United Nations ECE/TRANS/WP.15/AC.1/2018/25

Economic and Social Council

Distr.: General
29 June 2018

Original: English

Economic Commission for Europe

Inland Transport Committee

Working Party on the Transport of Dangerous Goods

Joint Meeting of the RID Committee of Experts and the Working Party on the Transport of Dangerous Goods
Geneva, 17–21 September 2018
Item 6 of the provisional agenda
Reports of informal working groups

Informal working group on telematics: meeting in London (4-5 June 2018)

Transmitted by the Government of France on behalf of the informal working group*, **

Summary

Executive summary: Information for the Joint meeting on work in progress concerning "telematics"

Introduction

1. As mentioned in paragraphs 62 to 66 of the report from the last session of the joint meeting (ECE/TRANS/WP.15/AC.1/150) the working group met on 4 and 5 June 2018 in London.

* In accordance with the programme of work of the Inland Transport Committee for 2018-2019, (ECE/TRANS/2018/21/Add.1, Cluster 9 (9.2)).

** Circulated by the Intergovernmental Organisation for International Carriage by Rail (OTIF) under the symbol OTIF/RID/RC/2018/25.

2. The working group produced a draft of a memorandum of understanding to help initiate the process of using the architecture previously approved for exchanging electronic documents between carriers and authorities.

3. The working group agreed that the draft memorandum reproduced in the appendix to this document, would serve as report of its session. It is submitted to the Joint Meeting for information on the work in progress.

4. The working group agreed to meet again from 12 to 14 November 2018 in Vienna to finalize the work.

Appendix

Memorandum of understanding for the use of 5.4.0.2 ADR/RID/ADN

Introduction

1. The purpose of this memorandum of understanding (MoU) is to support the development of a harmonised system for the use of electronic transport document during the carriage of dangerous goods, allowing a common understanding of 5.4.0.2 and fulfilling the conditions set out in 5.4.1 of ADR/RID/ADN.

2. The signatories to this MoU agree that the model and system architecture outlined here (Annex and technical documents) is the one that they will use.

3. It is recognised that the implementation of this harmonised system in each signatory will vary in pace, with some signatories already in advanced stages of its development and use at national level.

4. **Therefore, there are two categories of participant countries to this MoU; the first is one where a state is working towards implementing the system and the second category is one which is using the system fully.**

Country	Category	Date of signature
Country 1	1 or 2	
Country 2	1 or 2	"Date of signature category 1" "Date of signature category 2"

5. Whereas:

(a) **The system architecture** outlined in the annex is based on the concept of 2 types of service providing systems called trusted party TP1 and TP2. The model envisages a number of TP1 and TP2.

(b) TP2 holds the data required in accordance with section 5.4.1 of ADR/RID/ADN. A TP2 may be operated by a carrier or operated by a third party service provider to a carrier.

(c) TP1 provides services for sharing this data from the TP2 to authorities and emergency services upon request.

(d) A TP1 also provides the data from the TP2 to other TP1 upon request.

(e) eDG Transport Information is the acronym referring to the technical element which are describing the exchange format based on the UML model, the XSD schema, the WSDL webservices.

Section 1

Scope

6. The provisions of 5.4.0.2 ADR/RID/ADN are deemed to be fulfilled in the signatories under the conditions laid down in the annex. For the purpose of these MoU, an electronic transport document is an electronic documentation of the information required in the transport document in accordance with section 5.4.1 of ADR/RID/ADN.

Section 2

Principles for amending the Memorandum

General

7. The MoU may be amended at a yearly conference or instead through a written procedure.

8. Yearly conferences or written procedures should be so scheduled that amendments to the international transport regulations (ADR, RID and the ADN) can be taken into account.

9. A conference or a written procedure should be hosted by one of the signatory States usually in the following order: France, Germany, Italy, Austria, Belgium, United Kingdom. The chair host has the responsibility to organise the meeting and to take care the reference documents.

10. Each signatory may propose amendments to the MoU. Amendments may also be proposed by international or European organisations that have been accepted by the signatories. The signatories should agree on amendments by consensus.

11. The revised MoU should be reproduced and circulated by the host when new amendments have been adopted. The amended parts of the text should be indicated in the margin.

12. The revised MoU shall come into force six months after the new text is available or as otherwise decided.

13. Distribution and communication in general should be performed by electronic means.

Conference

14. Proposals should be sent to the host of the next conference at least three months before the conference takes place. The host should distribute the proposals to all signatories and international or European organisations at least one month before the conference. All signatories and organisations shall have the opportunity to respond to the documents presented within a period of two weeks after the distribution.

15. Working groups for special issues may be arranged in the time between the conferences. The reports or proposals from such working groups should be presented at the conference in the same way as other proposals. Working groups may also take place during a conference, and this should, if possible, be notified in advance. TP1s shall have the responsibility for the day to day maintenance and management of the system and may establish a technical working group to support them in this work.

Written procedure

16. A written procedure can be used as an alternative to a conference providing this is proposed by the signatory designated to host the next conference. In such case the designated signatory will host the written procedure.

17. A written procedure can also be initiated if at least three signatories request it. In such case, the participating country who hosted the latest conference should host the written procedure.

18. The host shall distribute proposals to the participating countries and announce the schedule for written comments. All participating countries should respond to the proposals within a period of six weeks. If the initial proposal is amended on the basis of comments of the participating countries, the revised proposal should be distributed again to the

participating countries. From the time when the revised proposal is distributed, the participating countries shall declare within four weeks whether they agree to the amended text of the MoU.

19. The amendments are adopted if supported by all participating countries. The host shall notify the adoption of the amendments and reproduce and circulate the revised MoU in accordance with item 11 of this section.

20. In such case all participating countries shall sign and return to the host a hard copy of the revised MoU. The signed hard copies shall be kept by the chair host. The chair host shall ensure that the updated UML, XSD and WSDL reference files named "eDG Transport Information" are made available on line.

21. Technical changes limited to UML, XSD, WSDL reference files agreed by the TP1s and the technical committee mentioned in 9) are accepted immediately and notified to the chair host.

22. Confirmation for proposal according to the Annex (I (b) (iv)) and proposal concerning maintenance as defined in 15) can be given in the yearly conference or in the written procedure. Alternatively proposed changes are accepted if participating countries do not raise objections within two weeks following notification.

Annex

1. Principles for the communication between various TP1s and TP2s on transport documents

(a) A TP1 can be publicly or privately operated. The TP1 operator has to work under conditions of certification defined in (b). Access to information provided by TP1s shall be free of charge to other TP1s and authorities. There can be one or more TP1 in a state. A state is not obliged to establish a TP1 as it can decide to rely on the functions/services provided by foreign TP1(s). TP1s with no registered TP2s are also accepted.

(b) Qualified TP1 entities ("TP1 certification"):

(i) France, Italy and Germany have already identified an initial set of TP1s (currently GBK as future TP1 in Germany, NeoGLS and Novacom Services as future TP1s in France, Italy's Ministry of Transport and UIRNet as future TP1s in Italy).

Signatories may nominate additional TP1s.

(ii) For future operations, this list of qualified TP1 entities (TP1 Trusted List) including all relevant information for identification should be deposited with UNECE for road transport and inland navigation, possibly ERA/OTIF for rail transport; UNECE/ERA/OTIF should also manage this list and publish extracts from it to the extent necessary for the system. As a consequence, these institutions would assume the responsibility of a Trusted List Manager.

(iii) All qualified TP1 entities are informed/updated about the TP1 Trusted List (i.e. they know which are the other qualified TP1 entities) by the trusted list managers.

(iv) More detailed requirements that are to be met by a TP1 still need to be defined and described and will be added in the future. To lay a sound foundation for defining these requirements, the aforementioned companies/entities are to develop rules and submit reports. These requirements for recognition would then be discussed and confirmed by the signatories and need to be applied to other interested companies.

(c) <u>For a start, the following "Rules of Procedure" have been identified</u>:

(i) A signatory of this MoU may only nominate a TP1 candidate which is established in its own country. This TP1 conforming to the requirement of this MoU shall obtain eDG Transport Information from its nominating signatory country. All qualified TP1 entities must support the entire XSD schema of the eDG Transport Information for the data exchange.

(ii) TP1s must accept requests from other TP1s.

(iii) TP1s must accept all TP2 registration.

(iv) TP1s must accept requests from competent authorities that are registered with it.

(v) After having been included in the Trusted List, new TP1s need to register with every existing TP1 providing all mandatory contact details.

(vi) The TP1 has discretion to determine its pricing policy, but has to follow a non-discriminating approach.

2. Requirements to be met by TP1s with regards to their operation

(a) National procedure to define authorities entitled to submit queries:

(i) Every signatory compiles its own list of authorities (e.g. enforcement bodies, emergency services) that are entitled to submit queries to a TP1. The signatory must also ensure that it includes the authorities' relevant certificate as set out in 4 (c). Only authorities on this list are entitled to register with a TP1.

(ii) The signatory is responsible for updating and managing the list.

(b) TP1 services

(i) TP1 and TP2 services are described using the Web Service Description Language (WSDL). Mainly, services accessible from the outside are described together with their parameters and return values.

(ii) The TP1 service getDGTDocument procures a specific transport document from a specific TP2. The parameters for identifying the TP2 and the specific transport document are described in 3 (a). This service is only available to emergency services and enforcement authorities (see 2 (a) (i)). The authority shall only request information from the TP1 for vehicles in its territory. The reason for seeking access must be specified by choosing from a predefined list (emergency services, enforcement bodies, customs, infrastructure managers…).

(iii) Every access must be logged for a minimum period of three months to comply with 5.4.1.1.

(iv) TP1 must record the journey from the start to the end of the carriage as set out in 5 (a).

(c) Certificates

(i) TP1s must use an HTTPS protocol. TP1s must have a static IP address and an X509 V3 certificate, which will be included in the Trusted List: authentication must take place by checking both IP address and certificate. Data protection must be achieved using http over TLS cryptographic protocol. Certificates have to be issued in accordance with national rules of the signatories. Certificates must be directly exchanged through secure channels.

(d) Registering with a TP1 entity (authorities, TP2)

(i) To allow machine to machine communication, the TP1 shall define a registration procedure which may be manual or automatic.

If automatic, it shall be based on the method included in the WebService description mentioned in (1) (c) (i). In particular:

- TP2 candidates will invoke the method "sendTP2RegistrationRequest" with these minimum set of data:
  - URL: TP2 entry point for the TP1
  - Public key of TP2 certificate
  - TP2 Company name
  - Contact name, mail and phone number of the responsible person
- For the public bodies, the method is "sendPublicServiceRegistrationRequest" and the minimum set of data is:
  - Public key of public bodies certificate

- Public body address (street, postal code, locality)
- Public body name
- Contact name, mail and phone number of the responsible person
- Actor type: competent authority (include also infrastructure manager), emergency responders, enforcement bodies, security bodies.

(ii) The registration procedure for TP2 is to be specified by the TP1.

(iii) In the case the entity requesting to register is an authority (i.e. it is a TP1), its name and certificate must be in the list of section 4 (a) (i), and verification can be done automatically or manually.

In case the entity requesting to register is a TP2, two methods can be used:

- either TP2 will send separately a statement digitally signed by the entity official representative who declares the public key, and then the verification is done manually offline; or
- TP1 trusts the signer of the certificate, on the basis of national laws, public registries or specific agreements, and then the verification is automatic.

3. Establishment and availability of the datasets to be used between TP2s, TP1s and the authorities/emergency services

(a) The following data set has to be transmitted to a TP1 before the commencement of the journey:

(i) Vehicle Identification Numbers (VINs), considering the VIN of truck and trailers

(ii) BIC code for containers (if available or regulated)

(iii) ADR: Registration number of the towing vehicle and the trailer(s)

ADN (if appropriate): ENI number

RID (if appropriate): UIC wagon number

(iv) Status of the carriage.

(b) Transaction between a TP2 and a TP1 entity:

(i) For each carriage a TP2 must transact with only one TP1.

4. Additional requirements in the transitional phase

As long as there are fire brigades and relevant authorities that are not connected to the TP1/ TP2 system, on board information is in addition necessary.

(a) Additional requirements concerning data storage and data output on board the vehicles/trains/ inland waterway vessels

(i) The data storage medium used in the on- board data terminal must be suitable for permanently storing all the relevant dangerous goods information in accordance with section 5.4.1 of ADR/RID/ADN for the duration of carriage. For this purpose, non-volatile storage media (currently EEPROM or flash memory) shall be used in all data terminals (e. g. tablets, scanners,

smartphones, OBUs). The data storage media installed in the data terminals needs protection against the commonly occurring stresses during carriage.

(ii) For carriage by road and rail, a portable data terminal and, for carriage by inland waterway, a portable data terminal or one permanently installed on-board is to be used. Where only one to three different dangerous goods (UN numbers) are carried in tanks or in bulk in vehicles subject to marking requirements in accordance with paragraph 5.3.2.1.2 or 5.3.2.1.4 of ADR, a permanently installed data terminal is permitted also for carriage by road.

The data terminal has to be designed in such a way that no loss of data can occur when the energy supply is interrupted. The energy storage device has to provide energy for the duration of the transport operation or be recharged during carriage by means of equipment on board.

(iii) The data must be displayed on a screen that is equivalent to paper both in terms of character size and readability (visual representation without layout requirements (e. g. PDF format) on a screen of at least 10 inches or an optimized and structured representation that makes it possible to display on the respective screen (at least 3.5 inches) all substance-related required data of a dangerous goods entry) in different light conditions. The operation of the reader must be easy and intuitive and give inspectors/the rescue services unrestricted access to all relevant dangerous goods information.

(iv) Usually, the responsibility for the operation of the data terminal rests with the vehicle drivers/train drivers/shipmasters. Within the framework of their obligation to provide information, they have to provide the authority responsible for monitoring with the aids required for performing the monitoring measures and provide the necessary assistance. Upon request, they must instruct the inspection staff in the operation of the data terminal or accompany them during the inspection and carry the data terminal along for this inspection. This also applies to emergencies in which they are able to do so. Vehicle drivers/train drivers/shipmasters have to be instructed by the carrier in the operation of the data terminal and they have to be advised in a verifiable manner of their obligation to cooperate in inspections or in the case of incidents or emergencies. For emergencies in road transport (driver not responsive), a readily identifiable and understandable note on how to access the dangerous goods data on the data terminal that are relevant for the emergency services has to be affixed in the driver's cab.

(v) It must be accepted that, in the case of a lack of mobile connectivity, the required storage on board and of identical data sets in TP2 will only take place after mobile connectivity has been restored and data exchange has become possible again.

(b) Marking of the vehicles for carriage by road if an electronic transport document is used

The front and back of the vehicle must be marked with a note indicating the use of an electronic transport document. If it is not possible to affix this mark to the back for structural or other obvious reasons, it may be affixed at both entrances to the driver's cab. Depending on the type of use of the vehicle, the mark can be detachable (folding or magnetic marks may be used) or permanently attached (fixed).

The mark consists of an illustration (pictogram) on an orange-coloured diamond-shaped symbol.

5. Further particularities for individual transport modes Railways

(a) For the rail transport mode, administrative controls of dangerous goods are carried out regularly on consignments in side-tracked trains, groups of wagons and individual wagons; here no staff of the carrier and thus no data terminal is available. Moreover, in such cases there is no information affixed to trains and wagons that would make an unambiguous identification of the carrier/railway undertaking possible. In these cases, the respective railway infrastructure company, upon request, informs the inspection authorities of the responsible railway undertaking.

(b) The railway undertaking has to provide to the signatory a central telephone number to be passed on to the inspection authorities via which the inspection authorities can, at any point during carriage, by stating the wagon number request the transmission of the data of the transport documents in accordance with 5.4.1 of RID. For the transmission of the data, no. 2 is applicable. Upon request of the railway undertaking, the inspection authority staff requesting the information has to prove their identity. For this purpose, a verification procedure in accordance with the explanations under no. 2 (c) has to be applied and coordinated between the inspection authorities and the railway undertaking.

(c) To ensure that emergency and rescue services have access to these transport document data in the case of an incident, the carrier/railway undertaking, in addition to the data required in accordance with 1.4.3.6 (b) of RID, has to make available a telephone number to the railway infrastructure company via which the control centres of the emergency and rescue services can retrieve the complete transport document data at any time. It is also permissible to allow the emergency and rescue services to electronically access the data of the railway undertaking in accordance with 5.4.1 of RID. The railway infrastructure company must ensure that the emergency and rescue services have knowledge of a contact point to retrieve the information. (For DB AG, this is ensured by means of the reporting channels agreed with the interior ministries of the federal states within the framework of the emergency management of DB AG.)

6. Inland navigation

(a) On board inland waterway vessels, a transport document can usually be printed out using an available printer. Thus, it is possible to apply the solution described if the general requirements concerning the data terminal and data storage are complied with on the inland waterway vessel. If the transport document cannot be printed out on board, it is also possible to use the solution described above consisting of an on-board terminal and data storage in a TP2. In this case, it must be possible for the emergency services to obtain the data after providing the vessel's name, the European number of identification (ENI) or the accident site.