Nations Unies ECE/TRANS/SC.1/GE.22/2023/4

# Conseil économique et social

Distr. générale
24 février 2023
Français
Original : anglais

## Commission économique pour l'Europe

Comité des transports intérieurs

### Groupe de travail des transports routiers

**Groupe d'experts de la mise en œuvre de l'eCMR**

**Cinquième session**
Genève, 3-5 avril 2023
Point 3 a) de l'ordre du jour provisoire
**Programme de travail :**
**Concepts et processus proposés pour le futur système eCMR**

# Procédures opérationnelles prévues dans le Protocole additionnel eCMR − environnement numérique*

**Document soumis par le secrétariat et le Groupe d'experts**

## I. Contexte

1. À sa quatrième session, le Groupe d'experts a examiné le document ECE/TRANS/SC.1/GE.22/2023/1, a formulé des observations et a demandé au secrétariat de le réviser ou d'élaborer pour la présente session un nouveau document sur la base de celui-ci, qui rendrait compte des débats tenus par le Groupe. En conséquence, le secrétariat a établi les documents ECE/TRANS/SC.1/GE.22/2023/3 et ECE/TRANS/SC.1/GE.22/2023/4. Les concepts et processus, une fois approuvés, formeront le socle de l'architecture de haut niveau du futur système eCMR.

2. Le Groupe d'experts est invité à examiner les documents officiels établis pour la présente session.

## II. Procédures opérationnelles prévues dans le Protocole additionnel à la CMR − 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.

* Il a été convenu que le présent [document] [rapport] serait publié après la date normale de publication en raison de circonstances indépendantes de la volonté du soumetteur.

C’est pourquoi il est nécessaire d’examiner et d’adopter une série de processus pour adapter cet outil à l’environnement numérique.

## A. Authentification des utilisateurs

4. L’article 3 du Protocole additionnel eCMR est consacré à l’authentification de la lettre de voiture électronique. Cependant, dans le monde numérique, l’authentification des utilisateurs et l’authentification de la lettre de voiture sont deux processus distincts (voir ci-après la partie relative aux signatures électroniques).

5. Afin que les utilisateurs aient confiance dans le système et que toutes les parties prenantes reconnaissent sa validité, les utilisateurs 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.

6. Par conséquent, tous les utilisateurs devraient être authentifiés avant d’utiliser le système, à l’aide de différents moyens convenus par eux-mêmes et par les parties au niveau international (par le Groupe de travail des transports routiers (SC.1) du Comité des transports intérieurs (CTI)), notamment :

a) Système d’authentification national (signatures électroniques, etc.) ;

b) Fournisseur externe ;

c) Base de données internationale des utilisateurs.

7. Chaque Partie contractante devrait 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 conviendrait peut-être 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. Cela pourrait se présenter comme suit :

| 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<br><br>SW − 03 − 00001 | xxxxxx |

## B. Signatures électroniques

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.

10. Les signatures électroniques, si elles sont acceptées, contribueront notamment aux processus suivants :

- Établissement en ligne d’une version finale de la lettre de voiture par les parties ;
- Formulation de réserves par le transporteur et acceptation par l’expéditeur ;

- Transfert du droit de disposition des marchandises ;
- Modifications concernant le destinataire ou communication d'instructions par l'expéditeur ;
- Acceptation de la livraison des marchandises par le destinataire avec ou sans réserves ;
- Contrôle des marchandises et formulation d'observations par les autorités douanières.

11. Il n'existe pas de convention internationale relatives aux signatures électroniques. Cependant, le Groupe a envisagé l'adoption des solutions suivantes, qui faciliteraient ce processus :

a) L'utilisation de 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.

b) La modification du Protocole additionnel eCMR.

Introduire la loi type de la CNUDCI sur les signatures électroniques dans les législations nationales serait le moyen le plus efficace de mettre en place une méthode internationale harmonisée d'utilisation des signatures électroniques, en particulier parmi les Parties contractantes au Protocole eCMR. Toutefois, étant donné que la modification de la législation nationale pourrait prendre beaucoup de temps, en particulier dans les pays qui se sont déjà dotés de lois sur les signatures électroniques mais où celles-ci ne sont pas alignées sur la loi type de la CNUDCI, et compte tenu du fait que les travaux du Groupe visent à disposer le plus rapidement possible d'un cadre international durable pour les lettres de voiture électroniques, la modification du Protocole eCMR pourrait constituer une solution temporaire. L'ajout dans le Protocole eCMR d'une nouvelle disposition générale, qui lierait toutes les Parties contractantes, suffirait à la mise en place des lettres de voiture électroniques. On pourrait par exemple envisager d'ajouter le paragraphe suivant : *Les parties prenantes qui établissent une lettre de voiture électronique utilisent les signatures électroniques émises en application de leur législation nationale. Les Parties contractantes liées par le Protocole eCMR acceptent les signatures électroniques émises par d'autres Parties contractantes.*

## C. Solutions informatiques

12. Une entité souhaitant établir des lettres de voiture électroniques mettra au point une solution informatique à cette fin en s'appuyant sur les spécifications fonctionnelles et

techniques élaborées par le Groupe d'experts et adoptées par le Groupe de travail des transports routiers.

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

- L'entité devrait être une société informatique privée, un expéditeur, un transporteur ou un transitaire ayant les moyens de consacrer du temps et de l'argent au développement de sa propre solution ;
- 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 ;
- Les entités devraient décider si leurs services sont ou non payants ;
- 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. 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/expéditeurs. 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

14. 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.

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

- 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 ;
- 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. Cela évitera également aux expéditeurs, 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. ;
- À défaut d'une autre solution, cet organisme d'agrément pourrait également assurer la sauvegarde ou le stockage sécurisé de toutes les données générées par les différents fournisseurs de services informatiques sur le territoire, de sorte que ces données puissent être utilisées par les tribunaux (du même pays ou d'autres pays), ou en cas de faillite d'un fournisseur informatique ou de perturbation technique, par exemple ;
- 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 ;
- 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 toutes les parties prenantes du système.

16. 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 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

17. Le stockage sécurisé des données entre dans le cadre des fonctions de l'organisme national d'agrément, mais il convient d'y accorder une attention toute particulière car elle est d'une importance capitale pour l'instauration d'un environnement de confiance pour le futur système eCMR.

18. 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.

## F. Cyber sécurité − Sauvegardes

19. 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 :

- Comparaison des données sur demande, pour s'assurer que les données fournies sont les données originales ;
- Sauvegarde en cas de panne technique de la solution informatique ;
- Sauvegarde en cas de faillite du fournisseur informatique ;
- Procédure de secours.

20. Les parties concernées doivent se conformer à la législation applicable en matière de cybersécurité, de protection de la vie privée, etc.

## G. Procédure de secours

21. 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.

22. Le Protocole eCMR ne contient pas de disposition définissant 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. Pour qu'elle soit reconnue et appliquée par toutes les Parties contractantes, la procédure de secours devrait être définie dans le Protocole et avoir force obligatoire. Le secrétariat propose d'élaborer une disposition relative à la procédure de secours, qui sera ajoutée au Protocole.

23. Dans le cadre d'une procédure de secours (en cas d'interruption de l'accès à Internet ou d'autre perturbation technique), au moment de la conclusion du contrat en ligne, le système générera un document électronique non modifiable (format PDF, jpeg, etc.) qui sera envoyé automatiquement à l'adresse électronique des parties visées dans la lettre de voiture (l'expéditeur, le transporteur et le destinataire si ce dernier y consent). Ce document devra comporter un « timbre électronique / Code QR » indiquant la plateforme, la date et le lieu de création du document. Le format de ce timbre électronique ou Code QR pourrait être précisé dans les spécifications techniques du système aux fins d'harmonisation, de façon à ce que toutes les Parties contractantes le reconnaissent.

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

24. 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.

25. Le paragraphe 2 de l'article 4 de la Convention CMR de Montréal dispose ce qui suit :

26. « 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. »

27. Explication possible de l'ajout de l'article 6 dans le texte du Protocole :

28. 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.

29. 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'expéditeur 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

30. Sur la base des débats du Groupe tenus jusqu'à présent, l'architecture de haut niveau ci-après est en train de prendre forme pour le futur système eCMR. Des milliers d'expéditeurs, de destinataires et de transporteurs devraient, d'une manière ou d'une autre, utiliser les services de centaines de sociétés informatiques privées qui fournissent des solutions informatiques pour les lettres de voiture électroniques sur la base des spécifications

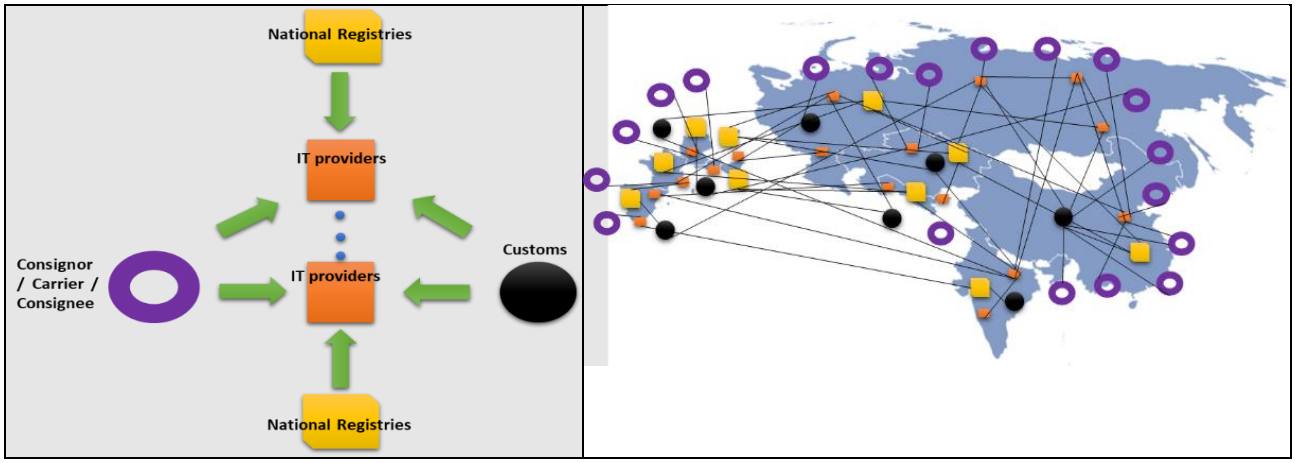
données par la CEE ou en utilisant leurs propres applications. L'interopérabilité entre les différents systèmes devrait être garantie dans la mesure où les normes CEFACT-ONU révisées, sur la base des travaux du Groupe, seront appliquées. L'interopérabilité est la capacité qu'un système, dont les interfaces 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.

31. Les solutions informatiques eCMR reposeront sur la communication entre machines, déclenchée par des événements donnés. C'est pourquoi les interfaces entre les différentes parties prenantes 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.

32. 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. Les solutions informatiques eCMR devraient être configurées de manière à ce que personne ne puisse y accéder depuis Internet, sauf depuis une liste restreinte d'adresses IP qui correspondent aux serveurs principaux des parties prenantes eCMR ayant achevé leurs projets d'interconnexion. Ce mode de fonctionnement réduit considérablement les possibilités de cyberattaques contre les fournisseurs de solutions informatiques eCMR, y compris les attaques par déni de service et les tentatives de mystification visant une partie prenante eCMR.

33. 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**




*Source* : Secrétariat.

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

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

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

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

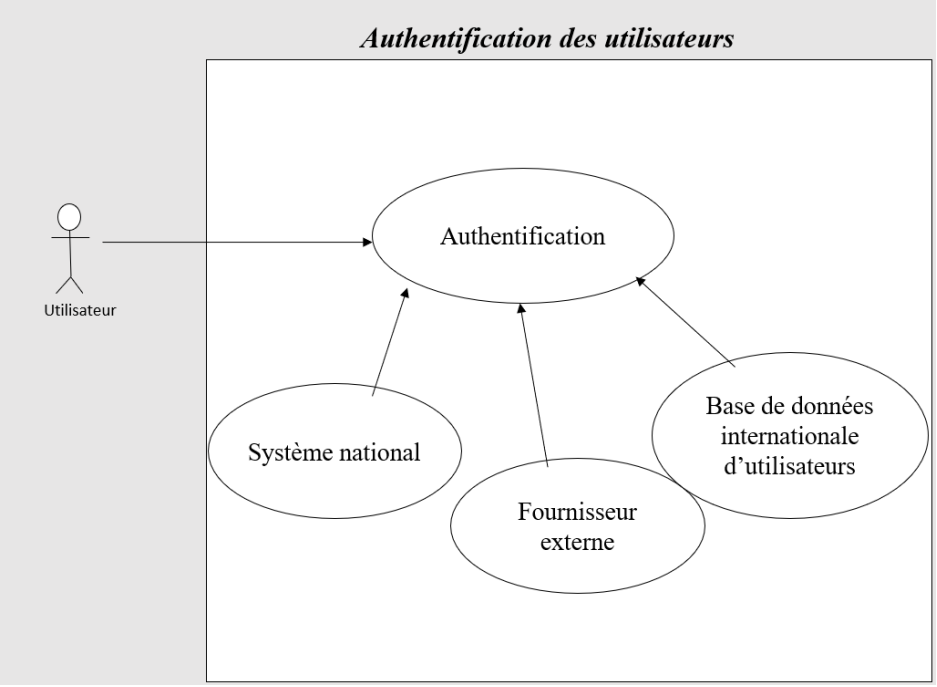
- Un organisme national devrait valider les solutions informatiques fournies sur son territoire et communiquer la liste des solutions agréées aux autres Parties contractantes et au marché (à convenir) ;
- Les mécanismes nationaux d'authentification à appliquer devraient être annoncés à toutes les Parties contractantes. Tout utilisateur du système (expéditeur, transporteur ou destinataire) devrait s'authentifier au moyen de ces mécanismes ;
- Les fournisseurs de solutions informatiques devraient faire en sorte que seuls les utilisateurs authentifiés puissent accéder à leurs systèmes ;
- Les transporteurs et les expéditeurs d'un pays devraient pouvoir utiliser les solutions informatiques agréées dans leur pays (qu'elles soient publiques ou privées) ;
- Les fournisseurs de solutions informatiques devraient veiller à ce que les données soient également stockées dans de bonnes conditions de sécurité par l'organisme national d'agrément ou au moyen de toute autre solution que l'État aura décidé d'adopter, à condition que le choix de cette solution ait été officiellement communiqué à toutes les Parties contractantes. contractantes (à convenir) ;
- 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 ;
- 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 ;
- 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 ;
- Il en sera de même, à terme, pour la police des transports et les tribunaux ;
- 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 ;
- 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 ;

- 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 et de parties prenantes devrait, on l'espère, considérablement augmenter dans les années à venir.

# IV. Analyse des cas d'utilisation (liste indicative)

36. L'analyse des cas d'utilisation donne une vue d'ensemble des échanges (utilisations) entre les acteurs et les utilisateurs.

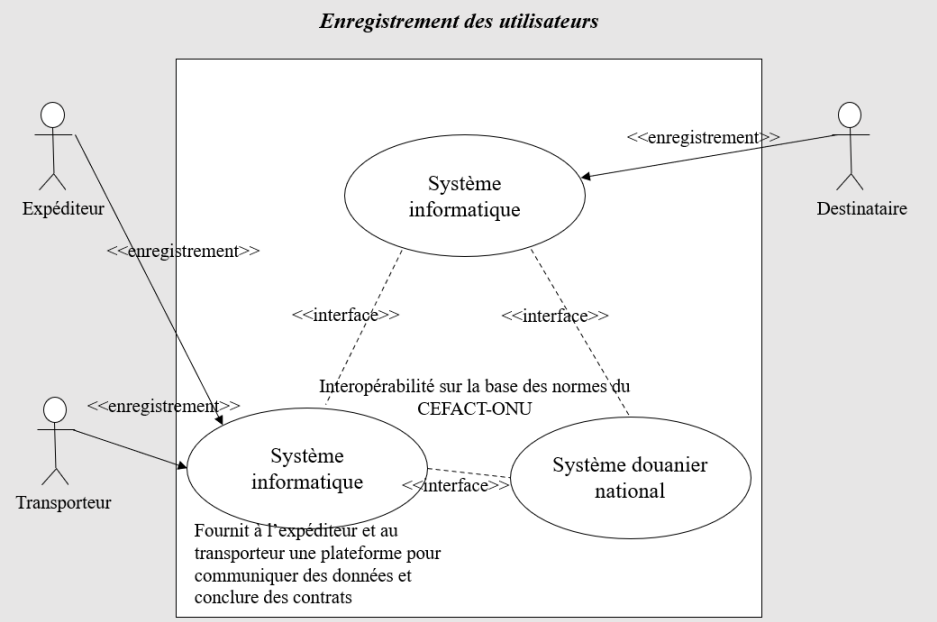
## A. Authentification des utilisateurs




| *Désignation* | *Authentification des utilisateurs par les mécanismes d'authentification nationaux – Cas d'utilisation* |
|---|---|
| Description | Chaque utilisateur devrait être authentifié et produire la preuve de cette authentification en utilisant ses mécanismes d'authentification nationaux. La preuve d'authentification (code unique ?) devrait être utilisée pour s'enregistrer dans les systèmes informatiques. |
| Acteurs | Utilisateurs |
| Objectifs | Seuls les utilisateurs authentifiés peuvent accéder à un système informatique et l'utiliser. |
| Conditions préalables | L'utilisateur est autorisé / authentifié. |
| Conditions a posteriori | L'utilisateur peut avoir accès à n'importe quel système informatique. |

| | |
|---|---|
| Scénario | **Authentification**<br><br>Les systèmes informatiques devraient permettre de vérifier si les informations fournies par l'utilisateur sont valides et enregistrées dans le mécanisme d'authentification national. |
| Autre scénario | **Scénario de secours**<br><br>Si, pour quelque raison que ce soit, il n'est pas possible de procéder à l'authentification, l'utilisateur en est informé. Il doit ensuite rectifier les informations fournies pour obtenir l'authentification. |
| Conditions spéciales | L'accès aux systèmes informatiques eCMR est subordonné à la communication des informations relatives à l'utilisateur |

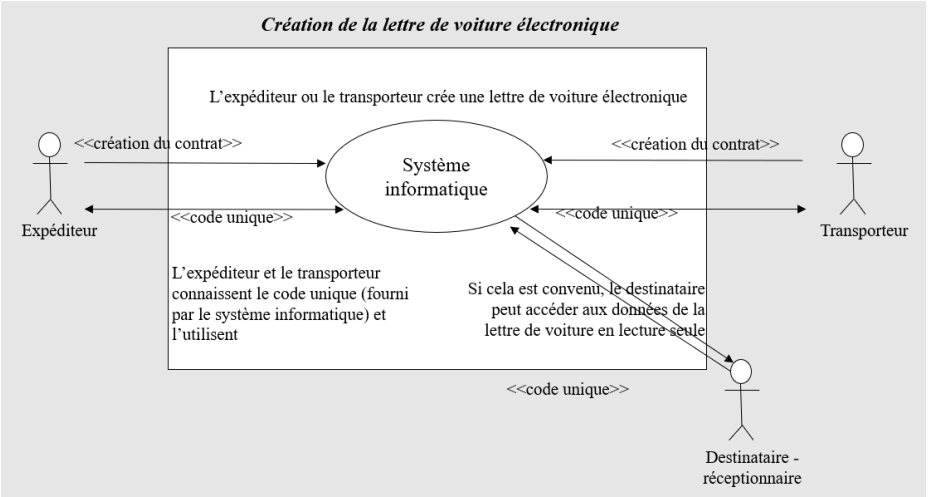
## B. Enregistrement des utilisateurs




| *Désignation* | *Enregistrement des utilisateurs dans les systèmes informatiques* |
|---|---|
| Description | Chaque utilisateur devrait s'enregistrer dans le système informatique de son choix afin de pouvoir soumettre, valider et recevoir des données. |
| Acteurs | Expéditeur, transporteur, destinataire |
| Objectifs | - |
| Conditions préalables | L'utilisateur qui s'enregistre dans un système informatique devrait avoir été préalablement authentifié au moyen de son mécanisme d'authentification national et son identifiant d'authentification unique devrait être communiqué aux fins de l'enregistrement. |
| Conditions a posteriori | Les données de l'utilisateur sont stockées dans le système informatique avec le statut « autorisé ». |

| | |
|---|---|
| Scénario | Enregistrement<br><br>Le système enregistre les utilisateurs au moyen d'une double procédure (par courriel et par téléphone mobile) et les informe des résultats de l'enregistrement. |
| Autre scénario | Scénario de secours<br><br>Si, pour quelque raison que ce soit, il n'est pas possible de procéder à l'enregistrement, l'utilisateur en est informé. Il devrait ensuite rectifier les informations fournies pour pouvoir s'enregistrer. |
| Conditions spéciales | Les utilisateurs pourront mettre à jour leurs informations dans le système informatique et conserver tous les éléments nécessaires à leurs dossiers, à l'établissement de statistiques, etc. |

## C. Création de la lettre de voiture électronique




| *Désignation* | *Création de la lettre de voiture électronique – Cas d'utilisation :* |
|---|---|
| Description | L'expéditeur ou le transporteur crée la lettre de voiture électronique dans le système informatique choisi en y intégrant toutes les informations pertinentes. La partie qui crée la lettre de voiture électronique devrait connaître le code unique des autres partenaires et l'utiliser. Le destinataire, si le transporteur et l'expéditeur en conviennent, devrait également être informé de la création de la lettre de voiture électronique. |
| Acteurs | Expéditeur, transporteur |
| Objectifs | Toute lettre de voiture électronique, délivrée à un expéditeur ou à un transporteur, doit être enregistrée dans le système informatique. |
| Conditions préalables | Les titulaires du contrat de transport doivent être authentifiés et enregistrés dans le système informatique. |
| Conditions a posteriori | Les informations relatives au contrat sont stockées dans le système informatique avec le statut « créée » ou « en cours d'utilisation ». |

| | |
|---|---|
| Scénario | **Création**<br><br>Une fois que la lettre de voiture électronique a été créée par l'expéditeur et le transporteur, l'autre partie en est informée par voie électronique et il lui est demandé de confirmer sa participation, toutes les informations requises par la lettre de voiture eCMR lui étant présentées. |
| Autre scénario | **Scénario de secours**<br><br>Si la lettre de voiture eCMR ne peut pas être envoyée au système informatique par voie électronique ou au moyen des services Web, la partie déclarant la lettre de voiture doit communiquer les informations dès que possible car aucune autre solution n'est prévue. |
| Conditions spéciales | - |