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

Economic and Social Council

Distr.: General
24 February 2023

Original: English

Economic Commission for Europe

Inland Transport Committee

Working Party on Road Transport

Group of Experts on the Operationalization of eCMR

Fifth session
Geneva, 3–5 April 2023
Item 3 (a) of the provisional agenda
Programme of work:
Proposed concepts and processes of the future eCMR system

Operational procedures stipulated by the eCMR Additional Protocol – digital environment*

Submitted by the Secretariat and the Group of Experts

I. Background

1. At its fourth session, the Group of Experts discussed ECE/TRANS/SC.1/GE.22/2023/1, provided comments and requested the secretariat to either revise it or to prepare a new document based on it for this session by taking into account the discussions of the Group. Accordingly, the secretariat has prepared ECE/TRANS/SC.1/GE.22/2023/3 and ECE/TRANS/SC.1/GE.22/2023/4. 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

* This [document] [report] was scheduled for publication after the standard publication date owing to circumstances beyond the submitter's control.

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, the digital world requires to separate the authentication of the users from the authentication of the consignment note (see below, electronic signatures).

5. In order to create trust in the system and ensure that all stakeholders 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 CMR Convention stipulates.

6. Therefore, all users should be authenticated before using the system by different means of authentication agreed by the users / parties at international level (ITC/SC.1) (non-exhaustive list) :

(a) National authentication system (electronic signatures etc.)

(b) Third party providers

(c) International user's database

7. Each of the contracting parties should 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 carries using the systems will be almost impossible. Maybe, generic guidelines should be provided 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. For instance:

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.

10. The electronic signatures if agreed would help on the following processes (non exhaustive list):

- Finalising the consignment note online by the parties
- Carrier making reservations and acceptance by the senderI.
- Transferring of right of disposal of the goods
- Sender making changes regarding consignee or providing instructions
- Acceptance delivery of goods by consignee with or without reservations

- Customs authorities checking the goods and providing comments

11. There is no international CMR Convention on electronic signatures. However, there are solutions discussed in the group that would facilitate this process. Specifically:

(a) Using 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.

(b) Amending the eCMR Additional Protocol.

Including in the national laws the UNICITRAL model law on electronic signatures would be the more efficient way to create an international and harmonised way for the use of the electronic signatures especially among the contracting parties to the eCMR Additional Protocol. However, since the changing of the national law could be a time consuming process especially in those countries that laws for electronic signatures exist already but they are not aligned with the UNICITRAL model law and since the efforts of the group aim at having an international and sustainable agreed solution for eCMRs as soon as possible, as temporary solution could be the amendment of the eCMR Additional Protocol. The inclusion of a new, generic provision in the eCMR Additional Protocol that would bind all contracting parties would be enough in order to initiate operations eCMRs. A possible amendment could be as follows: *The stakeholders that are issuing an electronic consignment note shall use electronic signatures generated based on their National Law. Contracting Parties bound by eCMR additional protocol shall accept the electronic signatures generated by other contracting parties.*

C. Information technology Solutions

12. An entity interested in generating electronic CMRs will make use of the functional and technical specifications developed by group of experts and adopted by the Working Party on road transport in order to develop an electronic solution that generates the electronic consignment notes.

13. The following principles should be followed regarding the development of these electronic solutions:

- The entity should be a private information technology company, a Carrier or a freight forwarder that afford to take the cost and time and develop their own solution or a shipper.
- 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,
- 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. 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

14. 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.

15. 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 stakeholders of the system for such temporary / permanently withdraw of validation.

16. 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, 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

17. 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.

18. 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 in National level.

F. Cyber security – Back ups

19. 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

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

G. Fallback procedure

21. 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.

22. There is no provision in the eCMR Additional Protocol eCMR that defines the fallback 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. The fallback procedure in order to be recognized and followed by all contracting parties should be a legally bind procedure included in the protocol. The secretariat suggests the preparation of a provision for the fallback procedure to be included in the protocol.

23. For the purposes of a fallback procedure (interruption of internet, several other technological disruptions etc) the moment the contract is concluded online then an electronic not changeable document will be produced (PDF, jpeg etc) that will be sent automatically to the emails of the parties to the consignment note (Consignor, Carrier and if agreed, the Consignee). This document should have “an electronic stamp / QR Code” of the platform generated indicating the platform, the date and the place that was generated. Possibly the format of this “electronic stamp/ QR code” should be included in the technical specifications of the system in order to ensure harmonization and therefore recognition by all contracting parties.

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

24. 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.

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

26. 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.

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

28. 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.

29. 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

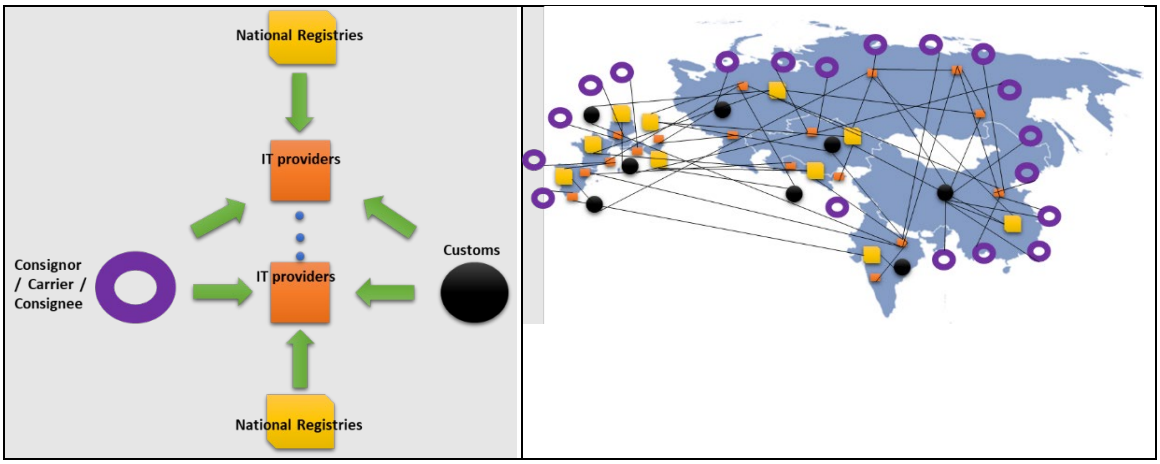
30. Based on the discussions of the group so far, the following high-level architecture of the future eCMR system is being formed. Thousands of Consignors, Consignees and Carriers should somehow use the services of hundreds private IT Companies that provide IT solutions for eCMRs based on the specifications provided by UNECE or using their own applications. 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.

31. The eCMR IT solutions will be based on machine to machine communication triggered by specific events. Therefore, the interfaces between the various eCMR stakeholders 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.

32. 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. The eCMR IT solutions should be configured not to be accessible by anyone from the internet, except by a restricted list of IP addresses which correspond to the main servers of the eCMR stakeholders which have completed their interconnection projects. This approach drastically reduces the potentiality of cyberattacks to the eCMR IT solutions, including “denial of service” and trying to “spoof “an eCMR stakeholder.

33. 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



Source: Secretariat

34. 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.

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

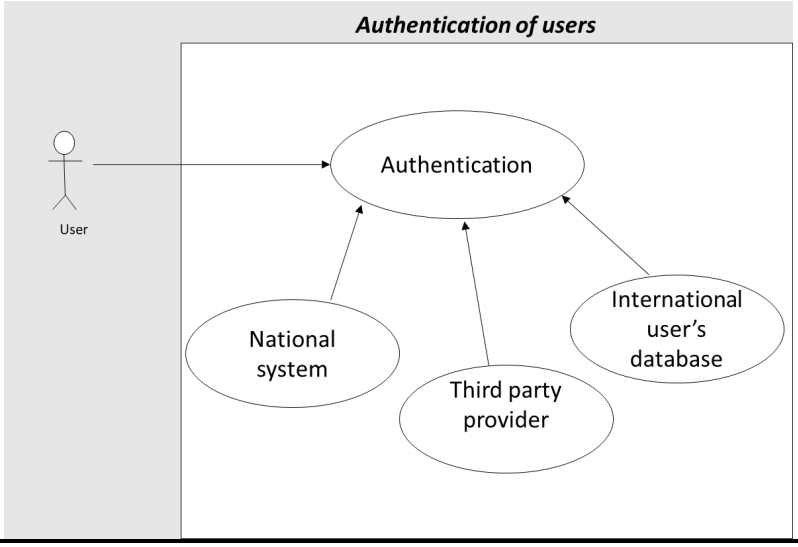
- A national body should validate the IT solutions provided in its territory and announce the list of validated solutions to other contracting parties and the market (to be agreed),
- The national authentication mechanisms to be followed should be announced to all contracting parties. Any user of the 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 / stakeholders – hopefully - will dramatically increase the years to come.

IV. Use cases analysis (indicative list)

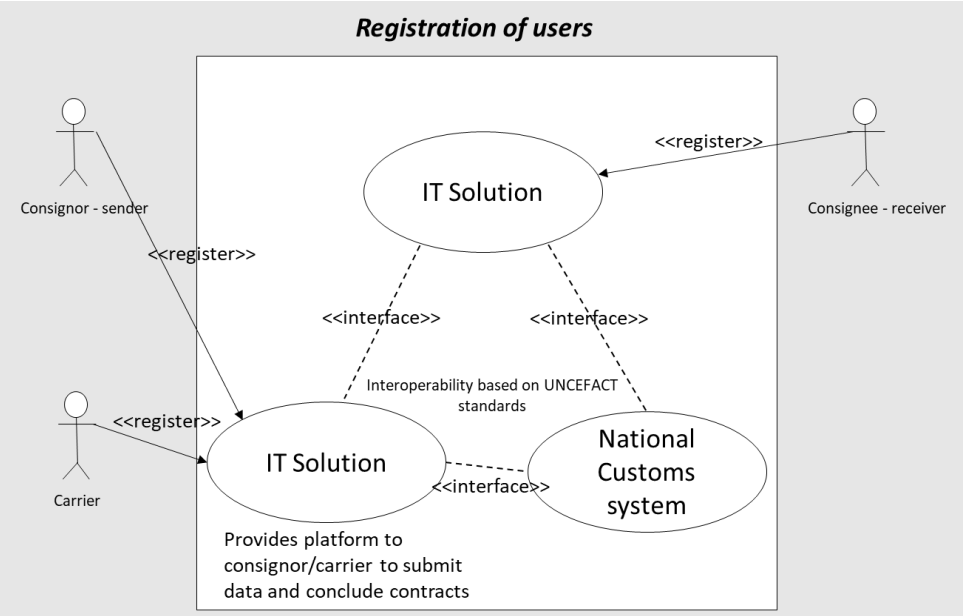
36. The use case analysis provides a high-level view on the interactions (uses) between the actors / users.

A. Authentication of users



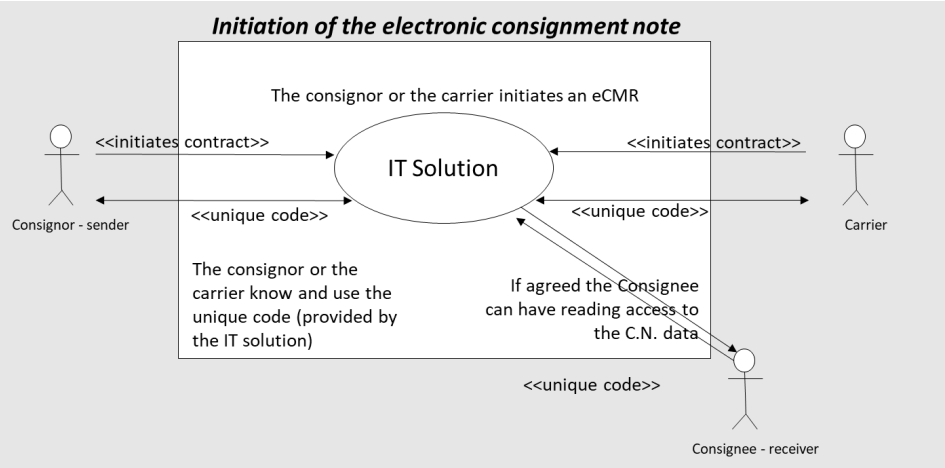
Name	*Authentication of users by the National authentication mechanisms use case*
Description	Each user should be authenticated and prove this authentication by using their national authentication mechanisms. The prove of authentication (unique code?) should be used in order to register at the IT solutions.
Actors	Users
Performance Goals	Only authenticated users can access and use any IT solution.
Preconditions	The user is an authorized / authenticated user.
Postconditions	The user is allowed to gain access to any IT solution.
Scenario	**Authentication** The IT solutions should be able to check if the information provided by the user is valid and registered in the national authentication mechanism.
Alternative Scenario	**Fallback scenario** If the authentication fails for any reason, the user will be informed accordingly. Then the user will be required to rectify the information provided for the authentication to be successful.
Special requirements	Required user information for accessing any IT eCMR solution

B. Registration of users



Name	*Registration of users in the IT solutions*
Description	Each user should register themselves in the IT solutions of their choice in order to be able to submit, validate and receive data.
Actors	Consignor – sender, Carrier, Consignee - receiver
Performance Goals	-
Preconditions	The user who registers in any IT solution should have been first authenticated by its national authentication mechanism and this unique authentication id should be provided for the registration
Postconditions	The details of the user are stored in the IT solution with the status “authorized”
Scenario	Registration The system registers the users with a double factor registration (email and mobile phone) and notifies them with results of the registration.
Alternative Scenario	Fallback scenario If the registration fails for any reason, the user will be informed accordingly. Then the user will be required to rectify the information provided for the registration to be successful.
Special requirements	The users will be able to update their information in the IT solution and keep all relevant to their work files, statistics etc.

C. Initiation of the electronic consignment note



Name	*Initiation of the electronic consignment note use case*
Description	The consignor or the carrier initiates the electronic consignment note in the selected IT solution by inserting all relevant information. The party initiating the electronic consignment note should know and use the unique code of the other partners. The consignee, if agreed by the carrier and consignor should also be informed for the new electronic consignment note issued.
Actors	Consignor, Carrier
Performance Goals	Any electronic consignment note, issued to a consignor or carrier, shall be registered in the IT solution.
Preconditions	The holders of the contract of carriage must be authenticated and registered in the IT solution.
Postconditions	The contract information is stored in the IT solution with the status “issued” or “in use”.
Scenario	**Initiation** Once the electronic consignment note has been initiated between the consignor and the carrier, the other party will receive an electronic notification that the new electronic consignment note has been initiated requesting their confirmation while providing all the information required by the eCMR consignment note.
Alternative Scenario	**Fallback scenario** If the eCMR consignment note cannot be sent to the IT solution by mean of any electronic means or web services, no functional fallback is foreseen, and the same information can be sent as soon as it is possible by the party declaring the eCMR consignment note.
Special requirements	-