United Nations ECE/TRANS/SC.1/GE.22/2023/4/Rev.1

Economic and Social Council

Distr.: General
26 April 2023

Original: English

Economic Commission for Europe

Inland Transport Committee

Working Party on Road Transport

Group of Experts on the Operationalization of eCMR

Sixth session
Geneva, 5–7 July 2023
Item 3 (a) of the provisional agenda
Programme of work:
Proposed conceptual and functional specifications of the future eCMR system

Operational procedures stipulated by the eCMR Additional Protocol – digital environment

Revision

Submitted by the Secretariat and the Group of Experts

I. Background

1. At its fifth session, the Group of Experts discussed ECE/TRANS/SC.1/GE.22/2023/3 and ECE/TRANS/SC.1/GE.22/2023/4, provided comments and requested the secretariat to revise these documents based on the discussions of the Group. The concepts and processes when agreed will form the basis of the high-level architecture of the future eCMR system.

2. The Group of Experts is invited to discuss the formal documents prepared for this session.

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 international and sustainable solution on electronic consignment notes. It has to be reminded that what is being described under these concepts is not a mechanism to disseminate the data contained in the electronic consignment note but rather the development of a validation mechanism which makes the electronic consignment note the legal equivalent of the paper consignment note. In that sense a series of processes that the digital word stipulates has to be discussed and agreed.

A. Authentication of the users

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:

- The authentication of the users
- The authentication of the consignment note (or of the final form of the consignment note).

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. Authentication of the users automatically means acceptance by the users of the rights and obligations that the CMR Convention stipulates. The group defined as users the following:

- Consignor / sender
- Carrier / Successive Carrier / Freight forwarder / Sub/Contractor
- Consignee / receiver
- Customs Authorities
- Police / frontier guards
- Courts and other public entities

6. 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.

7. For reasons of transparency and efficiency each of the contracting parties 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.

8. It is understandable that knowing the unique national I.D. of each user it would be very useful when generating an electronic consignment note because it would save time and it would increase the convenience of the systems to its users. However, knowing the national I.D. of each user when there will be thousands of importers, exporters and carriers using the systems will be almost impossible. A proposal could be to provide some generic guidelines on how to develop an international list of identification numbers connected with the national I.D. provided by the authentication mechanisms to be followed by all IT solutions internationally further facilitating the use of the system. These generic numbers, if agreed, will be automatically generated by the IT solutions every time a new user is registered in a system. However, afterwards, this unique number could be used by the user in every certified solution generating eCMRs. For instance, such guidelines could be the following:

International I.D. system	National id based on authentication mechanism
Country – IT Solution id – id number	xxxxxx
SW – 03 - 00001	

B. Electronic Signatures

9. 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. The

electronic signatures or any other mechanism used are not referring to “usernames’ and “passwords”.

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

- Authenticating the final form of the consignment note online by the parties (Consignor / Carrier)
- Authenticating Carrier’s reservations while loading the goods and Consignor / sender ‘s acceptance
- 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 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.
- 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.
- Authenticating the p roof of acceptance or not of the goods by the consignee with or without reservations. As described in ECE/TRANS/SC.1/GE.22/2023/3, the consignee has to fulfil two steps concerning the receive of the goods: a. the proof of delivery and b. the proof of acceptance or not of the goods. For the first one the consignee has already authenticated themselves in a system in order to receive the unique code required to perform the two-fold verification. For the proof of acceptance, the consignee requires to authenticate themselves in order to finally accept the goods with or without reservations or not accepting them.
- Authenticating customs authorities checking the goods and providing comments or courts requesting data. This applies if customs officers 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 customs authorities to register and authenticate their users with hundreds IT providers that generate eCMRs in order to received ad hoc this information, most probably this approach will not be followed.

11. There is no international convention on electronic signatures. However, there are solutions discussed in the group that would facilitate towards a harmonised approach. The group suggests the use of UNCITRAL Model Law on Electronic Signatures.

> The Model Law on Electronic Signatures (MLES) aims to enable and facilitate the use of electronic signatures by establishing criteria of technical reliability for the equivalence between electronic and hand-written signatures. Thus, the MLES may assist States in establishing a modern, harmonized and fair legislative framework to address effectively the legal treatment of electronic signatures and give certainty to their status. The MLES is based on the fundamental principles common to all UNCITRAL texts relating to electronic commerce, namely non-discrimination, technological neutrality and functional equivalence. The MLES establishes criteria of technical reliability for the equivalence between electronic and hand-written signatures as well as basic rules of conduct that may serve as guidelines for assessing duties and liabilities for the signatory, the relying party and trusted third parties intervening in the signature process. Finally, the MLES contains provisions favouring the recognition of foreign certificates and electronic signatures based on a principle of substantive equivalence that disregards the place of origin of the foreign signature. The Model Law is accompanied by a Guide to Enactment, which provides background and explanatory information to assist States in preparing the necessary legislative provisions and may guide other users of the text.

C. Information technology Solutions

12. An entity interested in generating electronic CMRs will make use of the functional and technical specifications adopted by UNECE Inland Transport Committee following proposal by the Working Party on road transport (SC.1) in order to develop an electronic solution that generates the electronic consignment notes ensuring that the CMR Convention and its protocol applies.

13. The experts should decide if the application of the functional and technical specifications is mandatory or not. 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 not use them the result would remain the same. There are several pros and cons connected with both approaches. Specifically:

- If the specifications are mandatory, then the users know that independently which IT solution they use:
    - 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)
    - 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*,
    - 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,
    - 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,
    - Making the specifications mandatory though, creates another obligation from the part of the states, this of certifying each IT solution. The ideal scenario is that the Governments will declare a national body that certifies the compliance of those solutions with the specifications. Another not so ideal approach would be that this certification process is facilitated by creating a central self-certifying platform (if by UN it has to be checked with legal services) where users self-declaring that their IT solutions are in conformance with the functional and technical specifications. Conformance tests might also be provided to check these solutions. The certified users will acknowledge in the case that in any future sample testing, incident vis vis courts etc they are risking losing this certification accepting any reputation damage from this act.
- If the specifications are not mandatory, then anyone practically can declare that can generate electronic CMR consignment notes. Any solution that exists today will continue to operate as is. This would facilitate the current status which is not ideal for the operations of eCMR simply because cannot be recognised who is applying the convention and who is not.
    - If a hybrid model will be followed with IT solutions following the specifications and others that are not, then there should be at least a mandatory declaration from their side in their web site “in compliance with UN eCMR specifications” and “not in compliance with UN eCMR specifications”.
    - Like that the users will be able to know and decide if they wish to use these platforms or not.

- For customs authorities will be even more difficult because practically the work done on the preparation of the functional and technical specifications is done for the public entities to mutually recognize these solutions, trust them and start using them internationally. If a hybrid model exists then Customs authorities will be obliged to use only those IT solutions that are in compliance with the technical specifications,
- If the model of the central interconnection platform will be used for the high-level architecture concerning the connection of the customs authorities, then it makes the situation even simpler since only certified IT solutions will be permitted to interconnect with such central platform and provide data to customs authorities.

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

- The entity should be anyone interested in developing an electronic solution. Private or Public entity.
- All entities are free to choose any technology they wish as long as they follow the specifications provided to them ensuring that the CMR Convention applies. Again, if the mandatory model on the specifications will be followed then the IT solution should be validated / certified by the National Validation Body / central platform etc
- The entities should decide if they have or not to charge for their services,
- 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. 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.

D. National Validation Body

15. The group discussed without having reached an agreement yet about the need to have a national validation body established. The main reason for the existence of such a body would be to make sure that compliance exist with the specifications and the CMR Convention applies. The group still examines this idea and other options that could be established. However, if the use of a validation body is proposed then Group suggests that then the validation procedures (conformance tests?) should be agreed.

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

- Provide the technical specifications as agreed on the level of ITC/SC.1 to be used for the development of platforms that generate eCMRs;
- Validate the electronic solutions developed based on those technical 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. This will also protect the senders, carriers and consignees from solutions that do not comply with the CMR CMR Convention and the eCMR specifications especially vis a vis a court, a damage of the goods etc.
- If no other solution found, this validation body could also play the role of backup / safe storage of all records generated by the different IT solutions in its territory for future use by courts (of the same or different countries) and in cases of bankruptcy of IT providers or technological disruptions etc.
- Monitoring the use of eCMR services in its territory and report cases on disruptions / monopolistic or oligopolistic practices etc. which are again the eCMR principles of operations.

- 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.

17. A national validation body with such mandate would create trust in the system and the mutual recognition required in order for such international electronic system to function without interruptions. Each Government should decide which body / organization should be nominated to perform these tasks. In that sense 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.

E. Safe storage of data

18. The safe storage of data is connected with the functions of the national validation body, but special reference should be made since it is of critical importance for the trustful environment that should be developed for the future eCMR system.

19. 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 monopolistic / oligopolistic practices should be avoided in order to protect the data and therefore system's integrity. 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. Most probably the group cannot provide a solution except of general recommendations and these kinds of issues should administered at a national level.

20. The number of years of safe storing the data should be harmonised. The group tentatively agreed 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. Cyber security – Back ups

21. Cyber security is also connected with 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:

- If requested, comparison of data to ensure that original data is provided,
- Back up in case of technological failure of the IT solution
- Back up in case of bankruptcy of the IT provider
- Fallback procedure

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

23. 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 "*original electronic consignment note plus amendments chronologically listed*" approach should be followed concerning safe storing of the data instead of "*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 were the final paper consignment note is being archived when the journey has been finalised having all stamps / signatures included.

G. Fallback procedure

24. 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.

25. There is no provision in the eCMR Additional Protocol as such 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.

26. It is very important to define the cases when 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 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 mob 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 accepts 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 be fore 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 2 fold identification.

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

27. 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. 1eCMR in the Explanatory memorandum of eCMR.

28. Article 4, para. 2 of Montreal CMR Convention mentions:

29. 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.

30. Possible explanation why Article 6 eCMR was included in the text of the protocol.

31. 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.

32. 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 description

High-level description of the eCMR system

33. 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, issuance 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.

34. The generators of the eCMR consignment notes – senders/consignors and carriers and when required consignees- will be able to use any validated platform / electronic solution to generate their electronic consignment notes. With use of UN CEFACT data standards as revised through the group of experts, interoperability of all electronic solutions would be warranted. These electronic solutions following the specifications agreed on UNECE level will be able to accommodate all electronic services required for the electronic consignment notes covering all needs, rights, obligations, 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.

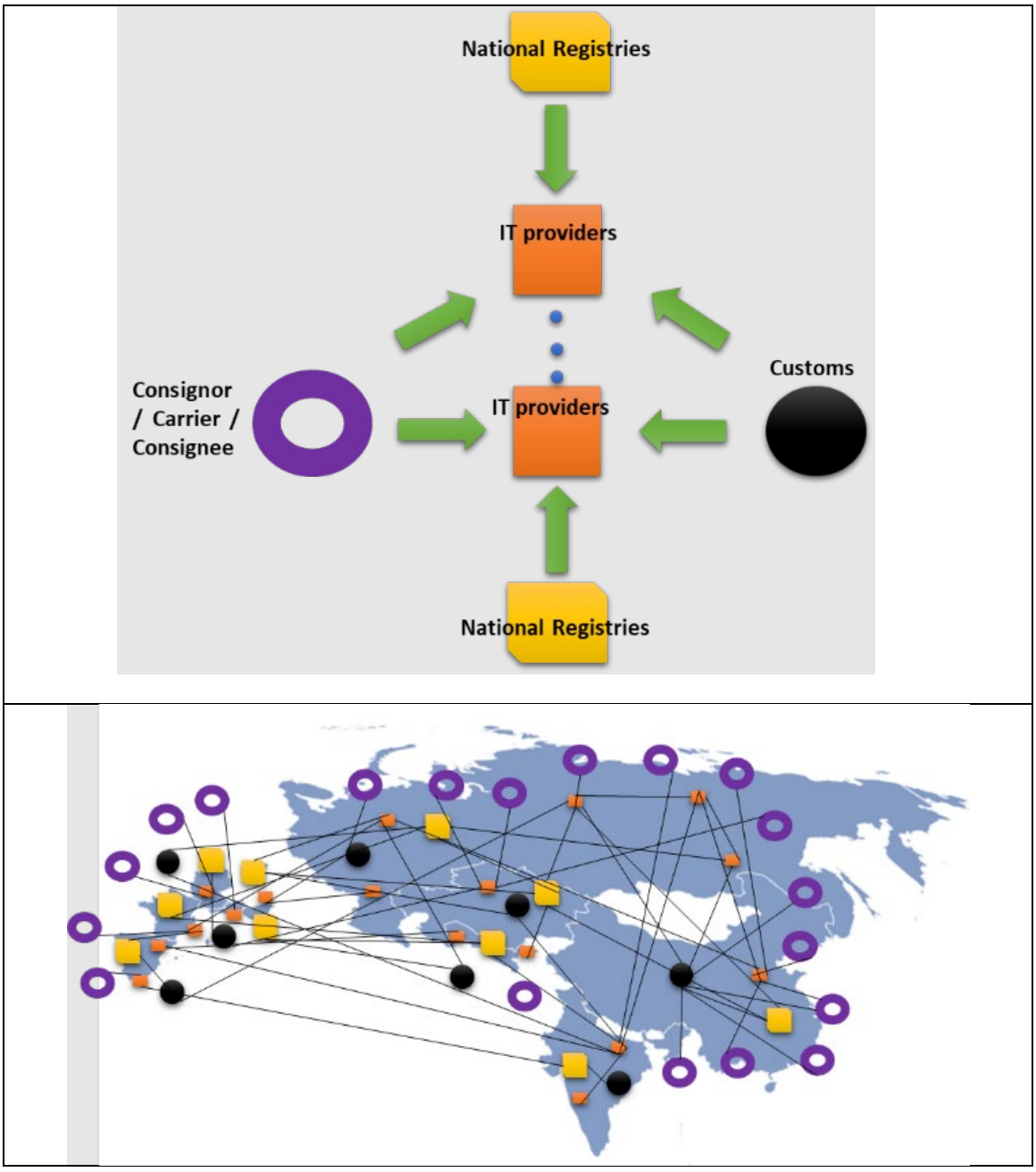
35. Based on the discussions of the group, the following high-level architecture of the future eCMR system is being formed. It should be recognised that in the future thousands of Consignors, Consignees and Carriers should somehow use the services of hundreds of IT solutions for eCMRs based or not (to be decided) on the specifications provided by UNECE .Interoperability between the different systems should be guaranteed since the revised - based on the group's work-, UNCEFACT standards will be used. Interoperability is a characteristic of a system, whose interfaces are comprehensively detailed, to work with other systems, at present or in the future, in either implementation or access, with full compatibility.

36. The eCMR IT solutions will be based on machine to machine communication triggered by specific events. Therefore, the interfaces between the various eCMR users must be clearly defined to ease the interconnection between the systems. Also, in order to further facilitate this interconnection, the interfaces should be based on the latest globally adopted communication standards.

37. However, even if the right standards are in place, an interconnection project should be required and initiated. The eCMR IT solutions systems shall be designed and documented to facilitate the interconnection with different parties, including the upgrade to new versions. Ease of connectivity minimizes the costs on the IT solutions service desk to assist parties in interconnecting their systems to the eCMR IT solutions.

38. On the other hand, the Customs Authorities of the Contracting Parties in order to have on demand access to the information of the eCMR, they have to have access (to be interconnected) to the hundreds of IT providers.

Figure high level architecture of eCMR future system option 1 (decentralised approach)



Source: Secretariat

39. Practically we do have three types of users:

- Occasional users – add comments to the electronic consignment note using certain type of links sent to occasional users. Then the occasional users should visit the relevant web sites. However, question marks still exist for the authentication of those users and registration to the IT solutions based on the authentication provided. Still those occasional users should be hundreds of thousands.
- Professional users – need to integrate their own systems with the eCMR IT solution. Need many methods to access IT solution.
- Public authorities – customs authorities need to have access to hundreds of IT providers.

40. The processes that this first very draft high-level architecture implies are:

- If available or agreed among the parties, a national body should validate the IT solutions provided in its territory and announce the list of validated solutions to other contracting parties and the market (to be agreed),
- The national authentication mechanisms to be followed should be announced to all contracting parties. Any user of the system (consignor, carrier, consignee) should be authenticated by using these national authentication mechanisms.
- The IT solutions should ensure that they permit only authenticated users in their systems.
- The Carriers and the Consignors of a country should be able to use the IT solutions validated in their country (private or publicly available).
- The providers of the IT solutions should make sure that the data is also safely stored at the national body that validates the IT solutions or any other solution that the Government has decided to follow as long as this solution has been formally communicated to all contracting parties (to be agreed).
- The 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 and have been authenticated by other national authentication systems / mechanisms.
- The different IT solutions from different countries and regions should be interconnected / and be interoperable. Practically this means that if we have one hundred (theoretical number) of IT providers in one year of operations of the eCMR system then four thousand nine hundred fifty (4,950) interconnections are required in order to ensure that all IT solutions are interconnected and interoperable. This practically is a quite big investment from the part of the providers of IT solutions.
- Furthermore, customs have the right upon request to read the data of the specific CMR arriving at their borders. These trucks can come from everywhere and could have used any IT solution validated in their country. Practically it means, if today we have 58 contracting parties to the CMR Convention and eventually if a solution is found for the operationalization of eCMR then all of them will ratify the protocol, that 58 Customs authorities will have – if permitted mainly due to security reasons – to interconnect with at least 100 IT solutions (theoretical number). This means that each Customs authority should perform eventually 100 interconnection projects if the wish to have reading access to data meaning 5,800 interconnections for all customs authorities of all contracting parties!
- The same conditions eventually will apply for the traffic police and the courts.
- A question exists about the consignees since the consignees normally are the ones using IT solutions abroad meaning a different IT solution from the one the consignor and carrier have chosen to use. The number of course of the interconnections that consignees have to perform will differ depending on the number of trade partners they do have, the number of carriers / freight forwarders that they are using etc. Also, these connections are not so time consuming as it would be for the customs for instance.
- Today, based on rough calculations, there are more than 600 million CMR consignment notes issued per year. This is a very big market and possibly the number of the 100 IT providers / solutions that we are referring to in our scenario is most probably pessimistic.
- It should be also noted that United Nations is taking the effort to ensure proper and sustainable operationalization of the eCMR in order to further promote the CMR Convention in other regions (Africa, Latin America) attracting new contracting parties and facilitating road transport in other regions too. This practically means that the number of users / users – hopefully - will dramatically increase the years to come.
- Another approach to be discussed, could be that instead of all of them interconnected to each other – meaning a lot of effort, time and cost- to interconnect to one central platform that it plays the role of messenger. This platform should not have access to

any data and based on data requests, it should be able to pull and push data among the different IT solutions and the public authorities meaning customs and police. This approach will dramatically reduce the cost and time of interconnection because each of them they should interconnect only with one, the central platform.

Figure high level architecture of eCMR future system option 2 (centralised approach)