Economic Commission for Europe

Inland Transport Committee

Working Party on the Transport of Dangerous Goods

107th session **7 November 2019**
Geneva, 11-15 November 2019
Item 4 of the provisional agenda
Work of the RID/ADR/ADN Joint Meeting

Guidelines for the use of RID/ADR/ADN 5.4.0.2

Introduction

1. RID/ADR/ADN 5.4.0.2 allows the use of electronic data exchange to satisfy the documentation requirements of Chapter 5.4, provided the procedure for capturing, storing and processing the data meet the legal requirements as regards evidential value and availability during transport in a manner at least equivalent to that of paper documentation.

2. However, RID/ADR/ADN does not further define this equivalence. In order to satisfy the goal of ensuring the availability of data, security and evidential value, web services, interfaces and a communication architecture supporting data communication must be implemented.

3. These guidelines are based on the outcome of the working group on telematics as approved by the Joint Meeting, but not all ADR and/or ADN Contracting Parties and/or RID Contracting States have implemented these guidelines yet. ADR and/or ADN Contracting Parties and/or RID Contracting States willing to use these guidelines may do so on a voluntary basis. However, once committed to using them, a Contracting Party/Contracting State must be consistent and use them in their entirety.

Section 1 – Scope and definitions

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

5. ADR and/or ADN Contracting Parties and/or RID Contracting Parties using these Guidelines are hereinafter referred to as “participants”.

6. The participants agree that the model and system architecture outlined in Annex A and in technical documents is the one that they will use.

7. Whereas:

(a) The system architecture outlined in Annex A is based on the concept of 2 types of service providing systems called trusted parties TP1 and TP2. The model envisages a number of TP1s and TP2s;

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

(c) TP1 provides services for sharing these data from TP2 with authorities and emergency services upon request;

(d) A TP1 also transmits the data from TP2 to other TP1 upon request;

(e) eDG Transport Information is the acronym referring to the technical elements which describe the exchange format based on the Unified Modelling Language (UML)

model, the eXtended Markup Language Schema Definition (XSD), the Web Service Description Language (WSDL) web services.

Section 2 – Obligations of the participants

8. A participant notifies the UNECE/OTIF secretariat that it is using the guidelines. It also notifies TP1s (if any) nominated in accordance with Annex A.

9. Participants accept electronic transport information in conformity with the guidelines and their Annex A.

Section 3 – Publication of the guidelines and list of participants

10. UNECE and OTIF will publish the list of participants and TP1s notified by participants.

11. The Guidelines will be made available on the UNECE and OTIF websites as well as the UML, XSD and WSDL reference files named “eDG Transport Information”.

Section 4 – Data security and technical maintenance

12. TP1s shall take appropriate technical and organisational measures to ensure data security. They shall not use confidential data for purposes (e.g. misuse through data mining) other than described in these Guidelines.

13. TP1s shall be responsible for the day to day maintenance and management of the system and shall cooperate in a technical working group, which will support them in this work. Maintenance also includes technical updates resulting from amendments to RID/ADR/ADN.

14. In case of severe communication problems, any technical changes to “eDG Transport Information” (limited to UML, XSD, WSDL reference files) which are essential for the function of the system and which are agreed by the technical working group, shall be accepted immediately.

15. The technical working group shall inform all TP1s about updates to the “eDG Transport Information” and the date of application and shall submit them to the UNECE/OTIF secretariat for publication on the UNECE and OTIF websites.

Section 5 – Principles for amending the Guidelines

16. Amendments to the Guidelines are adopted by the participants, either by a written procedure with consensus or at a meeting according to the rules to be defined by the meeting. Other Contracting Parties/Contracting States may also propose amendments.

17. Amendments to the system architecture may only be proposed by the technical working group and must be accepted by the Joint Meeting.

Annex A

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

(a) A TP1 can be publicly or privately operated. A TP1 operator must not participate (in particular as consignor, carrier, consignee, loader, packer, filler, tank-container /portable tank operator or unloader) in the carriage of dangerous goods. The TP1 operator has to work under the conditions of certification defined in (b). Access to information provided by TP1s shall be free of charge to other TP1s and authorities. There may be one or more TP1 for each participant. A participant is not obliged to establish a TP1, as it may 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) Austria, France, Germany and Italy have already identified an initial set of potential TP1s (currently DiGiDO in Austria, NeoGLS and Novacom Services in France, GBK in Germany and Italy's Ministry of Transport and UIRNet in Italy).

Participants 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 and with OTIF for rail transport; UNECE/OTIF should also manage this list and publish extracts from it to the extent necessary for the system. Consequently, these institutions 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 the other qualified TP1 entities are) by the trusted list managers.

(iv) More detailed requirements, e.g. regarding an agreed certificate and security policy, that TP1s must apply, will be specified 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 participants and must be applied to interested companies.

(c) The following "Rules" shall apply:

(i) A participant may only nominate a TP1 candidate which is established in its own country. All qualified TP1 entities must support the entire data exchange specifications of the "eDG Transport Information".

(ii) TP1s must accept requests from other TP1s.

(iii) TP1s must accept all TP2 registrations if these are compliant with the Guidelines and meet the contractual obligations of that TP1.

(iv) A TP1 may charge for the services it offers to a TP2. The TP1 has discretion to determine its pricing policy, but must adopt a non-discriminatory approach.

(v) TP1s must accept requests for registration of authorities listed in accordance with (d).

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

(vii) After being included in the Trusted List, new TP1s must register with every existing TP1 and provide all the mandatory contact details.

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

(i) Every participant compiles its own list of authorities (e.g. enforcement bodies, emergency services) that are entitled to submit queries to a TP1. The participant must also ensure that it includes the relevant authority certificate as set out in 2 (b). Only authorities on this list are entitled to register with a TP1.

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

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

(a) **TP1 services**

(i) TP1 and TP2 services are described using the WSDL. Services accessible from the outside are mainly 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 1 (d)). 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 (e.g. emergency services, enforcement bodies).

(iii) Every access must be logged for a minimum period of three months to comply with 5.4.4.1.

(iv) TP1 must store the start and the end of a transport operation as set out in 3 (a) in order so that the TP2 data set concerning every transport operation can be transmitted to enforcement bodies or emergency services on request.

(b) 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 in the country of the participant. Certificates must be directly exchanged through secure channels.

(c) Registration of authorities and TP2s with a TP1

(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 Web Service description mentioned in 1 (c) (i). In particular:

- TP2 candidates must invoke the method "sendTP2RegistrationRequest" with this minimum set of data:
  - URL: TP2 entry point for the TP1
  - Public key of TP2 certificate
  - TP2 name and address (street, post code, locality)
  - Contact name, mail and telephone number of the responsible person
- Public bodies must invoke the method "sendPublicServiceRegistrationRequest" with the minimum set of data:
  - Public key of public body certificate

– Public body name and address (street, post code, place)

– Contact name, mail and phone number of the responsible person

– Actor type: competent authority (e.g. emergency services, enforcement bodies, etc.).

(ii) TP1 must specify the registration procedure for TP2.

(iii) If the entity requesting registration is an authority, its name and certificate must be in the list of 1 (d) and verification may be carried out automatically or manually.

If the entity requesting registration is a TP2, two methods can be used:

- The official representative of the TP2 submits a digitally signed statement, including the public key, which is verified 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 concerning every transport operation must be transmitted to a TP1:

(i) ADR: Country code(s) (Vienna Convention), registration number(s) and Vehicle Identification Number(s) of the towing vehicle and the trailer(s)

ADN: ENI number

RID: Unique Vehicle Number[1]

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

(iii) Status: beginning/end of the transport operation

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

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

(c) The transport document information transmitted from TP2 to TP1 shall be digitally signed.

[1] Unique Vehicle Number in accordance with the Uniform Technical Prescription applicable to vehicle numbers and linked alphabetical marking on the bodywork: The railway vehicle marking (UTP Marking 2015) of the APTU Uniform Rules (Appendix F to COTIF 1999) (see www.otif.org) and European Vehicle Number in accordance with Commission Decision 2007/756/EC adopting a common specification of the national vehicle register provided for under Articles 14(4) and (5) of Directives 96/48/EC and 2001/16/EC ~~in accordance with paragraph 4.2.2.3 and Annex P of Commission decision 2011/314/EU of 12 May 2011 concerning the technical specification of interoperability relating to the "operation and traffic management" subsystem of the trans-European conventional rail system.~~

4. Requirements in the transitional phase

As long as there are emergency services and relevant authorities that are not connected to the TP1/TP2 system, on board information is also necessary.

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

(a) 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 RID/ADR/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 shall be protected against stresses that commonly occur during carriage.

(b) 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 5.3.2.1.2 or 5.3.2.1.4 of ADR, a permanently installed data terminal is also permitted for carriage by road.

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

(c) 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 optimised and structured representation that makes it possible to display on the respective screen (at least 3.5 inches) all the required substance-related data for a dangerous goods entry) in different light conditions. Operation of the reader must be easy and intuitive and give inspectors/the emergency services unrestricted access to all relevant dangerous goods information.

(d) The vehicle drivers/train drivers/shipmasters shall be able to operate the data terminal and provide the necessary assistance to the enforcement authority or emergency services. For example, upon request, they must instruct the inspection staff in the operation of the data terminal or accompany them with the data terminal during the inspection. This also applies in an emergency, where possible.

(e) If there is no mobile connectivity, it must be accepted that there may be a delay in synchronisation of the data on board and of the dataset in the TP2.

5. Transitional requirements specific to road transport

Instructions shall be affixed in the drivers cab on how to access the electronic dangerous goods data in case the driver is incapacitated.

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 on both doors of the driver's cab. Depending on the type of use of the vehicle, the mark may be detachable (folding or magnetic marks may be used) or permanently attached (fixed). The mark consists of an illustration (pictogram according to Annex B of these Guidelines).

Annex B

Pictogram “e” for using the electronic dangerous goods transport document (e DGTD)