United Nations ECE/TRANS/SC.1/2025/4

Economic and Social Council

Distr.: General
21 August 2025

Original: English

Economic Commission for Europe

Inland Transport Committee

Working Party on Road Transport

120th session
Geneva, 29-31 October 2025
Item 2 (c) (iv) of the provisional agenda
Road Transport Instruments:
Convention on the Contract for the International Carriage of Goods by Road:
Group of Experts on operationalization of eCMR

Group of Experts on operationalization of eCMR Report Part II: Revised operational procedures stipulated by the eCMR Additional Protocol – digital environment*

Submitted by the Group of Experts

I. Background

1. This document forms part II of the report of GE.22. It is based on ECE/TRANS/SC.1/GE.22/2025/2 with the revisions and inclusion of specific comments attributed to various participants that were made at the eighth session of GE.22.

2. The Working Party might wish to adopt the second part of the report of the group of experts that focuses on the analysis of the operational procedures stipulated by the eCMR Additional Protocol and the digital environment in which the future eCMR system(s) will operate.

II. Operational procedures stipulated by the eCMR Additional Protocol – digital environment

3. The eCMR Additional Protocol as well as the digital environment impose a series of new requirements that have to be addressed and agreed among the parties involved in order to ensure an internationally harmonised and sustainable solution on electronic CMR consignment notes. It has to be reminded, follow article 2 paragraph 1 of the eCMR protocol, that what is being described under these concepts is not a mechanism to disseminate the data contained in the future electronic consignment note but rather the development of

* The present report was submitted to the conference services for processing after the deadline so as to include the most recent information.

.

recommended conceptual and functional specifications covering all processes being defined in the CMR Convention that, if followed by eCMR users, will ensure that the electronic consignment note is the legal equivalent of the paper consignment note. In that sense, in addition, a series of processes that the digital world stipulates has to be discussed and agreed.

A. Authentication of the users including eCMR User I.D / eCN I.D.

4. The eCMR Additional Protocol refers to the authentication of the consignment note (Article 3). However, based on group's mandate which is about the operationalisation of eCMR and the high-level architecture of the future eCMR system, the experts identified two authentication requirements:

(a) The authentication of the users ;

(b) The authentication of the final form of the consignment note[1].

5. In order to create trust in the system and ensure that all users mutually recognise its validity, the users should be authenticated while accessing the system. The Group of Experts identified the need of strong authentication for the eCMR "Users" that, through their signatures (or any other electronic authentication method permitted by the national law of the country) of the electronic consignment note, accept their rights and obligations under the CMR Convention. These users comprise the consignor / sender, the carrier (transport operator, successive carrier, subcontractor), and the consignee / receiver.

6. As for the Public Authorities (Customs Authorities, Police, frontier guards, courts and other public entities) their authentication is necessary in a system-to-system context, allowing each party (the Users and the Interested Party) to verify with whom they share eCMR data. These authentication mechanisms will be addressed at the national level.

7. The authentication mechanisms to be used in order to authenticate the users and the electronic consignment notes should be those used already and foreseen in national legislations of the contracting parties to the additional protocol on the electronic CMR.

8. For reasons of transparency and efficiency each of the Contracting Parties to the eCMR Protocol may wish to announce the authentication mechanisms used in their territory ensuring that all are well informed for the official authentication mechanisms used in each country. Each of these national authentication mechanisms generates a unique identification number (id) for their users.

9. While the recommendation is to use existing IDs according to national legislation (e.g. Tax ID, EORI numbers, Commerce Register ID), in order to identify each user, if those are unavailable or decided otherwise, the IT solutions providers should use an algorithm to generate globally unique eCMR user IDs, such as "{User-Country-Code}-{UUIDv4 generated ID}" (UUIDv4 generated IDs are randomly generated IDs with extremely very low chances of collision/duplicate used in many other IT systems), eg: "CH- 80294bd7-b51d-415d-acb7-646c037f7397".

10. Similarly as for eCMR User ID, eCN ID may need to be issued by a wide variety of disconnected and uncoordinated eCMR users, therefore, if no national requirements exist already for numbering electronic Consignment Notes, eCMR IT Solution Providers may need to implement a simple algorithm to generate globally unique eCN IDs, such as "{Initiating-User-Country-Code}-{Sequential-Number}-{Unique IT Solution Code}, eg: "TR-0001521-XBL".

[1] eCMR protocol / Article 3 / Authentication of the electronic consignment note
1. The electronic consignment note shall be authenticated by the parties to the contract of carriage by means of a reliable electronic signature that ensures its link with the electronic consignment note. The reliability of an electronic
signature method is presumed, unless otherwise proved, if the electronic signature:
(a) is uniquely linked to the signatory;
(b) is capable of identifying the signatory;
(c) is created using means that the signatory can maintain under his sole control; and
(d) is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

B. Electronic Signatures

11. Article 3 of the eCMR Additional Protocol makes specific reference to the use of electronic signatures for the authentication of the electronic consignment notes even though para. 2 of the same article mentions that the consignment note may also be authenticated by any other electronic authentication method permitted by the law of the country.

12. The electronic signatures or any other national authentication mechanism would be used to authenticate the following processes (non-exhaustive list):

(a) Authenticating the final form of the consignment note online by the parties (Consignor / Carrier);

(b) Authenticating Carrier's reservations while loading the goods and Consignor / sender 's acceptance;

(c) Authenticating the transferring of the right of disposal of the goods. Who has the right of disposal of the goods at certain points of a journey while there is no second copy of the paper consignment note to prove it, it is a major function of the CMR Convention. This is one of the main functions that a future eCMR system should accommodate and serve. Every time that this event is taking place (please see ECE/TRANS/SC.1/GE.22/2023/3) an authentication should be warranted;

(d) Authenticating the Consignor / Sender's making of changes regarding the consignee / receiver or providing new instructions. This event is directly connected with the liability of the carrier, and it has to be ensured who provides those new instructions;

(e) Authenticating the proof of acceptance or not of the goods by the consignee with or without reservations. As described in ECE/TRANS/SC.1/2025/3, the consignee has to fulfil two steps process concerning the receipt of the goods: a. the proof of delivery and b. the confirmation of acceptance or not of the goods. For the first one the consignee has already authenticated themselves in a system. For the confirmation of acceptance, the consignee requires to authenticate themselves in order to finally accept the goods with or without reservations or not accepting them;

(f) Authenticating customs authorities checking the goods and providing official annotations or courts requesting data. This applies if customs officers are required to authenticate themselves before accessing any data - it depends on the design of the high-level architecture and on how in the end the customs authorities will be interconnected -. Since it seems inefficient for customs authorities to register and authenticate their users with hundreds of IT providers that generate eCMRs in order to receive this information, ad hoc most probably this approach will not be followed;

13. There is no international convention on electronic signatures to be ratified by the UN member States. There are solutions discussed in the group that would facilitate towards a harmonised approach, however, it should be noted that the group acknowledges that there is no need to have an "internationally harmonised approach" on electronic signatures in order for future eCMR system(s) to operate and current practices / national laws are efficient enough.

C. Information technology Solutions

14. The scope of the group is to finalise the conceptual and functional specifications of the future eCMR system(s). Those specifications following article 2 of the eCMR protocol should focus on the digitalisation of the paper CMR consignment note including the events / processes being described in the CMR Convention. Only then the CMR Convention will apply in full also in the digital world and the electronic CMR will be "the equivalent to the consignment note referred to in the convention and shall therefore have the same evidentiary value and produce the same effects as the consignment note".

15. The secretariat is working closely with the UN CEFACT secretariat in order to revise, if needed, the existing eCMR data standards, ensuring interoperability among the different eCMR systems in the future. All specifications and the data standards will be offered as UN

public goods to the private sector for immediate use and cannot be mandatory. However, when adopted by the UN intergovernmental bodies, UN ECE will ask governments to encourage the private sector to follow those specifications and standards since they ensure the implementation of the CMR Convention in the electronic world.

16. The article 5 of the protocol however mentions that the parties should agree on the procedures clearly implying that all parties should agree and use the same procedures since if they agree and don't use them the result would remain the same. As we described in previous document, the carriers are thousands. They cannot really sit down and agree on those processes. This is the great value that this group of experts brings to the private sector and the public authorities, contributing to the rapid implementation of eCMR.

17. Indeed, UN ECE Inland Transport Committee cannot impose those functional specifications to anyone. However, the Committee has the obligation to inform all users, Governments and Private Sector, that nobody has the right to advertise in their website that they have developed a solution on eCMR that follows the UN protocol or specifications when in practice they do not. We must protect the CMR Convention and its electronic version, the eCMR, from such practices because by doing that we are actually protecting the actual users of the Convention, the Carriers.

18. By following the functional specifications that the Group worked on, the users will be sure that:

(i) The electronic consignment note produced will have *the same evidentiary value and produce the same effects* as the paper *consignment note* (article 2, para 2, protocol).

(ii) There is agreement among the contracting parties to the Protocol on the *manner in which the party entitled to the rights arising out of the electronic consignment note is able to demonstrate that entitlement (article 5)*.

(iii) There is agreement among the contracting parties to the Protocol on the procedures for supplementing or amending the electronic consignment note including the assurance that the electronic consignment note retained its integrity.

(iv) Therefore, while en route customs authorities will recognize this electronic consignment note as an original one and in any future court case, courts will recognize the authenticity of their electronic consignment note which was generated based on the convention.

19. In practice, acknowledging also the fact that already some applications exist declaring that generate eCMRs without of course following the functional specifications developed by the Group, a period would exist that users have to choose between applications that were developed following the UN specifications and others that they did not. Maybe UN should consider establishing a kind of "certification" process, most probably an automated one, where the IT applications developed following the functional specifications would be evaluated with conformance tests. Those applications successfully passing the conformance tests would be awarded with an emblem to be uploaded on their web site, proving compliance with the UN specifications. Maybe UN could have also a web site where all those "certified" applications are listed for users' convenience.

20. The below principles should be followed regarding the development of these electronic solutions:

(a) The entity should be anyone interested in developing an electronic solution. Private or Public entity;

(b) All entities are free to choose any technology they wish;

(c) The entities should decide if they have or not to charge for their services;

(d) It would make sense in order to ensure integrity of data, that the IT provider should not have reading / amending access to the CMR data being generated by the system they have developed when this system is publicly available unless this is required due to operational reasons with the consent of the system users. If the system has been developed

by the transport/shipper company itself for their own business, then they should have access to data based on the rules apply for the carriers/senders. The IT provider should not permit to sell or exchange the data being generated in their platform for profiting or any other reasons including competition etc. All these terms should be further reviewed with practices / national laws that apply regarding data protection etc.

D. National Certification Body

21. The group discussed and agreed about the need to have a national certification body established. The main reason for the existence of such a body would be to make sure that compliance exist with the recommended functional specifications/ UNCEFACT Standards and the CMR Convention applies.

22. The idea is that a national body (bodies) should be officially nominated by the governments with the following obligations / tasks:

(a) Provide the recommended conceptual and functional specifications including the UNCEFACT standards as agreed on the level of ITC/SC.1 to be used for the development of platforms that generate eCMRs;;

(b) Validate the electronic solutions developed based on those specifications (independently of the technology used) and provide the official list of IT solutions recognized to be used for the generation of eCMRs in its territory (as well as recognized by the Contracting Parties of the eCMR Protocol). This will also protect the senders, carriers and consignees from solutions that do not comply with the CMR Convention and the eCMR recommended specifications especially vis a vis a court, a damage of the goods etc;

(c) Monitoring the use of eCMR services in its territory and report cases on disruptions / monopolistic or oligopolistic practices etc. which are against the eCMR principles of operations;

(d) Temporary/permanently withdraw validation to generate eCMR from IT solutions when such practices as mentioned above have been observed while informing all users of the system for such temporary / permanently withdraw of validation.

23. A national certification body with such mandate would create trust in the system and the mutual recognition required in order for such an international electronic system to function without interruptions. Each Government should decide which body / organization should be nominated to perform these tasks. In that sense it could be the chambers, the national road transport association, accreditation bodies, a new body etc. The government though should have the obligation to officially announce this body including its tasks and obligations. It shall be noted that this body should not be the body that authenticates the users (consignor, carrier consignee) which is a different function.

24. Governments are strongly recommended to identify and declare such a certification body, but it is, by no means, an obligation that they have to follow, and it is their prerogative to decide upon.

E. Safe storage of data

25. The group discussed and identified a list of challenges that relate to the safe storage of data. These challenges could be summarised as follows:

(a) An assurance that the electronic consignment note retains its integrity and that a manner should exist that the party entitled to the rights arising out of the electronic consignment note is able to demonstrate that entitlement are provisions stipulated in article 5 to the eCMR protocol. In that sense, the experts identified a possible challenge with the storage of the original data. The CMR applies when something goes wrong, and the parties need to solve their disputes at the court. The courts therefore (Articles 31-33 to the CMR Convention) must have access to the original data;

(b) CMR data includes commercially sensitive information that should not be disseminated in one hand or be concentrated by a minority of IT companies. In that sense, as a generic comment, monopolistic / oligopolistic practices should be avoided in order to protect the data and therefore system's integrity, but this is something that the market should regulate and not the group of experts. However, in a free-market environment where a company can be merged with another from a neighbouring country or acquire another company from a neighbouring country or just establish branches everywhere, it is almost impossible for such practices to be avoided;

(c) In order to ensure the availability of the original data, even in case an eCMR technology provider goes bankrupt, the original authenticated version of each eCMR should be shared with each of the users of the eCMR;.

(d) The number of years of safe storing the data might also require to be harmonised. The group, if such a requirement is agreed, tentatively suggests that the eCMR data should be kept for a period of ten years after its generation for future use by any entity, public or private.

F. Information security policy

26. Cyber security is also connected with the above-mentioned topic and with the trustful environment that this IT solution should operate. The issue of integrity of the particulars is strictly connected with trust in the system. The future eCMR system should first keep a strict – not changeable – sequence of events based on the days and time that events take place. For instance, regular backups of data by the private IT solutions should take place. However, it should be clarified where these backups will take place etc. This will serve several purposes:

(a) If requested, a comparison of data to ensure that original data is provided;

(b) Back up in case of technological failure of the IT solution;

(c) Back up in case of bankruptcy of the IT provider;

(d) Fallback procedure.

27. The parties involved should comply with accepted industry best practices on Information Security. These practices ensure the security of eCMR systems and cover areas such as security governance, infrastructure security (network, endpoint, physical, backup and restore), application security (log management, access management, encryption), employee training, incident response management, application audits and compliance (as per article 25 above.

28. The parties involved must comply with applicable cyber security, privacy etc. legislation.

29. The protocol stipulates (article 4, para 3) that *"the procedure used for supplementing or amending the electronic consignment note shall make it possible to detect as such any supplement or amendment to the electronic consignment note and shall preserve the particulars originally contained therein*". Also, Article 4, para 2 mentions "*The procedure used to issue the electronic consignment note shall ensure the integrity of the particulars contained therein from the time when it was first generated in its final form*". It is therefore clear based on the protocol that an "*original electronic consignment note plus amendments chronologically listed*" approach should be followed concerning safe storing of the data instead of a "*final electronic consignment note when journey finalised plus amendments chronologically listed"* approach. Clearly the protocol suggests an approach which is focused on the *final form of the electronic consignment* initially authenticated by the consignor and the carrier before the journey starts contrary to the paper world practice where the final paper consignment note is being stored when the journey has been finalised having all stamps / signatures included.

G. Fallback procedure

30. In an electronic environment it is difficult to speak about the loss or absence of the consignment note since there is always the possibility to access the document / data online, in the initial platform where it was generated.

31. There is no provision in the eCMR Additional Protocol that speaks about a fallback procedure. However, article 5 para 2-point f mentions that that the parties should agree on "*procedures for the possible replacement of the electronic consignment note by a consignment note issued by different means*" implying a fall-back procedure. The fallback procedure is of paramount importance for the operations of the future eCMR system when for some reasons the system does not work as designed.

32. It is very important to define the cases when a fallback procedure will be required and then to define the fallback procedure used. The following table consolidates the different cases where a fallback procedure might be required with a suggested procedure to be followed.

Cases where a fallback procedure might be required	**Fallback procedure to be followed**
Processes for initiating an eCN / generating a final form of eCN / authenticating the final form of eCN :	1. Use of paper consignment note
a. Do not function or generate errors	a. System should provide feedback with guidelines on how to solve the issue b. Possibility for the users to automatically contact the administration of the system seeking a solution c. Use of another system / IT solution
b. No access due to internet / electricity cuts	b. Use of paper consignment note
In cases of issues en route for instance no internet at a specific border point, police device does not work, consignee does not have internet access to retrieve the unique code (for example, QR code, bar code) sent to perform the proof of delivery process etc	When the final form of the electronic consignment note has been authenticated then: a. A non-changeable pdf should be generated and sent to all users involved b. If mobile number of carrier is provided then a QR code will be sent to be stored in his/her wallet similar to boarding passes, c. If the IT solution provides mobile application then the whole information with the QR code will be stored in the mobile application, d. Advanced eCMR information will be shared to all customs en route and destination when the journey starts if the customs are connected to the IT solution, if the carriers accept to include the itinerary that he will follow (always able to change it en route if required). Customs, will be able to perform risk analysis well before truck arrives, already stored in their system when the truck arrives e. Customs should accept paper CMRs

	f. The consignee should be able to receive the unique code in both his/her email and mobile phone using a two-fold identification.

H. Explanation on Article 6 - Additional obligations of the carrier when using electronic consignment notes (Article 6, para. 1, eCMR)

33. This specific provision was literally copy pasted from Montreal CMR Convention of 1999 which establishes airline liability in the case of death or injury to passengers, as well as in cases of delay, damage or loss of baggage and cargo. It unifies all of the different international treaty regimes covering airline liability that had developed haphazardly since 1929. Secretariat will try to see if there is any info on the reason for including Article 6, para. 1 eCMR in the explanatory memorandum of eCMR.

34. Article 4, para. 2 of Montreal CMR Convention mentions: “Any other means which preserves a record of the carriage to be performed may be substituted for the delivery of an air waybill. If such other means are used, the carrier shall, if so requested by the consignor, deliver to the consignor a cargo receipt permitting identification of the consignment and access to the information contained in the record preserved by such other means.”

35. This is a possible explanation as to why Article 6 eCMR was included in the text of the protocol.

36. In document TRANS/SC.1/2002/1, page 3 which was submitted by UNIDROIT (February 2002) mentions about the specific paragraph: “this paragraph is taken from Article 4.2. of the Montreal Convention. Article 4 provides that: any other means which preserves a record of the carriage to be performed may be substituted for the delivery of an air waybill” but in order to avoid electronic “imperialism”, it requires the carrier to issue a paper receipt when the cargo is handed over”. Also, in the same document a questionnaire was listed where the last question was referring to this specific provision asking the Governments if they agree with its inclusion in the protocol.

37. In the draft of 2003, there were Article 7 with the title right of disposal. The article was mentioning: (1) where an electronic consignment note is issued, the sender’s right of disposal of the goods shall cease to exist as soon as the carrier transfers the access key to the consignee in accordance with Article 5. It also includes the following remark: “As the electronic consignment note is not issued in more than one copy, the requirement to produce the first copy does not apply. By allocating a key which enables only the person having the right of disposal to enter instructions on the consignment note and it is ensured that it is only the person having the right of disposal that is entitled to enter an instruction on the consignment note”.

III. eCMR high level architecture

38. As elaborated in the introduction to the eCMR, the final objective of the computerization of the CMR Convention encompasses the computerization of the whole CMR Consignment note life cycle from distribution and issuance, to loading, delivery and archiving, reflecting all rights and obligations that the CMR Convention stipulates and it should, ultimately, be aimed at replacing the current paper CMR consignment note without changing the basic philosophy of the CMR Convention.

39. In the future, the generators of the eCMR consignment notes – senders/consignors and carriers and when required consignees- will be able to use any - certified IT solution to generate their electronic consignment notes. With use of the United Nations Centre for Trade Facilitation and Electronic Business (UN CEFACT) data standards as revised, interoperability of all electronic solutions would be warranted. These electronic solutions following the recommended conceptual and functional specifications agreed on ECE level will be able to accommodate all electronic services required for the electronic consignment

notes covering all needs, rights, obligations, instructions, reservations and processes stipulated by the CMR convention. This is why the electronic consignment note could be recognised as the legal equivalent of the paper consignment note.

40. The Group while considering possible high-level architectures of the future eCMR systems, identified and listed several challenges to be solved by following practical approaches and coordination between the Governments, the public authorities and the private sector. The UNECE platform / SC.1 should be used whenever is required to negotiate and agree on high level issues seeking harmonisation and possibly further amending the recommended conceptual and functional specifications. The challenges identified are as follows:

(a) In the future, hundreds of applications / technological solutions will exist on National level that would generate eCMRs servicing thousands of carriers and consignees of this World. These applications / technological solutions could have been developed by anyone interested in implementing the eCMR protocol including private and public entities. These IT solutions should be able to include / accept as users of their IT solutions consignees, freight forwarders, sub-contractor and successive carriers that are operating abroad, users that have been authenticated by other national authentication systems / mechanisms, and exchange eCMR data with users that may be using different eCMR IT solutions.

(b) Facilitation of International Road transport counts on seamless and efficient border crossings operations. The CMR Convention serves that role with the use of paper consignment notes since 1956. Read access to data by the public authorities is a requirement that Governments in coordination with the private sector should work to ensure.