison ; b) attester de l'acceptation ou de la non-acceptation des marchandises. En ce qui concerne la première opération, le destinataire s'est déjà authentifié dans le système. En ce qui concerne l'attestation d'acceptation, le destinataire doit s'authentifier pour accepter définitivement les marchandises avec ou sans réserves ou ne pas les accepter ;

f) Authentification des autorités douanières qui contrôlent les marchandises et formulent des commentaires ou des tribunaux qui demandent des données. Ce point s'appliquera si les agents des douanes doivent s'authentifier avant d'accéder aux données, ce qui dépendra de la manière dont l'architecture de haut niveau sera conçue et dont les autorités douanières seront interconnectées. Comme il serait inefficace d'obliger les autorités douanières à enregistrer et authentifier chacun de leurs utilisateurs auprès des centaines de fournisseurs informatiques qui génèrent des lettres de voiture électroniques afin que ces utilisateurs puissent obtenir des informations de manière ponctuelle, il est peu probable que cette approche soit suivie.

11. Il n'existe pas de convention internationale relatives aux signatures électroniques. Cependant, le Groupe a envisagé l'adoption de solutions qui faciliteraient la mise en place d'une approche harmonisée. Il suggère d'utiliser la loi type de la Commission des Nations Unies pour le droit commercial international (CNUDCI) sur les signatures électroniques.

La loi type sur les signatures électroniques (LTSE) vise à permettre et faciliter l'utilisation des signatures électroniques en établissant des critères de fiabilité

technique pour l'équivalence entre ces signatures électroniques et les signatures manuscrites. En conséquence, elle peut aider les États à mettre en place un cadre législatif moderne, harmonisé et juste pour régler efficacement la question du traitement juridique des signatures électroniques et garantir leur statut. La loi type sur les signatures électroniques est basée sur les principes fondamentaux communs à tous les textes de la CNUDCI relatifs au commerce électronique, à savoir la non-discrimination, la neutralité technologique et l'équivalence fonctionnelle. Elle établit des critères de fiabilité technique pour l'équivalence entre signatures électroniques et signatures manuscrites ainsi que des règles fondamentales de conduite pouvant servir de référence pour évaluer les obligations et responsabilités du signataire, de la partie se fiant à la signature et des tiers de confiance intervenant dans le processus de signature. Enfin, la loi type énonce des dispositions favorisant la reconnaissance des certificats et des signatures électroniques étrangers en se fondant sur le principe de l'équivalence substantielle, pour lequel le lieu d'origine de la signature n'est pas pris en considération. La loi type est accompagnée d'un guide pour son incorporation présentant des informations de base et des explications afin d'aider les États à élaborer les dispositions législatives nécessaires et éventuellement de guider d'autres utilisateurs du texte.

C. Solutions informatiques

Observations relatives aux paragraphes 12 à 14 que l'IRU et ses associations membres (ABADA, BGL et LAA) ont formulées à la sixième session et qui ont recueilli l'adhésion de la République islamique d'Iran : le Protocole eCMR s'applique au droit international privé. Les dispositions de la Convention ne prévoient pas l'utilisation de spécifications fonctionnelles et techniques particulières. Il n'existe donc aucun fondement juridique justifiant que ces spécifications fonctionnelles et techniques soient élaborées par le SC.1 et adoptées par le Comité des transports intérieurs (CTI), ou qu'elles soient considérées comme obligatoires. En outre, l'approche proposée, qui consiste à rendre ces spécifications obligatoires, remettrait en cause les solutions actuellement en place. Même si des spécifications fonctionnelles et techniques sont nécessaires pour l'établissement de la lettre de voiture électronique, elles doivent être élaborées par le secteur privé au lieu de lui être imposées. Pour ce qui concerne les moyens de transmission des données, le secteur privé doit avoir la possibilité de choisir parmi une gamme d'outils informatiques et de solutions interopérables déjà à sa disposition, pour autant que les conditions nécessaires à l'établissement de la lettre de voiture électronique soient réunies. L'harmonisation ne doit porter que sur l'ensemble de données afin de permettre leur échange entre les différents acteurs. Les lettres de voiture électroniques CIM/SMGS pour le transport ferroviaire et la lettre de transport aérien, déjà mises en œuvre et opérationnelles, peuvent servir d'exemples.

La FIATA, l'Association slovène de logistique et la BIFA, qui représentent une partie du secteur privé, ainsi que les autorités suédoises ont dit qu'elles ne souscrivaient pas aux observations formulées par l'IRU, ses associations membres et les autorités iraniennes.

12. Une entité souhaitant établir des lettres de voiture électroniques mettra au point une solution informatique permettant de le faire conformément à la Convention CMR et à son Protocole en s'appuyant sur les spécifications fonctionnelles et techniques adoptées par le Comité des transports intérieurs (CTI) sur proposition du SC.1.

13. Les experts devraient décider si l'application des spécifications fonctionnelles et techniques est obligatoire ou non. En clair, l'élaboration de spécifications techniques pourrait faire l'objet d'un mandat confié à un nouveau groupe d'experts en informatique/technique. L'article 5 du Protocole mentionne toutefois que les parties conviennent des procédures, ce qui implique clairement que toutes les parties doivent se mettre d'accord sur les mêmes

procédures et les appliquer, car en l'absence d'application cet accord n'aurait aucun effet. Ces deux approches présentent des avantages et des inconvénients, à savoir :

a) Si les spécifications sont obligatoires, chaque utilisateur sait que, quelle que soit la solution informatique il utilise :

i) La lettre de voiture électronique produite aura *la même force probante et produira les mêmes effets* que la *lettre de voiture* sur papier (par. 2 de l'article 2 du Protocole) ;

ii) Les Parties contractantes au Protocole se sont mises d'accord sur *la façon dont le titulaire des droits découlant de la lettre de voiture électronique peut démontrer qu'il en est le titulaire* ;

iii) Les Parties contractantes au Protocole se sont mises d'accord sur les procédures permettant de compléter ou de modifier la lettre de voiture électronique, y compris l'assurance que la lettre de voiture électronique a conservé son intégrité ;

iv) Par conséquent, pendant le trajet, les autorités douanières considéreront cette lettre de voiture électronique comme un document original et, dans toute affaire judiciaire future, les tribunaux reconnaîtront l'authenticité de la lettre de voiture électronique qui a été établie conformément à la Convention ;

v) Le fait de rendre les spécifications obligatoires entraîne cependant une autre obligation pour les États : celle de certifier chaque solution informatique. Idéalement, les gouvernements devraient créer un organisme national chargé de certifier que les solutions sont conformes aux spécifications. Une autre approche, moins optimale, consisterait à faciliter le processus de certification en créant une plateforme centrale d'autocertification (si celle-ci est mise en place par l'ONU, elle devra être validée par les services juridiques) sur laquelle les utilisateurs déclarent eux-mêmes que leurs solutions informatiques sont conformes aux spécifications fonctionnelles et techniques. Des tests de conformité peuvent également être prévus pour vérifier ces solutions. Les utilisateurs certifiés prendront acte que dans les cas, notamment, où un test serait effectué ou un problème serait porté devant un tribunal, ils risqueraient de se voir retirer leur certification et de subir une atteinte à leur réputation du fait de cette situation.

b) Si les spécifications ne sont pas obligatoires, n'importe qui peut prétendre être en mesure d'établir des lettres de voiture électroniques conformes à la Convention CMR. Toute solution existante continuera à fonctionner sous sa forme actuelle. Cela favoriserait le maintien du statu quo, qui n'est pas optimal pour le fonctionnement de l'eCMR car il est impossible de savoir qui applique la Convention et qui ne l'applique pas.

i) Si un régime mixte est adopté et que certaines solutions informatiques sont conformes aux spécifications et d'autres ne le sont pas, il faudrait au moins prévoir l'obligation de déclarer sur le site Web que la solution est « conforme aux spécifications eCMR de l'ONU » ou « non conforme aux spécifications eCMR de l'ONU » ;

ii) Ainsi, les utilisateurs seront informés et pourront décider s'ils souhaitent utiliser ces plateformes ou non ;

iii) Pour les autorités douanières, la tâche sera encore plus difficile car l'élaboration des spécifications fonctionnelles et techniques a pour but de permettre aux entités publiques de reconnaître mutuellement les solutions, de les utiliser en toute confiance et de commencer à les utiliser au niveau international. Si un régime mixte est appliqué, les autorités douanières seront tenues de n'utiliser que les solutions informatiques qui sont conformes aux spécifications techniques ;

iv) Si une plateforme centrale d'interconnexion est utilisée dans l'architecture de haut niveau pour la connexion des autorités douanières, la situation sera encore plus simple puisque seules les solutions informatiques certifiées permettront de se connecter à cette plateforme centrale et de fournir des données aux autorités douanières.

14. Lors de l'élaboration de ces solutions, les principes suivants devraient être respectés :

a) L'entité devrait être toute personne ou société intéressée par la mise au point d'une solution électronique. Il peut s'agir d'une entité privée ou publique ;

b) Toutes les entités peuvent choisir librement la technologie qu'elles souhaitent utiliser pour autant qu'elles se conforment aux spécifications qui leur sont fournies afin de s'assurer que les dispositions de la Convention CMR sont respectées. À nouveau, si les spécifications sont appliquées à titre obligatoire, la solution informatique doit être certifiée par l'organisme national d'agrément, par la plateforme centrale ou d'une autre façon ;

c) Les entités devraient décider si leurs services sont ou non payants ;

d) Le fournisseur informatique ne devrait pas avoir accès, ni en lecture ni en écriture, aux données CMR générées par le système qu'il a mis au point une fois que ce dernier est mis sur le marché, à moins que cela soit nécessaire pour des raisons opérationnelles, avec le consentement des utilisateurs du système. Si une entreprise de transport a mis au point son propre système pour ses activités, elle devrait alors avoir accès aux données selon les règles applicables pour les transporteurs ou envoyeurs. Il devrait être strictement interdit au fournisseur informatique de vendre ou d'échanger les données générées sur sa plateforme à des fins lucratives ou pour quelque autre raison que ce soit, y compris à des fins concurrentielles.

D. Organisme national d'agrément

Observations relatives aux paragraphes 15 à 17 que l'IRU et ses associations membres (ABADA, BGL et LAA) ont formulées à la sixième session et qui ont recueilli l'adhésion de la République islamique d'Iran : il n'y a pas lieu de créer un organisme national d'agrément chargé de garantir le respect des spécifications fonctionnelles et techniques. En effet, ni l'organisme national d'agrément ni lesdites spécifications ne sont prévus dans le Protocole eCMR. En outre, la création d'un tel organisme entraînera une charge supplémentaire pour les utilisateurs actuels de la lettre de voiture électronique, pour les raisons susmentionnées. Les pouvoirs publics seraient également touchés par cette proposition puisque plusieurs nouvelles obligations leur seraient imposées. En fait, la création d'un tel organisme, parmi d'autres procédures lourdes (création d'une plateforme permettant de générer des lettres de voiture électroniques, publication d'une liste de solutions informatiques, stockage des données, sauvegarde, etc.), est fondée sur le besoin de se conformer aux spécifications fonctionnelles et techniques élaborées par les organes de la CEE et doit être rejetée.

La FIATA, l'Association slovène de logistique et la BIFA, qui représentent une partie du secteur privé, ainsi que les autorités suédoises ont dit qu'elles ne souscrivaient pas aux observations formulées par l'IRU, ses associations membres et les autorités iraniennes.

15. Le Groupe a examiné la nécessité de mettre en place un organisme national d'agrément, sans parvenir à un accord. Cet organisme serait principalement chargé de s'assurer de la conformité aux spécifications et à la Convention CMR. Le Groupe continue à étudier cette possibilité et examine d'autres options. Toutefois, si le recours à un organisme d'agrément est proposé, le Groupe suggère que les parties conviennent des procédures d'agrément (éventuellement un test de conformité).

16. Il s'agirait pour chaque pays de désigner officiellement un ou plusieurs organismes d'agrément qui auraient les obligations ou tâches suivantes :

a) Établir, comme convenu au niveau du SC.1, les spécifications techniques qui seront utilisées pour la mise au point des plateformes servant à générer les lettres de voiture électroniques ;

b) Valider les solutions informatiques mises au point sur la base de ces spécifications techniques (quelle que soit la technologie utilisée) et communiquer la liste officielle des fournisseurs de solutions informatiques agréés pour générer des lettres de voiture électroniques sur le territoire (et reconnus par les Parties contractantes au Protocole

eCMR). (Observation formulée par l'Association slovène de logistique et l'IRU : cette mesure n'est pas facile à mettre en pratique.) Cela évitera également aux envoyeurs, aux transporteurs et aux destinataires d'adopter des solutions qui ne sont pas conformes à la Convention CMR et aux spécifications eCMR, notamment en ce qui concerne les tribunaux, les dommages aux marchandises, etc. ;

c) Surveiller l'utilisation des services eCMR sur le territoire et signaler les interruptions, ainsi que les pratiques monopolistiques ou oligopolistiques qui sont contraires aux principes de fonctionnement du système eCMR ;

d) Retirer de façon temporaire ou permanente l'agrément des fournisseurs de solutions informatiques utilisées pour générer des lettres de voiture électroniques lorsque de telles pratiques sont observées et en informer tous les utilisateurs du système.

17. Un tel organisme national d'agrément contribuerait à établir la confiance dans le système et la reconnaissance mutuelle qui sont nécessaires pour qu'un tel système électronique international puisse fonctionner sans interruption. Chaque pays devrait décider quel organisme sera désigné pour accomplir ces tâches. Il pourrait par exemple s'agir des chambres, de l'association nationale du transport routier, d'un organisme d'accréditation ou d'un nouvel organisme. Les autorités seraient tenues d'annoncer officiellement la désignation de cet organisme, en précisant ses tâches et ses obligations. Il convient de noter qu'il devrait s'agir d'un organisme distinct de celui qui s'occupera de l'authentification des utilisateurs (expéditeur, transporteur, destinataire), cette fonction étant différente.

E. Stockage sécurisé des données

Observations relatives aux paragraphes 18 à 20 que l'IRU et ses associations membres (ABADA, BGL et LAA) ont formulées à la sixième session et qui ont recueilli l'adhésion de la République islamique d'Iran : la création d'un organisme national d'agrément n'étant pas nécessaire, le stockage sécurisé des données ne l'est pas non plus. Il convient d'évaluer juridiquement si cet organisme national d'agrément aurait le droit de stocker des données commerciales, conformément aux dispositions de la législation interne de chaque Partie au Protocole eCMR. Si les données peuvent être conservées, la durée de leur conservation doit également être évaluée sur le plan juridique car elle est fixée au niveau national. Compte tenu de ce qui précède, on ne peut pas imposer une approche harmonisée.

La FIATA, l'Association slovène de logistique et la BIFA, qui représentent une partie du secteur privé, ainsi que les autorités suédoises ont dit qu'elles ne souscrivaient pas aux observations formulées par l'IRU, ses associations membres et les autorités iraniennes.

18. Le stockage sécurisé des données (c'est-à-dire la lettre de voiture électronique originale, suivie des modifications énumérées chronologiquement) est d'une importance capitale pour l'instauration d'un environnement de confiance pour le futur système eCMR. Il serait assuré par une solution de stockage sécurisé propre au sytème eCMR ou par une solution tierce satisfaisant à toutes les normes de sécurité requises.

19. Les données CMR comprennent des informations sensibles sur le plan commercial, qui ne devraient pas être détenues par une seule entité ou être concentrées entre les mains d'un petit groupe de sociétés informatiques. À cet égard, les pratiques monopolistiques ou oligopolistiques sont à proscrire afin de protéger les données et, partant, l'intégrité du système. Toutefois, dans un environnement de marché libre, où une entreprise peut acquérir une autre entreprise d'un pays voisin ou fusionner avec elle, ou tout simplement établir des succursales n'importe où, il est quasiment impossible d'éviter ces pratiques. Il est très probable que le Groupe ne pourra dans ce cas qu'énoncer des recommandations générales, et que les questions de ce type devront être traitées au niveau national.

20. Il conviendrait d'harmoniser le nombre d'années prévu pour la conservation des données. Le Groupe est provisoirement convenu que les données eCMR devraient être conservées pendant une période de dix ans après leur production, en vue d'une utilisation future par des entités publiques ou privées.

F. Cybersécurité − Sauvegardes

Observations relatives aux paragraphes 21 à 23 que l'IRU et ses associations membres (ABADA, BGL et LAA) ont formulées à la sixième session et qui ont recueilli l'adhésion de la République islamique d'Iran : la création d'un organisme national d'agrément n'étant pas nécessaire, il en va de même pour les méthodes de cybersécurité et de sauvegarde. Si les parties au contrat de transport ont besoin de renforcer la cybersécurité ou d'assurer la sauvegarde des données, elles sont libres d'appliquer les solutions de leur choix. Les questions relatives à la cybersécurité et aux sauvegardes sont réglementées au niveau national. Il est donc difficile d'imposer une approche harmonisée. En outre, dans nombre de pays, les autorités exigent que les données soient physiquement conservées sur leur territoire et non à l'étranger. Par conséquent, il est impossible d'imposer une approche harmonisée en matière de cybersécurité et de sauvegardes.

La FIATA, l'Association slovène de logistique et la BIFA, qui représentent une partie du secteur privé, ainsi que les autorités suédoises ont dit qu'elles ne souscrivaient pas aux observations formulées par l'IRU, ses associations membres et les autorités iraniennes.

21. La cybersécurité est également liée au thème ci-dessus et à l'environnement de confiance dans lequel l'entreprise informatique doit mener ses activités. La question de l'intégrité des données est strictement liée à la confiance dans le système. Le futur système eCMR devrait conserver une trace exacte, non modifiable, de la chronologie, établie à partir de la date et de l'heure de chaque événement. Par exemple, les fournisseurs de solutions informatiques privés devraient effectuer régulièrement une sauvegarde des données. Il faudrait toutefois préciser où les données sont enregistrées. Cette procédure servira à plusieurs fins :

a) Comparaison des données sur demande, pour s'assurer que les données fournies sont les données originales ;

b) Sauvegarde en cas de panne technique de la solution informatique ;

c) Sauvegarde en cas de faillite du fournisseur informatique ;

d) Procédure de secours.

22. Les parties concernées doivent se conformer à la législation applicable, notamment en matière de cybersécurité et de protection de la vie privée.

23. Le Protocole (par. 3 de l'article 4) prévoit que « *la procédure employée pour compléter ou modifier la lettre de voiture électronique doit permettre la détection en tant que telle de tout complément ou toute modification et assurer la préservation des indications originales de la lettre de voiture électronique* ». En outre, au paragraphe 2 de l'article 4, il est précisé que « *le procédé employé pour l'établissement de la lettre de voiture électronique doit garantir l'intégrité des indications qu'elle contient à compter du moment où elle a été établie pour la première fois sous sa forme définitive* ». Il ressort donc clairement du Protocole qu'en ce qui concerne la conservation des données en toute sécurité, il convient de conserver la lettre de voiture électronique originale, suivie des modifications énumérées chronologiquement, plutôt que de conserver la version finale de la lettre de voiture électronique établie à la fin du trajet, suivie des modifications énumérées chronologiquement. Il ne fait pas de doute que le Protocole favorise l'approche axée sur *la version finale de la lettre de voiture électronique* authentifiée au départ par l'expéditeur et le transporteur avant le début du trajet, contrairement à la pratique en usage avec les documents sur papier selon laquelle la lettre de voiture finale sur papier est conservée à la fin du trajet lorsque tous les cachets et signatures ont été apposés.

G. Procédure de secours

Observations relatives aux paragraphes 24 à 26 que l'IRU et ses associations membres que (ABADA, BGL et LAA) ont formulées à la sixième session et qui ont recueilli l'adhésion de la République islamique d'Iran : la création d'un organisme national d'agrément n'étant pas nécessaire, il en va de même pour les procédures de secours. Ce concept propose une solution mondiale unique dans laquelle l'utilisation de codes QR et de notifications par courrier électronique sera définie comme « obligatoire », mais les expéditeurs et les transporteurs sont libres de convenir entre eux de la solution informatique, de la technologie et du type de notification qu'ils utiliseront, conformément à l'alinéa f) du paragraphe 2 de l'article 5 du Protocole eCMR. Il est donc impossible d'imposer une approche harmonisée en matière de procédure de secours.

La FIATA, l'Association slovène de logistique et la BIFA, qui représentent une partie du secteur privé, ainsi que les autorités suédoises ont dit qu'elles ne souscrivaient pas aux observations formulées par l'IRU, ses associations membres et les autorités iraniennes.

24. Dans un environnement électronique, il est difficile de parler de la perte ou de l'absence de la lettre de voiture puisqu'il est toujours possible d'accéder au document ou aux données en ligne, sur la plateforme où le document a été généré initialement.

25. Le Protocole eCMR ne contient pas de disposition traitant d'une procédure de secours. Toutefois, l'alinéa f) du paragraphe 2 de l'article 5 prévoit que les parties conviennent des « *procédures de remplacement éventuel de la lettre de voiture électronique par une lettre de voiture établie par d'autres moyens* », ce qui implique une procédure de secours. La procédure de secours est d'une importance cruciale pour assurer le fonctionnement du futur système eCMR dans les cas où, pour quelque raison que ce soit, le système ne fonctionne pas comme prévu.

26. Il est très important de déterminer les cas dans lesquels une procédure de secours est nécessaire, puis de définir la procédure de secours utilisée. Le tableau suivant présente succinctement les différentes situations où une procédure de secours peut s'avérer nécessaire, ainsi qu'une suggestion de procédure à suivre.

Situation où une procédure de secours peut s'avérer nécessaire	**Procédure de secours à suivre**
Processus d'élaboration d'une lettre de voiture électronique/d'établissement d'une version finale de la lettre de voiture électronique/ d'authentification de la version finale d'une lettre de voiture électronique :	1. Utilisation de la lettre de voiture sur papier
a. Ne fonctionne pas ou produit des erreurs	a. Le système devrait fournir un retour d'information avec des orientations sur la manière de résoudre le problème b. Possibilité pour les utilisateurs de prendre contact automatiquement avec l'administration du système pour trouver une solution c. Utilisation d'un autre système ou d'une autre solution informatique
b. Pas d'accès au système en raison de coupures d'électricité ou d'Internet	b. Utilisation de la lettre de voiture sur papier
En cas de problèmes en cours de route, par exemple s'il n'y a pas d'accès à Internet à un poste frontière, l'appareil de la police ne fonctionne pas, le destinataire n'a pas accès	Lorsque la version finale de la lettre de voiture électronique a été authentifiée : a. Un document PDF non modifiable doit être créé et envoyé à tous les utilisateurs concernés

à Internet pour récupérer le code unique (code QR ou code-barres, par exemple) envoyé pour effectuer la procédure d'attestation de livraison, etc.	b. Si le numéro de téléphone mobile du transporteur est fourni, un code QR lui sera envoyé afin qu'il puisse être conservé dans son application de stockage, comme pour les cartes d'embarquement c. Si la solution informatique comprend une application mobile, l'ensemble des informations avec le code QR sera conservé dans l'application mobile d. Les informations eCMR anticipées seront communiquées au début du trajet à toutes les douanes sur l'itinéraire et à destination si les douanes sont connectées à la solution informatique et si les transporteurs acceptent de préciser l'itinéraire qu'ils suivront (modification possible en cours de route si nécessaire). Les douanes pourront effectuer une analyse des risques bien avant l'arrivée du camion et celle-ci sera déjà enregistrée dans leur système à l'arrivée du camion e. Les douanes devraient accepter les lettres de voiture sur papier f. Le destinataire doit pouvoir recevoir le code unique à la fois dans son système de courrier électronique et sur son téléphone portable, ce qui permet une double identification

H. Autres obligations du transporteur en cas d'utilisation de la lettre de voiture électronique (par. 1 de l'article 6 du Protocole eCMR)

27. Cette disposition a été reprise textuellement de la Convention de Montréal de 1999, qui établit la responsabilité des compagnies aériennes en cas de mort ou de lésion corporelle d'un passager, ainsi qu'en cas de retard, de dommage aux bagages ou à la marchandise ou de perte de ceux-ci. La Convention de Montréal vise à unifier les différents régimes conventionnels internationaux relatifs à la responsabilité des transporteurs aériens qui ont été élaborés sans souci de cohérence depuis 1929. Le secrétariat essaiera de trouver dans le mémorandum explicatif du Protocole eCMR des informations justifiant l'ajout du paragraphe 1 de l'article 6.

28. Le paragraphe 2 de l'article 4 de la Convention CMR de Montréal prévoit ce qui suit : « L'emploi de tout autre moyen constatant les indications relatives au transport à exécuter peut se substituer à l'émission de la lettre de transport aérien. Si de tels autres moyens sont utilisés, le transporteur délivre à l'expéditeur, à la demande de ce dernier, un récépissé de marchandises permettant l'identification de l'expédition et l'accès aux indications enregistrées par ces autres moyens. ».

29. Voici une explication possible de l'ajout de l'article 6 dans le texte du Protocole :

30. À la page 3 du document TRANS/SC.1/2002/1, présenté par UNIDROIT en février 2002, il est dit ce qui suit à propos du paragraphe 1 de l'article 6 : « Ce paragraphe est repris de l'article 4.2 de la Convention de Montréal. Cet article 4 dispose en effet, que : "l'emploi de tout autre moyen constatant les indications relatives au transport à exécuter peut se substituer à l'émission de la lettre de transport aérien", mais, pour éviter "l'impérialisme" de l'électronique, oblige néanmoins le transporteur à délivrer un récépissé papier de la prise en charge. ». Ce même document contient également un questionnaire ; dans la dernière question, il est demandé aux États s'ils approuvent l'inclusion de cette disposition dans le texte du Protocole.

31. Dans le projet de 2003, l'article 7, intitulé « Droit de disposition », établit ce qui suit : « 1. Lorsqu'une lettre de voiture électronique est émise, le droit de l'envoyeur de disposer de la marchandise s'éteint dès que le transporteur transfère la clef d'accès au destinataire, conformément à l'article 5. ». Le projet comporte également la note ci-après : « La lettre de voiture électronique n'étant délivrée qu'en un seul exemplaire, l'obligation de produire le premier exemplaire ne s'applique pas. L'attribution d'une clef qui n'autorise que la personne ayant le droit de disposition à saisir des instructions sur la lettre de voiture permet de s'assurer que seule la personne ayant le droit de disposition est habilitée à saisir une instruction sur la lettre de voiture. ».

III. Description de l'architecture de haut niveau du système eCMR

Description d'ensemble du système eCMR

Observations relatives aux paragraphes 33 à 40 que l'IRU et ses associations membres (ABADA, BGL et LAA) ont formulées à la sixième session et qui ont recueilli l'adhésion de la République islamique d'Iran : contrairement à ce qui est indiqué, les processus proposés dans l'architecture de haut niveau entraînent plusieurs changements par rapport aux pratiques actuelles. Si ces changements entrent en vigueur, les utilisateurs actuels de l'eCMR devront adapter leurs activités, ce qui aura un coût. Par ailleurs, en raison de la grande complexité de ce concept, il se peut que les utilisateurs actuels de l'eCMR souhaitent continuer à utiliser des lettres de voiture sur papier. Les solutions eCMR doivent conserver tous les avantages de la version papier, tout en modernisant le système en supprimant la paperasserie et les coûts de gestion. L'élaboration de solutions eCMR pratiques, adaptées et efficientes devrait être laissée au secteur privé.

La FIATA, l'Association slovène de logistique et la BIFA, qui représentent une partie du secteur privé, ainsi que les autorités suédoises ont dit qu'elles ne souscrivaient pas aux observations formulées par l'IRU, ses associations membres et les autorités iraniennes.

32. Comme il est indiqué dans l'introduction relative au Protocole eCMR, l'objectif final de l'informatisation de la Convention CMR est de dématérialiser tout le cycle de vie de la lettre de voiture CMR depuis sa distribution, sa délivrance devant tenir compte de l'ensemble des droits et obligations définis dans la Convention CMR et l'objectif ultime étant la suppression définitive du support papier sans pour autant aller à l'encontre de l'esprit de la Convention.

33. Les entités qui établissent des lettres de voiture électroniques − expéditeurs/envoyeurs, transporteurs et, le cas échéant, destinataires − pourront utiliser toute solution informatique certifiée pour créer une lettre de voiture électronique. L'application des normes du Centre des Nations Unies pour la facilitation du commerce et les transactions électroniques (CEFACT-ONU) relatives aux données, telles que révisées par le Groupe d'experts, garantirait l'interopérabilité de toutes les solutions électroniques. Ces solutions électroniques, qui seront conformes aux spécifications convenues au niveau de la CEE, seront capables de fournir tous les services électroniques requis pour les lettres de voiture électroniques, en tenant compte de tous les besoins, droits, obligations et procédures définis dans la Convention CMR, ce qui permettrait à la lettre de voiture électronique d'être reconnue comme l'équivalent juridique de la lettre de voiture sur papier.

34. Sur la base des débats du Groupe, l'architecture de haut niveau ci-après est en train de prendre forme pour le futur système eCMR. Il convient de noter qu'à l'avenir, des milliers d'expéditeurs, de destinataires et de transporteurs devraient, d'une manière ou d'une autre, utiliser les services de centaines de prestataires informatiques qui fournissent des solutions informatiques pour les lettres de voiture électroniques fondées ou non (à déterminer) sur les spécifications données par la CEE. L'interopérabilité entre les différents systèmes devrait être garantie dans la mesure où les normes CEFACT-ONU révisées, sur la base des travaux du Groupe, seront appliquées. L'interopérabilité est la capacité qu'un système, dont les interfaces sont détaillées de manière exhaustive, a ou aura de fonctionner de manière

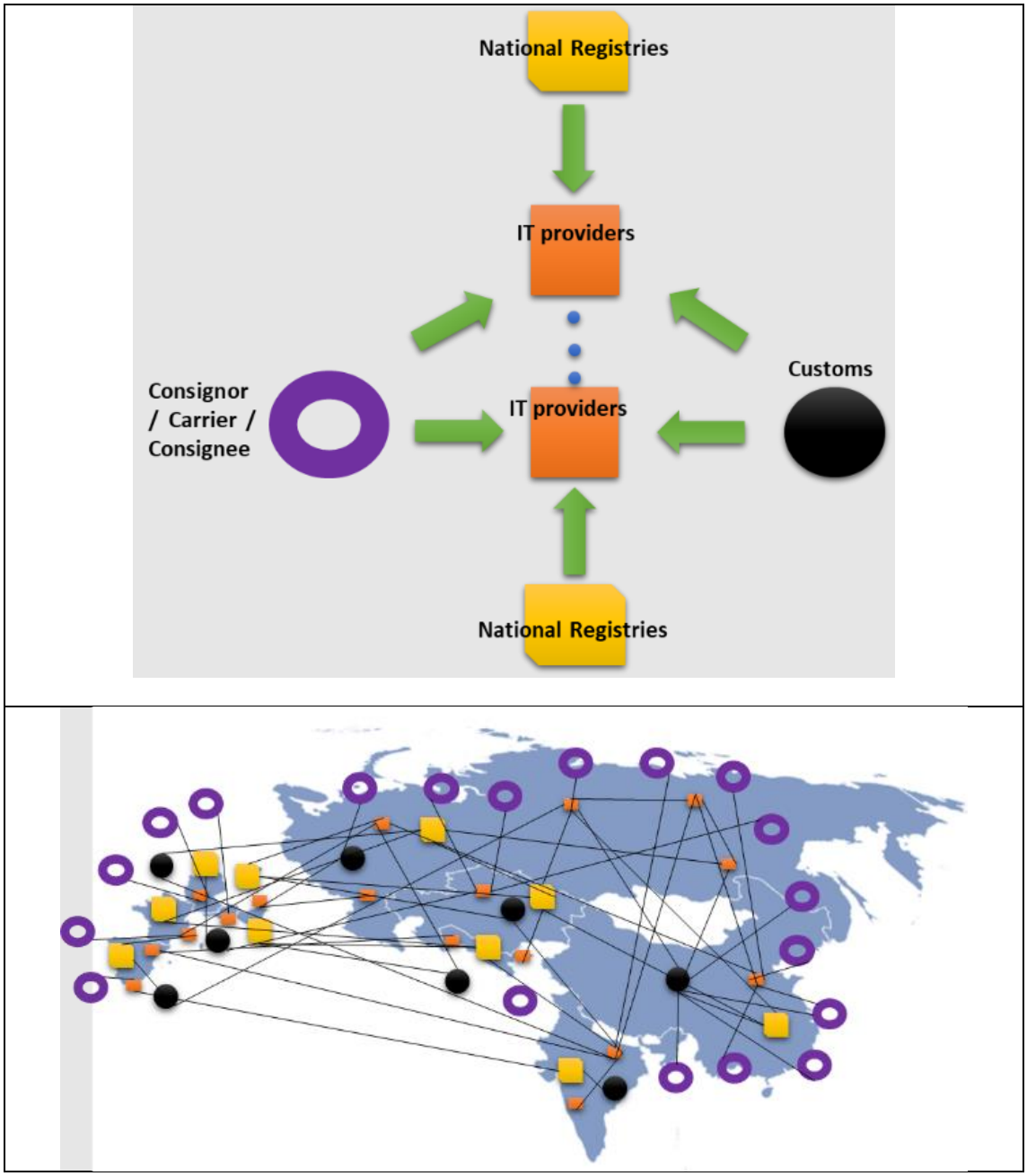
pleinement compatible avec d'autres systèmes, sur le plan soit de la mise en œuvre, soit de l'accès.

35. Les solutions informatiques eCMR reposeront sur la communication entre machines, déclenchée par des événements donnés. C'est pourquoi les interfaces entre les différents utilisateurs de l'eCMR doivent être clairement définies, ce qui facilite l'interconnexion entre les systèmes. De plus, et dans le même but, les interfaces devraient être fondées sur les normes mondiales les plus récentes en matière de communication.

36. Cependant, même dans ce cas, il convient d'élaborer et de mettre en œuvre un projet d'interconnexion. Les systèmes informatiques eCMR doivent être conçus et la documentation pertinente doit être élaborée de manière à faciliter la connexion avec les différentes parties, y compris lorsqu'une nouvelle version doit être installée. La facilité de connexion permet de réduire au minimum les dépenses engagées par le service d'assistance des fournisseurs de solutions informatiques lorsqu'il aide les Parties contractantes à connecter leurs systèmes aux solutions informatiques eCMR.

37. D'autre part, afin d'avoir un accès sur demande aux informations relatives aux lettres de voiture électroniques, les autorités douanières des Parties contractantes doivent avoir accès (être connectées) aux centaines de fournisseurs informatiques.

Figure : Architecture de haut niveau du futur système eCMR − option 1 (approche décentralisée)



Source : Secrétariat.

38. Concrètement, il existe trois types d'utilisateurs :

a) Utilisateurs occasionnels − ils doivent ajouter des commentaires à la lettre de voiture électronique au moyen de liens spécifiques qui leur sont envoyés, puis se rendre sur les sites Web pertinents. Cependant, il reste à déterminer de quelle manière authentifier ces utilisateurs et les enregistrer dans les systèmes informatiques sur la base de l'authentification fournie. Une fois la procédure accomplie, ils devraient encore se compter par centaines de milliers ;

b) Utilisateurs professionnels − ils doivent intégrer leurs propres systèmes au système informatique eCMR. De nombreuses méthodes d'accès au système doivent pouvoir être utilisées ;

c) Pouvoirs publics − les autorités douanières doivent avoir accès à des centaines de fournisseurs de solutions informatiques.

39. Cette première ébauche d'architecture de haut niveau implique les processus ci-après :

a) Un organisme national devrait valider les solutions informatiques fournies sur son territoire, si elles sont disponibles ou ont fait l'objet d'un accord entre les parties, et communiquer la liste des solutions agréées aux autres Parties contractantes et au marché (à convenir) ;

b) Les mécanismes nationaux d'authentification à appliquer devraient être annoncés à toutes les Parties contractantes. Tout utilisateur du système (expéditeur, transporteur ou destinataire) devrait s'authentifier au moyen de ces mécanismes ;

c) Les fournisseurs de solutions informatiques devraient faire en sorte que seuls les utilisateurs authentifiés puissent accéder à leurs systèmes ;

d) Les transporteurs et les expéditeurs d'un pays devraient pouvoir utiliser les solutions informatiques certifiées dans l'une quelconque des Parties contractantes au Protocole eCMR (qu'elles soient publiques ou privées) ;

e) Les fournisseurs de solutions informatiques devraient proposer des solutions permettant de conserver les données en toute sécurité dans l'environnement de l'utilisateur ou dans un environnement tiers, dans le respect des normes de sécurités requises ;

f) Les solutions informatiques devraient permettre d'ajouter ou d'accepter comme utilisateurs des destinataires, des transitaires, des sous-traitants et des transporteurs successifs qui exercent à l'étranger et qui ont été authentifiés au moyen d'autres systèmes ou mécanismes nationaux d'authentification ;

g) Les diverses solutions informatiques des différents pays et régions devraient être interconnectées et interopérables. Concrètement, cela signifie que, s'il y a 100 fournisseurs informatiques (nombre théorique) pour une année d'opérations dans le système eCMR, il faut alors 4 950 interconnexions pour que toutes les solutions soient interconnectées et interopérables. Dans la pratique, cela représente donc un investissement considérable de la part des fournisseurs de solutions informatiques ;

h) En outre, les douanes ont le droit de demander à consulter les données relatives à la lettre de voiture lorsqu'un camion se présente à la frontière. Le camion peut venir de n'importe où, et la lettre de voiture peut avoir été générée par n'importe quelle solution informatique agréée dans le pays d'où il vient. Concrètement, comme les Parties contractantes à la Convention CMR sont aujourd'hui au nombre de 58, si une solution est trouvée à terme pour la mise en œuvre de la lettre de voiture électronique et si toutes les Parties ratifient le Protocole, alors les autorités douanières de 58 pays devront − si possible, principalement pour des raisons de sécurité − être interconnectées avec au moins 100 solutions informatiques (nombre théorique). Cela signifie que chaque autorité douanière devra, au final, mener à bien 100 projets d'interconnexion si elle souhaite pouvoir consulter les données, soit au total 5 800 interconnexions pour l'ensemble des autorités douanières des Parties contractantes ;

i) Il en sera de même, à terme, pour la police des transports et les tribunaux ;

j) Une question subsiste au sujet des destinataires, puisque ce sont normalement eux qui utilisent des solutions informatiques étrangères, c'est-à-dire des solutions différentes de celle que l'expéditeur et le transporteur ont choisi d'utiliser. Bien entendu, le nombre d'interconnexions que les destinataires doivent effectuer dépendra du nombre de partenaires commerciaux qu'ont les destinataires, du nombre de transporteurs ou de transitaires auxquels ils ont recours, etc. De plus, l'établissement de ces connexions ne prendrait pas autant de temps que dans le cas des douanes, par exemple ;

k) Aujourd'hui, selon des calculs approximatifs, plus de 600 millions de lettres de voiture CMR sont établies chaque année. Il s'agit d'un énorme marché, et le nombre de 100 fournisseurs de solutions informatiques évoqué dans le scénario ci-dessus est très probablement sous-estimé ;

l) Il convient de noter également que l'ONU s'efforce de mettre en œuvre le système de façon adéquate et viable afin d'attirer de nouvelles parties contractantes et de promouvoir la Convention CMR dans d'autres régions (Afrique et Amérique latine) en vue

d'y faciliter aussi le transport routier. Concrètement, cela signifie que le nombre d'utilisateurs devrait, on l'espère, considérablement augmenter dans les années à venir ;

m) Une autre approche à examiner pourrait consister, au lieu de connecter toutes les entités les unes aux autres (ce qui nécessite beaucoup d'efforts, de temps et d'argent), à les interconnecter au moyen d'une plateforme centrale qui jouerait le rôle de système d'échanges de messages. Cette plateforme ne devrait pas avoir accès directement aux données mais, en fonction des requêtes, devrait pouvoir collecter et envoyer des données entre les différentes solutions informatiques et les autorités publiques, c'est-à-dire les douanes et la police. Cette approche permettrait de réduire considérablement les coûts et les délais de connexion, car chaque entité ne devrait se connecter qu'à un seul système, à savoir la plateforme centrale.

Figure : Architecture de haut niveau du futur système eCMR − option 2 (approche centralisée)