UNITED
NATIONS

E

Economic and Social
Council

Distr.
GENERAL

ECE/TRANS/SC.1/2006/9
10 August 2006

Original: ENGLISH

ECONOMIC COMMISSION FOR EUROPE

INLAND TRANSPORT COMMITTEE

Working Party on Road Transport

One hundredth session
Geneva, 17-19 October 2006
Item 4 of the provisional agenda

IMPLEMENTATION OF THE AETR

Note by the secretariat

Members of the Working Party will find below a project plan for non-EU AETR Contracting Parties on what needs to be done to implement the digital tachograph system at their respective national level.

It is submitted by the Project on the Monitoring of the Implementation of the Digital Tachograph (MIDT), funded by the European Commission and the Swedish Road Administration, and the Confederation of Organizations in Road Transport Enforcement (CORTE).

Attention is drawn in particular to proposals made in paragraphs 30 b) and d), 40 e) and f) and 131 u), which would have resource implications for the ECE secretariat.

Project plan for AETR Contracting Parties

As from 16 June 2010, the digital tachograph will become mandatory for new vehicles put into service for the first time in the non EU-AETR Contracting Parties. Such introduction requires considerable efforts from non EU-AETR Contracting Parties.

This project plan has been drafted for the non EU-AETR Contracting Parties for them to get an overview of what needs to be done to implement the digital tachograph system at their respective national level.

An assessment in terms of timing is supplied although timing depends a lot on the administrative organisation of each State. As an example based on EU experience, in Lithuania, the same organisation is competent to issue cards (and therefore to issue and maintain a security policy), to connect to TACHOnet, to approve workshops and to enforce Drivers' hours' rules and the proper use of tachographs, whilst in Germany each responsibility as described in the following table belongs to a different organisation. As a result of this, Lithuania has been much quicker to implement the digital tachograph system than Germany. But having started sooner, Germany was up and running more than one year before Lithuania.

It has anyway to be underlined that:

- despite the fact that the digital tachograph system is mandatory for domestic and international road transport at EU level,
- despite the fact that it is known in its very details since 2002,
- and despite the very intensive support supplied to national administrations by the European Commission,

it has been and still is difficult for a couple of EU Member States to complete their implementation process within the required timeframe. It is therefore only realistic to think that without any support, the non EU-AETR Contracting Parties will not be ready by 16 June 2010.

Attention is also drawn to the fact that the MIDT (www.eu-digitaltachograph.org) project will end in March 2008 at the very latest and that every effort should be made by the UN-AETR secretariat to promote it in the non EU-AETR Contracting Parties for them to get some support from as early a stage as possible.

The MIDT team will do its utmost to guide them in their efforts and to help them to identify, in the EU countries, partners they could cooperate with so as to not start from scratch.

This project plan describes the essential steps of the introduction process. Each step of the project plan is presented shortly before being summarised in a table accessible at the end of this document.

TABLE OF CONTENTS

1 – Type approval

1.1. – The issuing of type approval certificates

1. The type approval procedure is defined by the Annex to the AETR as last amended and by its Appendix 1B.

2. Article 2, first paragraph of the Annex states among others that:

A Contracting Party shall grant its type approval to any type of control device, to any model record sheet or memory card which conforms to the requirements laid down in Appendix 1 or 1B to this Annex, provided the Contracting Party is in a position to check that production models conform to the approved type.

3. It is therefore ultimately the responsibility of Contracting Parties to type approve digital tachographs and tachograph cards.

4. But before issuing a type approval certificate, requirements 271 and 288 of Appendix 1B add that:

(271) Contracting Parties type approval authorities will not grant a type approval certificate in accordance with Article 2 of this Annex, as long as they do not hold:

- a security certificate,
- a functional certificate,
- and an interoperability certificate,

for the recording equipment or the tachograph card, subject of the request for type approval.

(288) The type approval authority of the Contracting Party may deliver the type approval certificate as soon as it holds the three required certificates.

5. In that respect, Article 2, second paragraph of the Annex states that:

The control device may not be granted type-approval until the whole system (the control device itself, driver card and electrical gearbox connections) has demonstrated its capacity to resist attempts to tamper with or alter the data on driving times. The tests necessary to establish this shall be carried out by experts familiar with up to date tampering techniques.

6. This Article has been implemented through requirement 274 of Appendix 1B and its sub-appendix 10 which refer to the Information Technology Security Evaluation Criteria (ITSEC).1

[1] See http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf

7. Security targets of vehicle units, motion sensors and tachograph cards as well as security enforcing functions are defined against ITSEC criteria and security certificates can therefore only be issued by ITSEC authorities.

8. Requirement 277 of Appendix 1B states that:

The type approval authority delivers the functional certificate. This certificate shall indicate, in addition to the name of its beneficiary and the identification of the model, a detailed list of the tests performed and the results obtained.

9. A minimum list of tests is laid down in sub-appendix 9 of Appendix 1B.

10. Requirement 278 of Appendix 1B states that:

Interoperability tests are carried out by a single laboratory.

11. This responsibility has been allocated at EU level to the European Commission (DG – JRC) and more specifically to the IPSC Laboratory established in Ispra (Italy).

12. According to requirements 281 and 284 of Appendix 1B:

(281) No interoperability tests shall be carried out by the laboratory, for a recording equipment or a tachograph card that have not been granted a security certificate and a functional certificate.

(284) The interoperability certificate shall be delivered by the laboratory to the manufacturer only after all required tests have been successfully passed.2

13. Therefore, although the ultimate responsibility to type approve digital tachographs and tachograph cards is with Contracting Parties type approval authorities, this responsibility is shared with those issuing the three required certificates listed in requirement 271 of Appendix 1B.

14. Article 2, third paragraph of the Annex to the AETR adds that:

Any modifications or additions to an approved model must receive additional type approval from the Contracting Party which granted the original type approval.

15. This provision is completed by requirements 272 and 273 of Appendix 1B which state that:

(272) Any modification in software or hardware of the equipment or in nature of materials used for its manufacture shall, before being used, be notified to the authority which granted type-approval for the equipment. This authority shall confirm to the manufacturer

[2] See http://dtc.jrc.it/InteropDocs/SPI03116.pdf

the extension of the type approval, or may require an update or a confirmation of the relevant functional, security and/or interoperability certificates.

(273) Procedures to upgrade in situ recording equipment software shall be approved by the authority which granted type approval for the recording equipment. Software upgrade must not alter nor delete any driver activity data stored in the recording equipment. Software may be upgraded only under the responsibility of the equipment manufacturer.

16. Therefore, type approval authorities, beyond the issuing of the three above-mentioned certificates, are also responsible for the compliance of any up-date of the type approved equipments with the rules laid down in Appendix 1B.

17. Once digital tachographs or tachograph cards have been granted

- a security certificate by an ITSEC authority,
- a functional certificate by a type approval authority,
- an interoperability certificate by the interoperability authority,

they can then be issued – or not - with type approval certificates and the information can circulate to other Contracting Parties authorities.

18. Article 4 of the Annex to the AETR states indeed that:

The competent authorities of the Contracting Party to which the application for type approval *has been submitted shall, in respect of each type of control device or model record sheet or memory card which they approve or refuse to approve, either send within one month to the authorities of the other Contracting Parties a copy of the approval certificate accompanied by copies of the relevant specifications, or, if such is the case, notify those authorities that approval has been refused; in cases of refusal they shall communicate the reasons for their decision.*

19. This provision is completed by requirement 290 of Appendix 1B which states that:

*The laboratory competent for interoperability tests shall run a public web site*3 *on which will be updated the list of recording equipment or tachograph cards models:*

- *for which a request for interoperability tests have been registered,*
- *having received an interoperability certificate (even provisional),*
- *having received a type approval certificate.*

20. The issuing of a type approval certificate implies that a Contracting Party authority (after having received the necessary information from an ITSEC authority and from the interoperability authority) considers that recording equipment or tachograph cards are security compliant with Appendix 1B and interoperable with all the other products already type approved.

[3] See http://dtc.jrc.it/pages/Interoperability%20Status.htm

1.2. – The withdrawal of type approval certificates

21. The Annex also contains some provisions dealing with cases where type approval may have to be withdrawn.

22. These provisions are as follows:

Article 5

1. If a Contracting Party which has granted type approval as provided for in article 2 finds that a certain control device or record sheet or memory card bearing the type approval mark which it has issued does not conform to the prototype which it has approved, it shall take the necessary measures to ensure that production models conform to the approved prototype. The measures taken may, if necessary, extend to withdrawal of the type approval.

2. A Contracting Party which has granted type approval shall withdraw such approval if the control device or record sheet or memory card which has been approved is not in conformity with this Annex or its Appendixes or displays in use any general defect which makes it unsuitable for the purpose for which it is intended.

3. If a Contracting Party which has granted type approval is notified by another Contracting Party of one of the cases referred to in paragraphs 1 and 2, it shall also, after consulting the latter Contracting Party, take the steps laid down in those paragraphs, subject to paragraph 5.

4. A Contracting Party which ascertains that one of the cases referred to in paragraph 2 has arisen may forbid until further notice the placing on the market and putting into service of the control device or record sheets or memory card. The same applies in the cases mentioned in paragraph 1 with respect to control devices or record sheets or memory cards which have been exempted from the initial verification, if the manufacturer, after due warning, does not bring the equipment into line with the approved model or with the requirements of this Annex.

In any event, the competent authorities of the Contracting Parties shall notify one another within one month, of any withdrawal of type approval or of any other measures taken pursuant to paragraphs 1, 2 and 3 and shall specify the reasons for such action.

5. If a Contracting Party which has granted type approval disputes the existence of any of the cases specified in paragraphs 1 or 2 notified to it, the Contracting Parties concerned shall endeavour to settle the dispute.

[…]

Article 8

All decisions pursuant to this Annex refusing or withdrawing approval of a type of control device or model record sheet or memory card shall specify in detail the reasons on which they are based. A decision shall be communicated to the party concerned, who shall at the same time be informed of the remedies available to him under the laws of the Contracting Party and of the time limits for the exercise of such remedies.

1.3. – Issues to be solved

1.3.1. – The interoperability tests

23. Theoretically speaking, tachograph and/or card manufacturers could request their products to be type approved in any Contracting Party.

24. Nevertheless, two thirds of the tests to be performed cannot be done in the non EU-AETR Contracting Parties:

- the security tests (ITSEC), since the ITSEC official laboratories are located in France, Germany, UK and the Netherlands,
- the interoperability tests, which have to be carried out by a single laboratory.

25. Some years ago, it was expressly requested to modify requirement 278 of Appendix 1B so as to refer only to a single laboratory whilst the equivalent requirement in Regulation (EC) n° 1360/2002 states that:

Interoperability tests are carried out by a single laboratory ***under the authority and responsibility of the European Commission.***

26. There are therefore two/three questions which remain unanswered:

- is there still any opposition to non EU-AETR Contracting Parties to deal with the European Commission? If yes, what would be the alternative considering that to avoid interoperability problems, it is essential to work with one single laboratory?
- If not, how to make this explicit?

1.3.2. – Contestations of type approval certificates

27. Article 5 of the Annex to the AETR is written differently than its equivalent in Regulation (EEC) n° 3821/85.

28. Paragraph 5 of Article 8 of Regulation (EEC) n° 3821/85 states indeed that:

If a Member State which has granted an EEC type approval disputes the existence of any of the cases specified in paragraphs 1 or 2 notified to it, the Member States concerned shall endeavour to settle the dispute and the Commission shall be kept informed. If talks between the Member States have not resulted in agreement within four months of the date of the notification referred to in paragraph 3 above, the Commission, after consulting

experts from all Member States and having considered all the relevant factors, e.g. economic and technical factors, shall within six months adopt a decision which shall be communicated to the Member States concerned and at the same time to the other Member States. The Commission shall lay down in each instance the time limit for implementation of its decision.

29. The UN AETR secretariat does not play the role at AETR level that the EC plays at EU level. This might be problematic in case of dispute between Contracting Parties since the outcome of such may be the undue prohibition of recording equipment and/or of tachograph cards in the field.

1.3.3. – Proposals

30. Considering the timing for non EU-AETR Contracting Parties to implement the digital tachograph system, it is proposed:

a) to work with the EC – DG JRC as the single laboratory (interoperability tests),

b) the UN AETR secretariat to inform in writing each Contracting Party of the interpretation of requirement 278 of Appendix 1B and of the details of this "single laboratory",

c) to envisage at the mid-term, in case of political problems, the possibility to outsource this service to the private sector through an international tender,

d) the UN AETR secretariat to request in writing from each Contracting Party, in the light of Article 4 of the Annex, either to send it within one month a copy of the approval certificate that they have decided to grant, accompanied by copies of the relevant specifications, or, if such is the case, to notify it that approval has been refused; in cases of refusal they shall communicate the reasons for their decision. This should allow the UN AETR secretariat if not to monitor the type approval process at AETR level, at least to keep an eye on it.

2. – Security

2.1. – The ERCA policy

31. The European Commission is responsible for the European Root Certification Authority (ERCA) of the cryptographic key management infrastructure supporting the digital tachograph system.

32. An ERCA policy was approved by the European Commission/DG TREN, acting as the European Authority on 9 July 2004. The policy of the ERCA applies only to the cryptographic keys and keys certificates used in the mutual authentication, secure messaging and digital signature mechanisms of the digital tachograph system.

33. It does not cover, therefore, the overall security of the digital tachograph system.

34. According to points 4.3.1 and 5.2.1 of the ERCA policy, Member States Authorities (MSA) have to submit security policies for approval since "the objective of the approval process is to assure comparable levels of security in each Member State".

35. Points 5.1.1 and 5.1.2 of the ERCA policy state that:

(5.1.1) The MSA shall produce and maintain a MSA policy covering the following processes, where applicable:

a) issuing of tachograph cards, including keys and certificates;
b) issuing of vehicle unit keys and certificates;
c) issuing of motion sensor keys;
d) management of the Member State keys.

(5.1.2) The operation and management practices related to these processes shall be documented in practices statements approved by the MSA.

36. In other words, at EU level, cryptographic keys are issued by the ERCA, which is a task in practice allocated to EC – DG JRC. Without keys, digital tachographs cannot be introduced on the market and States cannot issue tachograph cards.

37. To be issued with keys, EU Member States have to:

- be identified (Member State Authority - MSA) by the European Authority (EA, in practice EC- DG TREN),
- and to issue a security policy proving that cryptographic keys will be managed securely which has to be approved by the ERCA.
-

2.2. – Issues to be solved

38. The agreement reached at EU level between the European Commission and the EU Member States to deal with the approval of security policies and the issuing of cryptographic keys does not legally speaking cover non EU countries.

39. The same kind of solutions have to be implemented at AETR level as a matter of urgency. If not, non EU AETR Contracting Parties will be unable to issue cards.

2.3. – Proposals

40. Considering the timing for non EU AETR Contracting Parties to implement the digital tachograph system, it is proposed:

e) the UN AETR secretariat to inform in writing each Contracting Party of the interpretation of sub-appendix 11 of Appendix 1B and of the necessity - for the digital tachograph system to be introduced in the field - to implement an AETR Root Certification Authority (AETR-RCA), which, for the period 2007-2010, could be the EU-ERCA (EC- DG JRC),

f) possibly to work with the UN AETR secretariat as the AETR Authority (equivalent to the European Commission acting as the European Authority, i.e. authority in charge of identifying AETR Contracting Parties authorities),

g) to envisage at the mid-term, in case of political problems, the possibility to outsource this service to the private sector through an international tender.

3. Workshop approval procedure

3.1: Approval of workshops

41. Article 9.1 of the Annex to the AETR states that:

The control device may be installed or repaired only by fitters or workshops approved by the competent authorities of Contracting Parties for that purpose after the latter, should they so desire, have heard the views of the manufacturers concerned.

42. Chapter VI.1, 1st paragraph of Appendix 1B adds that:

Contracting Parties will approve, regularly control and certify the bodies to carry out:

- *installations*
- *checks,*
- *inspections,*
- *repairs.*

43. Once done, and in accordance with Article 9.3 of the Annex:

The competent authorities of the Contracting Parties shall send each other their lists of approved fitters and workshops and the cards issued to them and also copies of the marks and of the necessary information relating to the electronic security data used.

44. The Annex to the AETR exists to provide a legal framework to ensure that appropriate equipment is available and maintained to support the associated AETR Drivers Hours' rules. All digital tachographs need to be, at some point, activated, calibrated, inspected, and, ultimately, decommissioned from service and workshops are expected to provide this front-line support and expertise.

45. The national Competent Authorities should therefore set out their own approval criteria as appropriate for each Contracting Parties. They should not attempt to intervene in the commercial setting up of workshops other than to ensure that legal requirements are adhered to.

46. Whatever commercial constraints are considered appropriate by Contracting Parties it is important to ensure that approved workshops are able to provide, at least, an inspection and calibration service to the requirements of the AETR for all types of digital tachograph with which they are presented.

47. All workshops should be approved against two sets of criteria:

- Technical competence and facilities,
- Suitability of Applicant.

48. Assessment of technical competence can be best achieved by ensuring that workshops have available, appropriate and/or approved equipment to allow them to carry out the required tachograph-related tasks and by ensuring that all technicians who carry out the work have successfully completed appropriate training.

49. The national Competent Authority may also have an interest in the environment in which the work is to be conducted, for example to ensure that facilities are adequate to accommodate vehicles, and that where other considerations may apply, these will also be met (e.g. health and safety guidelines).

50. Whilst the national Competent Authorities should have little interest in the commercial arrangements that are reached between a workshop and a manufacturer (providing these are legally acceptable), they do, however, have an obligation to ensure that the transport industry as a whole has access to workshops in order that their recording equipment can be installed, activated, calibrated, inspected, repaired and decommissioned properly. Therefore, the criteria used for approval should clearly set out the conditions that a workshop must meet in order to do so. Such conditions should include at least an undertaking to receive "all-comers". This means that all tachograph workshops will be able to provide a consistent level of service to vehicles fitted with different makes of digital tachographs so as to ensure that the requirements of the AETR are met. The activities that workshops are expected to conduct on all-comers is specified as:

Installation (requirement 239 of Appendix 1B),

- Activation (requirement 243 of Appendix 1B),
- Calibration (requirement 248 of Appendix 1B),
- Periodic inspections (requirement 256 of Appendix 1B),
- Downloading (requirement 260 of Appendix 1B),
  Decommissioning/Undownloadability Certificates (requirement 261 of Appendix 1B),

3.2. – Audit of workshops

51. If the workshop scheme is to work effectively and continue to keep its integrity and repute, it is vital that it is properly enforced. To achieve this, national Competent Authorities have to develop a robust legal base from which to work and at the same time, be in a position to discipline in those areas that need it.

52. Monitoring of the competence and of the activities of workshops by (or on behalf of) the Competent Authority should always be treated as a continuing activity.

53. To maintain the security of the overall digital tachograph system, proper audit trails of all activities relating to digital tachographs should be kept and each workshop should keep a complete record of all its tachograph-related activities.

54. Whilst it is possible that records could be kept in paper form, in practice, and with the existing need for the transfer of electronic data from workshop cards and the need to audit the use of those cards, electronic systems for maintaining records and for conducting audit would be the recommended and preferred method.

55. It is always for the Competent Authorities of each Contracting Party to decide the appropriate level of discipline to be taken against workshops when they do not comply with the conditions of approval.

56. The nature of disciplinary sanctions taken may be dependent on factors such as the civil code of the Contracting Party and the legal capacity of the Competent Authority concerned. However, the principle to be adhered to is that the quality of work conducted by workshops (and therefore the integrity of the monitoring systems for ensuring compliance with Drivers' Hours rules) is always assured by effective control.

57. In principle the national Competent Authorities should have in place disciplinary procedures which, ultimately, enable consideration to be given regarding the suspension or withdrawal of an approval to prevent further operation and/or the prosecution of a workshop.

3.3. – Issues to be solved

58. Contracting parties need to regulate the way workshops can be approved to deal with digital tachographs.

3.4. – Proposals

59. Considering the timing for non EU AETR Contracting Parties to implement the digital tachograph system, it is proposed:

h) to use the "Guidelines to approve workshops" issued in the framework of the IDT-MIDT project, which can almost be translated and cut and pasted into a national legislative text

i) to offer assistance to the non EU AETR Contracting Parties in the framework of the MIDT project (www.eu-digitaltachograph.org).

4. – Card issuing

60. Contracting Parties have to comply with requirements laid down in the Annex as last amended, but are lacking:

- requirements laid down at EU level in the ERCA policy,
- TACHOnet.

61. This document will focus on driver cards only, since they are in terms of volume those used to define a business model at national level when defining a card issuing strategy.

4.1. – Driver cards

62. Contracting Parties have to issue driver cards to drivers who:

- have their normal residence on their territory,

The driver card as defined in Appendix1B shall be issued, at the request of the driver, by the competent authority of the Contracting Party where the driver has his normal residence (Article 11.3, first paragraph of the Annex),

- are subject to the provisions of the AETR,

Driver cards shall be issued only to applicants who are subject to the provisions of the Agreement (Article 11.4 (b) of the Annex),

- who are therefore, at one stage or another of the application process, clearly identified by the Card Issuing Authority (CIA),

The competent authority of the Contracting Party shall personalise the driver card in accordance with the provisions of Appendix 1B (Article 11.4 (a) first paragraph of Annex 1).

63. At EU level, these provisions are reinforced by the following:

The MSA shall ensure that users of cards are identified at some stage of the card issuing process (ERCA policy, "Users Registration", point 5.3.35).

To avoid a driver holding cards from other Member States […] a check should not only be carried out by the own Member States' authority, but also by the competent authorities of other Member States. In order to guarantee a reliable system of checking the issuing of unique driver cards between Member States, it was felt necessary to have an appropriate telematics network [TACHONET] (TACHOnet XML Messaging Reference Guide, version 1.41, page 8).

64. According to Article 11.4 (f) of the Annex to the AETR:

Contracting Parties have to take the necessary measures to prevent any possibility of driver cards being falsified.

65. This is implemented through requirements 180 and 181 of Appendix 1B which state that:

(180) Tachograph cards shall bear at least the following features for protection of the card body against counterfeiting and tampering:

- *a security design background with fine guilloche patterns and rainbow printing,*
- *in the area of the photograph, the security design background and the photograph shall overlap,*

- *at least one two-coloured microprint line.*

(181) After consulting the UN/ECE Secretariat, Contracting Parties may add colours or markings, such as national symbols and security features, without prejudice to the other provisions of this Appendix.

66. Contracting Parties have, at least for driver cards, to keep records of the issuance of cards:

The issuing authority shall keep records of issued, stolen, lost or defective driver cards for a period at least equivalent to their period of administrative validity (Article 11.4 (a), 4th paragraph of the Annex).

67. Once issued, cards are mutually recognised, which implies that they may be exchanged by drivers when leaving a Contracting Party for another one:

Driver cards issued by Contracting Parties shall be mutually recognised.

Where the holder of a valid driver card issued by a Contracting Party has established his normal place of residence in another Contracting Party, he may ask for his card to be exchanged for an equivalent driver card; it shall be the responsibility of the Contracting Party which carries out the exchange to verify if necessary whether the card produced is actually still valid (Article 11.4 (d) of the Annex.

68. They can also have to be replaced (if lost, stolen or defective) or renewed (administratively expired),

If the driver card is damaged, malfunctions or is lost or stolen, the authority shall supply a replacement card within five working days of receiving a detailed request to that effect (Article 11.4 (a), 5th paragraph of the Annex),

In the event of a request for the renewal of a card whose expiry date is approaching, the authority shall supply a new card before the expiry date provided that the request was sent to it within the time limits laid down in the second subparagraph of Article 12(1) (Article 11.4 (a), 6th paragraph of the Annex),

Where a driver wishes to renew his driver card, he shall apply to the competent authorities of the Contracting Party in which he has his normal residence not later than fifteen working days before the expiry date of the card (Article 12.1, 4th paragraph of the Annex).

69. They can finally be withdrawn or confiscated in some special circumstances:

The driver card shall be personal. It may not, during its official period of validity, be withdrawn or suspended for whatever reason unless the competent authority of a Contracting Party finds that the card has been falsified, or the driver is using a card of which he is not the holder, or that the card held has been obtained on the basis of false declarations and/or forged documents. If such suspension or withdrawal measures are taken by a Contracting Party other than the Contracting Party of issue, the former shall

return the card to the authorities of the Contracting Party which issued it and shall indicate the reasons for returning it (Article 11.4 (c) of the Annex).

70. Contracting Parties have to liaise on a mandatory basis in some cases at least:

Contracting Party carrying out an exchange shall return the old card to the authorities of the Contracting Party of issue and indicate the reasons for so doing (Article 11.4 (d), 3rd paragraph of the Annex),

Where the authorities of the Contracting Party in which the driver has his normal residence are different from those which issued his card and where the latter are requested to renew, replace or exchange the driver card, they shall inform the authorities which issued the old card of the precise reasons for its renewal, replacement or exchange (Article 13.3, 4th paragraph of the Annex).

4.2. – TACHOnet

71. To ensure the uniqueness of driver cards, Member States and the Commission have set up at EU level a network aiming at facilitating the exchange of information between CIAs:

The TACHOnet project's final objective is to create a telematics network aiming at facilitating the data exchange between national administrations in charge of the issuing tachograph cards, as stated in Council Regulation (EEC) n° 3821/85 amended by Council Regulation (EC) n° 2135/98.

The TACHOnet network will:

- *ensure a reliable and secure exchange of the necessary and sufficient data between the Member States issuing tachograph cards to help them fulfil the requirements of the Council Regulation (EC) n° 2135/98.*
- *Make sure that the exchange is done in the legal framework envisaged and that it does not allow other uses of the same data,*
- *Impose only a set of limited constraints on the local systems managing the driver cards in the Member States.*

[…] (TACHOnet XML Messaging Reference Guide, version 1.41, page 8).

72. Without such a network, drivers could easily apply for a card in country A and in country B and be issued with a driver card in each country. This would of course have a significant impact on the security of the digital tachograph system.

4.3. – Issues to be solved

73. Contracting Parties need to:

- identify their competent authority to be issued with keys,
- adopt an AETR-RCA,

- issue a security policy,
- be issued with cryptographic keys,
- put in place procedures to issue cards,
- ensure the uniqueness of the cards to be issued.

4.4. – Proposals

74. Considering the timing for non EU AETR Contracting Parties to implement the digital tachograph system, it is proposed:

j) to implement proposals e), f) and g) mentioned above (see point 2.3, page 9),

k) to use the "Card issuing Guidelines" issued in the framework of the CIWG project for the Contracting Parties to put in place the appropriate procedures,

l) to offer assistance to the non EU AETR Contracting Parties in the framework of the MIDT project (www.eu-digitaltachograph.org),

m) to evaluate how non EU Contracting Parties could ensure the uniqueness of the cards to be issued by their CIAs,

n) at the mid-term, to outsource the maintenance of this system through an international call for tender.

5) Enforcement

75. AETR has been founded and developed to safeguard minimum standards in road transport for:

- fair competition,
- working conditions,
- road safety.

76. The philosophy behind the content of the existing legislation must remain at least unchanged. Provisions that are necessary or desirable for the analogue tachograph are also appropriate for the digital one.

77. Harmonisation of social legislation leads to uniform (or at least equivalent) procedures for all Contracting Parties. Boundary conditions for the whole field of transport business must be at least comparable on the AETR territory.

78. Effective enforcement is required to ensure that in general transport companies and drivers will comply with Drivers' Hours rules.

79. With the introduction of digital tachographs it is important to attain at least the same level of enforcement as with the analogue tachograph. However digital tachographs should also allow more efficient enforcement.

5.1. – Digital tachograph and enforcement

80. With digital tachographs and tachograph cards, enforcement will be based on digital data, spread over the digital tachograph mass memory and driver cards mass memory.

81. Some laws/decrees need therefore to be adopted at each national level to ensure the availability of data for control officers.

82. The main principles that should govern the management of data from digital tachographs and driver cards are that:

- transport undertakings are responsible for their own data ;
- they have to be considered as liable for any loss of data and
- they must, therefore, be in a position to hand over all data requested by the enforcement authorities within the prescribed time limits.

83. The conclusions reached by the experts having worked on this topic are that:

- for digital tachographs, there is an obvious need for downloading data for enforcement purposes ;
- downloading is preferred over producing print-outs as printouts will not guarantee the safety and accuracy of the data ;
- downloading should be performed at certain intervals and at certain defined fixed moments ;
- in order to be able to monitor compliance with AETR rules, it is necessary to have a continuous record, which can only be achieved by downloading all digital tachographs as well as all driver cards of the drivers working under the instructions of a transport company ;
- downloading of driver cards and digital tachographs should be mandatory ;
- there is insufficient legal basis, and no explicit requirement, in the AETR for mandatory downloading of the digital tachograph ;
- there is no legal basis at all in the AETR for mandatory downloading of driver cards.

84. Therefore, the recommendations are:

- That companies should use the lock-in facility as soon as they begin using a vehicle and lock-out immediately before permanently or temporarily transferring control of the vehicle to another company. To ensure the availability of timely data for enforcement purposes, downloading should occur:

  - For the Vehicle Unit:

- *Immediately before permanently or temporarily transferring control of the vehicle to another person[4] or company*
- *If it ceases to function correctly but can still be downloaded*
- *In any case, at least every three months.*

- For the Driver Card:

- *Prior to overwriting of data. The 28-day period referred to in Appendix IB is dependent on the driving pattern of the driver and also on the memory capacity of the particular card. If, in practice, all driver cards have a capacity of at least 32 kbytes, it is recommend that the driver card be downloaded at least once every 31 days. Otherwise, it is recommend that all driver cards be downloaded at least once every 21 days.*
- *Before the driver leaves his/her company (that is, when a driver ceases to be employed by a company or - where companies use self-employed drivers or drivers hired from an agency - at the end of the period for which that driver is used).*

- For either/both :

- *Data will have to be downloaded within 24 hours following a request by an enforcement officer involved in the investigation of a serious incident.*
- *Within 7 days in other cases.*
- *In any case, the downloaded data will be made available to the enforcement officer within 7 days of the request.*

- Companies should have a backup system for downloaded data: any downloaded data should be protected against accidental (or other) loss by provision of an adequate backup system.

Enforcement officers must also require a copy of the original files that have been downloaded to be presented in the original format and with the digital signature intact:

- by VRN and by driver ;
- in the chronological order that they have been downloaded;
- with file names to be clearly identifiable.

5.2. – Training and equipment

85. The way of checking drivers' activities through digital tachographs will change considerably compared to the way they are checked though analogue tachographs and paper discs.

[4] By this it is meant the transfer of a vehicle to a person acting as/or for another transport operator not the transfer of the vehicle to a driver employed by the same person or company.

86. Control officers need a proper training and to be supplied with enforcement tools (downloading facilities, computers, software, card readers…) to do efficient roadside and company checks.

87. Training and equipment have a cost that needs to be planned when implementing the digital tachograph system.

5.3. – Issues to be solved

88. Contracting Parties need to:

- adopt the necessary set of laws to deal with data management,
- train and equip their control officers.

5.4. – Proposals

89. Considering the timing for non EU-AETR Contracting Parties to implement the digital tachograph system, it is proposed:

o) to use the "Data Management report" issued in the framework of the IDT-MIDT project,

p) to offer assistance to non EU AETR Contracting Parties in the framework of the MIDT project (www.eu-digitaltachograph.org),

6) Data protection

90. The digital tachograph, as described in Appendix 1B records and stores digital data concerning individuals (drivers and enforcement officers) as well as legal persons (transport companies and approved workshops). See requirements 73 to 105 b of Appendix 1B.

91. These data are accessible in different ways, depending on whether or not tachograph cards are used to get access to them, and in case tachograph cards are used, depending on the type of card that is used (driver, company, control or workshop card) and of the mode of operation of the tachograph. See requirements 007 to 11 of Appendix 1B.

92. These data are also going to be downloaded and could also be transferred for freight and fleet management, but also for enforcement purposes. See requirements 149 to 151 of Appendix 1B.

93. Finally, the digital tachograph records and stores data on tachograph cards, to be issued to the different persons submitted to the provisions of the AETR. See requirements 108 to 112 of Appendix 1B.

94. Each tachograph card then contains data that are accessible in different ways.

See requirements 194 to 212 b of Appendix 1B for the driver card.

See requirements 213 to 230 a of Appendix 1B for the workshop card.
See requirements 231 to 234 of Appendix 1B for the control card.
See requirements 235 to 238 of Appendix 1B for the company card.

95. These data, their recording, their storing, their accessibility, their transfer and their use fall, at EU level, under the scope of the Directive n° 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

96. Therefore, non EU-AETR Contracting Parties which have to introduce the digital tachograph system shall make sure that their implementation scheme does not contradict their national data protection rules, if any.

6.1. – Issues to be solved

97. Contracting Parties need to check the compatibility of their implementation scheme against their national data protection rules.

6.2. – Proposals

98. Considering the timing for non EU AETR Contracting Parties to implement the digital tachograph system, it is proposed:

q) to use the "Data protection report" issued in the framework of the IDT-MIDT project (issued to the UN-AETR Secretariat),

r) to offer assistance to the non EU-AETR Contracting Parties in the framework of the MIDT project (www.eu-digitaltachograph.org).

7) Risk Management

99. The sound management of digital tachographs throughout their life-cycle is an essential national activity in order to minimise risk, and/or prevent the occurrence of adverse impacts.

100. The function of risk management is to decide whether a level of risk is acceptable, and if not, to translate the information into policies and actions designed to, for example, reduce risk through national legislative action, or to reduce risk in a variety of other ways.

101. Risks can occur at any, or all of the stages of the digital tachograph life-cycle, which may consist for example of:

- interoperability problems between digital tachographs and tachograph cards;
- wrong calibrations of digital tachographs;
- issuing of cards to unauthorised persons;
- manipulation of digital tachographs and/or of tachograph cards;

and

- alteration of the recorded data.

102. This is the reason why a risk management procedure is requested by each Member State at EU level and why an EU-wide risk management procedure has been set up under the responsibility of the European Commission.

103. The same should be done at AETR level to ensure the maintenance of the digital tachograph system once introduced in the non EU AETR Contracting Parties. This implies AETR Contracting Parties:

- to set up and implement a risk management procedure at national level,
- to nominate at their respective national level a Risk Manager who could be the interface with other Risk Managers at AETR level,
- to join, in one way or another, the EU Risk Management procedure and the EU Risk Management Group (EURMG), set up at EU level,
- to consequently consider with the UN AETR secretariat how to extend the EU Risk Management procedure to AETR level and to transform the EURMG into an AETR-EURMG

7.1. – Risk Management at national level

Rationale

104. The purpose of a risk management policy is to enhance the Trust's mechanism of risk management and to provide a procedure and supportive framework to manage and coordinate risk not compatible with the objectives of the introduction of the digital tachograph system. The policy provides information and guidance to enable a Risk Management Group to be set up at each national level, to:

- identify the immediacy, severity and likelihood of dangerousness,
- minimise and manage dangerousness,
- develop defensible practice,
- operate proactive rather than reactive risk management plans for the benefit of the various stakeholders,
- provide a framework for the sharing of confidential information across national risk management groups.

Scope

105. This policy applies to all the specific issues laid down under points 1 to 6 of this document and to any others that the Risk Management Group could decide to tackle.

Policy: Who should be involved in Risk Management Decision-Making at national level? Roles and responsibilities

106. AETR Contracting Parties are required to set up at their respective national level a Risk management group and procedure. This part of the procedure is left up to them to define since its structure depends on the political and administrative organisation of each of the AETR

Contracting Parties. It is expected anyway to be based on the Guidance document issued under the reference EU-MIDT-RMG-002-2006 rev 1.

107. When identifying the parties to be involved in risk management decision-making, it is important for AETR Contracting Parties to first establish what entity/entities will be responsible for, and have the authority to organise the work, to establish its scope, and determine any boundaries to the management process. It is also important to establish who will gather the necessary information, document and develop the recommended risk reduction strategy.

108. It is furthermore useful to identify at an early stage which public authority and/or non-governmental organisations (NGOs) might be responsible for the adoption, implementation and assumption of any liability for the risk strategy. Even if some parties are likely to play a main role only later in the process, e.g. during implementation, efforts should be made to involve them at an early stage in the process. Finally, interested and affected parties (stakeholders) that need to be consulted throughout the entire risk management process should be identified so that they adopt the concept of shared responsibilities.

109. As many different ministries play a role in the process of managing the digital tachograph system at the national level, any one of which may be an appropriate lead agency or supervisor for a particular problem. The title of Risk Manager(s) is sometimes applied to individuals or departments or agencies that will help supervise and manage this process. The relevant authorities involved may include:

- *Enforcement authorities: involved in road traffic enforcement;*
- *Workshops approval authorities;*
- *Card Issuing authorities: involved in the issuing of tachograph cards*;
- *Certification/Security authorities: involved in the overall security of* the system at *national level;*
- *Type approval authorities: involved in the type approval of digital tachographs and tachograph cards.*

110. Representatives of many of these authorities, along with national and/or international regulators and officials, should be involved in the risk management decision-making process. Technical experts as well as decision-makers may all be involved depending upon the nature of the issues and the stage of the decision-making process. Risk management responsibilities may well be shared between different ministries depending upon the complexity of the risk situation. It is unusual for only one ministry to be involved in such situations.

111. In addition to governmental participants, the risk management decision-making process should be carried out in continuous consultation with interested and affected parties, or “stakeholders”. Stakeholders are likely to include all those who are affected by the problem, or who might be affected by a proposed risk reduction measure. They may include, for example, associations of transport companies, unions, national associations of workshops and manufacturers. Discussions involving such diverse groups with a wide range of skills and abilities should be conducted in such a manner to be meaningful to participants without specialist knowledge.

Organising the Decision-Making Process at national level

112. The risk management decision-making process should ideally be orchestrated by a core working group which can draw on the expertise of, and promote communication among the various concerned ministries as well as other stakeholder groups. Such a group (or committee) should typically include, as a minimum, representatives of:

- type approval authorities,
- enforcement authorities,
- card issuing authorities,
- authorities approving and auditing workshops,
- authorities in charge of defining, implementing and auditing security policies at national and international level.

113. Each country will have to find the organisational arrangement that best meets its needs and that will be most likely to lead to cooperation among concerned parties. The process through which risk management decision-making is carried out and the degree to which concerned parties feel appropriately involved often is a key determinant of success and should be carefully considered and clearly communicated from the outset. While each problem may require a different approach for stakeholder involvement, formulating a decision-making process can help to increase transparency and ensure that the various concerned parties know what to expect and understand how they can effectively contribute to the process. Clearly, such a process should ensure that the credibility of the regulators and the government is upheld.

Conducting a Situation Analysis/Needs Assessment

114. An analysis of the situation is the first step and is really an examination of the national/international circumstances or conditions in which the issue occurs. This can provide insight into where challenges lie and where opportunities exist. It involves asking in broad terms: “what do we have?”, “what do we lack?”, and “what is inadequate?”. Some basic questions could include:

- which Ministry/Department(s) is/are involved in managing the digital tachograph system?
- What specific legislation/regulations are in place in the country?
- Is enforcement of regulations undertaken as necessary?
- What relevant industry(ies) is involved? Are there university departments, research institute or industry(ies) that are undertaking relevant research/investigations?
- What level of understanding exists in government and industry about the hazards the problem poses?
- What level of awareness exists among the various stakeholders?
- What related technical infrastructure exists (e.g. information on quantities of defective cards or digital tachographs in use)?
- Are there any “bottlenecks” in the management of the problem nationally and/or internationally?

115. Identification of the problem is the second important component when initiating the analysis. This means that the risks to – the problem – will be considered in the national or international context – the situation. When identifying the issue it is important at this stage to have an appreciation of the magnitude of the problem. Was it a "one-off" event, or is the problem an on-going one? Are large numbers of stakeholders directly affected or has the problem arisen through misuse?

AETR Contracting Parties are not only expected to set up a risk management group, they are also supposed to assess risks.

116. They are in that respect in the front line of the implementation of the digital tachograph system and have therefore to take an active part in the assessment and management of risks.

117. After having gone through their procedure, including an assessment of the issue, national Risk Management groups can conclude:

- that the issue was not a risk,
- that the issue can be characterised as a risk and that its impact is limited to their territory,
- that the issue can be characterised as a risk and that its impact is EU wide.

How to work with the AETR-EU Risk Management Group?

118. In all cases, national Risk Management Groups have to document the AETR-EU RMG accordingly.

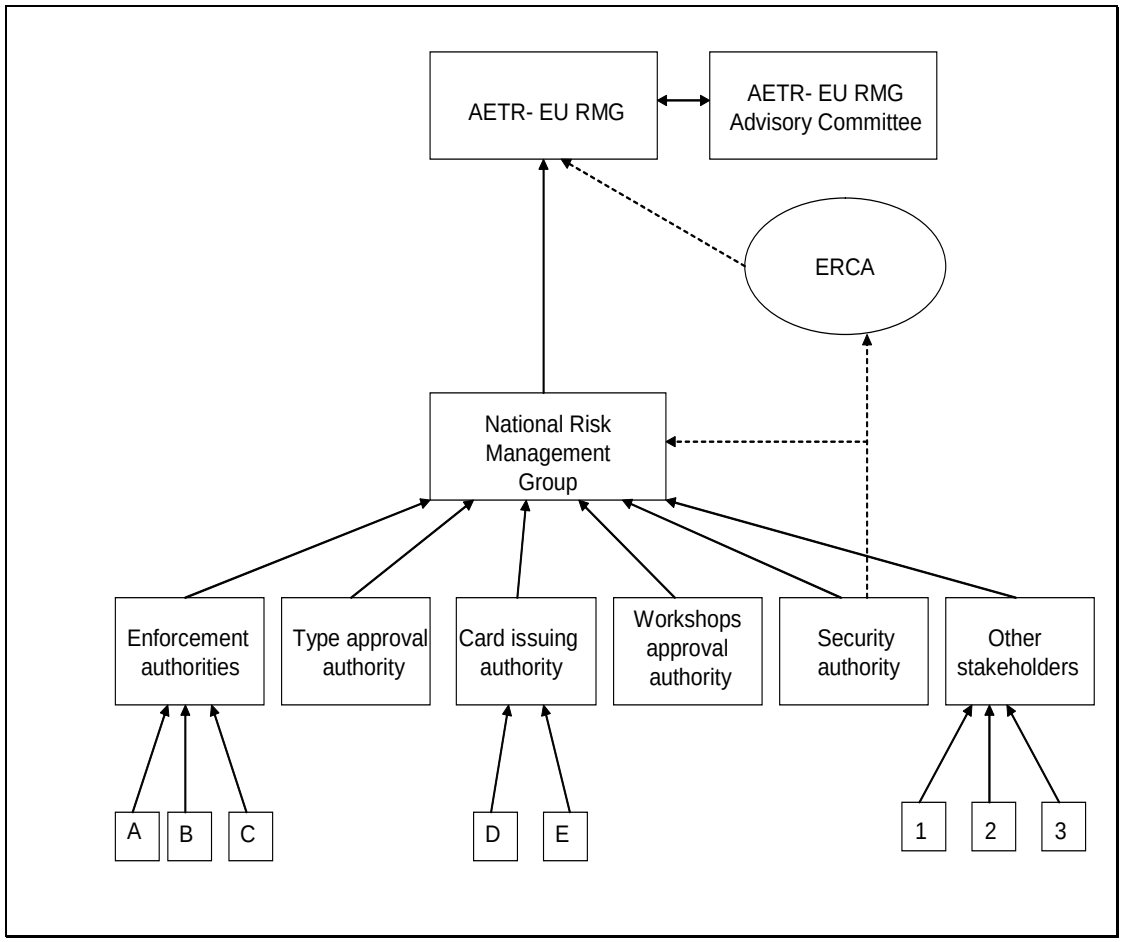
119. The role of the AETR-EU RMG would be to tackle all issues having an impact beyond the frontiers of the country which had initially to assess it and to come back with recommendations to be implemented at each Contracting Party's level.

120. A record of all of the information used in the problem analysis should be established as an example for future evaluators to study. Specific details should include not only the basic data and information, but also assumptions, controversies, uncertainties, etc. What data gaps were uncovered and how they were considered within the risk management options under discussion, are two further critical questions. Information should be stored not only on the immediate problems and their effects but also on the underlying causes so that a longer-term perspective is established. Such an approach should also help increase the degree of confidence within which the options were considered.

121. Receiving feedback on the problem analysis from affected stakeholders will also help strengthen the analysis. This sharing of knowledge helps create the shared responsibility necessary to select and develop the risk reduction strategy. The collection of such information constitutes in itself an important element of the analytical process.

122. National RMGs are invited to inform and document the AETR-EU RMG in English.

Step 1: from the national Risk Management Groups to the AETR- EU RMG



7.2. – Risk Management at AETR level

123. The AETR-EU risk management procedure begins with the initial referral to the AETR-EU RMG. The referral is made by registered mail or by secure e-mail.

124. The referral can be any national risk management group, international stakeholders like card, tachograph and vehicle manufacturers or their representations in Brussels as well as the UNO AETR secretariat and the European Commission itself.

125. When deciding to launch the AETR-EU RMG procedure, the following points should be communicated in a confidential manner by national risk management groups in justifying the referral:

- detailed description of the issue sent with documentation whenever applicable,
- date at which the issue has occurred,

- date at which the issue has been acknowledged by the national Risk Management group,

- identification of the stakeholders put at risk by the issue,
- identification of the digital tachograph system's characteristics put at risk by the issue,
- summary of the risk assessment conducted by the national risk management group,
- composition (full name, organisation and field of competence) of the experts having taken part in the assessment exercise,
- contact details of the risk manager and/or of the specific expert to contact,
- description of corrective action if any.

126. If no action is required by the national risk management group from the AETR-EU RMG, this latter has to:

- evaluate the assessment made by the national risk management group,
- inform in a confidential manner the other national risk management groups accordingly if the information is considered as adequate and appropriate,
- inform the referrer that further action is needed either at national level, or at European level to manage the risk identified if the assessment made and/or action undertaken are considered as unsatisfactory.

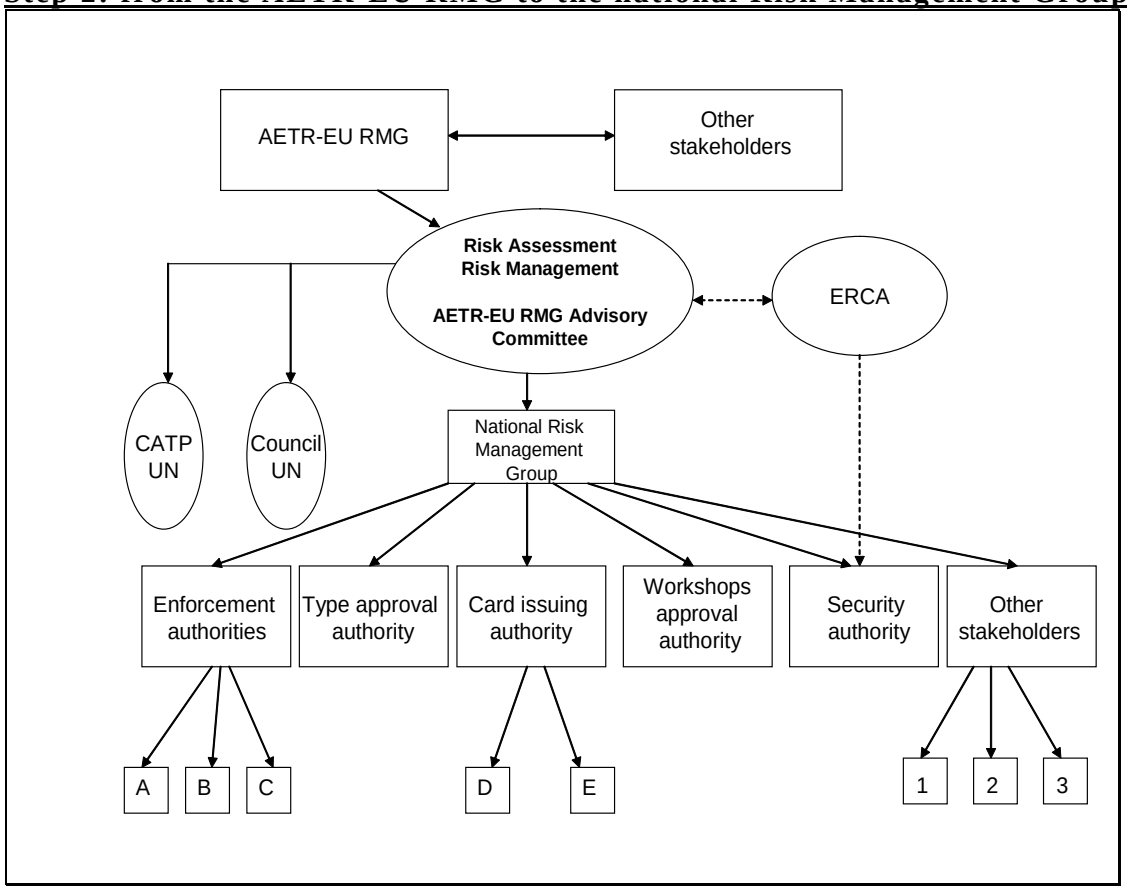
127. If action is required by the national risk management group from the AETR-EU RMG, because its impact goes beyond its national territory, the AETR-EU RMG has to:

- evaluate the assessment made by the national risk management group (it is nevertheless the responsibility of the "initiating referrer" to present the information which led to the AETR-EU RMG. It will be the responsibility of other stakeholders to bring information that is relevant, appropriate and proportionate to the management of risk),
- inform the national risk management group in case the issue is considered as being limited to its territory and request it to take the necessary measures,
- inform the other national risk management groups of its decision to send the request back to the referrer,
- if the case is considered as relevant, select on an *ad hoc* basis the members of the advisory committee who will have to assess the measures to be taken at European level,
- issue on a confidential manner and in English detailed recommendations to the national risk management groups covering the assessment of the risks and the actions to be taken, whenever actions can be taken in the framework of the existing legislative texts,
- issue in a confidential manner and in English detailed recommendations to the UN and/or EU legislator whenever the necessary actions to be taken cannot be implemented in the framework of the existing legislative and inform the national risk management groups accordingly,

- keep the data base up-to-date at all stages of the process.

128. The methodology to be followed by the AETR-EU RMG when assessing a risk and defining an action can be based on the Guidance document issued under the reference EU-MIDT-RMG-002-2006 rev 1.

Step 2: from the AETR-EU RMG to the national Risk Management Groups



7.3. – Issues to be solved

129. Each AETR Contracting Party will have to set up a risk management procedure at national level and design it so as to be able to work with the other AETR Contracting Parties in the scope of the AETR-EU Risk Management procedure to be implemented.

130. The role of the European Commission and of the UN AETR secretariat will have to be clarified in that respect.

7.4. – Proposals

131. Considering the timing for non EU-AETR Contracting Parties to implement the digital tachograph system, it is proposed:

s) the non EU-AETR Contracting Parties to use the Guidelines issued at EU level to implement their national risk management procedures,

t) to extend the EU Risk Management procedure to AETR Contracting Parties,

u) to ask the UN AETR secretariat to act as a contact point for the AETR-EU Risk Management Group when it has to deal with non EU-AETR Contracting Parties,

v) in the meantime, to offer assistance to the non EU-AETR Contracting Parties in the framework of the MIDT project (www.eu-digitaltachograph.org).

	Issues to be dealt with	Role of AETR Contracting Parties	Role of European Commission	Role of AETR-UN secretariat	Role of third parties	Timing	Guidelines
1	**Type approval**	Manufacturers can theoretically seek approval in each AETR Contracting Party (see article2 of the Annex) Ensure type approval of the cards to be issued See point 4	Type approval is a three-step process. Type approval can be granted only if the applicant has first been issued with a functional, a security and an interoperability certificate. The interoperability certificate can only be issued by a single body which is currently EC-DG JRC (see requirement 278)	Check of the cards' additional features Coordination of type approval disputes See point 4.1	See point 4.1	See point 4.1	**EU/MIDT/PLE/012-2006** Guidelines on type approval
2	**Security**	Necessity to issue a security policy ensuring the management of the keys to be issued by the ERCA and the maintenance of the digital tachograph system	EC-DG TREN/DG JRC (ERCA) Assessment of the security policies to be issued by AETR Contracting Parties	Acting as the AETR Authority (equivalent to the European Authority at EU level) Information Coordination	See point 4.1	See point 4.1	**EU/MIDT/PLE/009-2006** Certification Practises Statements EU/MIDT/PLE/010-2006 European Root Policy
3	**Workshop approval**	Necessity to approve workshops to deal with	None	Information Coordination	Tachograph manufacturers	From 12 to 18 months	**EU/MIDT/IPC/004-2006** *Guidelines to approve*

		installation, activation, calibration, repair/exchange, inspection, downloading and decommissioning of digital tachographs. This implies: - adoption of a new set of rules against which workshops will have to be approved - training of fitters - new calibration equipment to be bought by approved workshops - approval procedures to be completed					*workshops* **EU/MIDT/IPC/003-2006** *Guidelines on activation/calibration* **EU/MIDT/PLE/011-2006** *Guidelines on security at workshops* **EU/MIDT/PLE/008-2006** *Guidelines on decommissioning*

4-1	**Card issuing**	Adoption of set of rules to regulate the issuing of cards (application, issuing, renewal, replacement, exchange, withdrawal, etc) Setting up of a card issuing architecture (front desks, data bases, etc.). Cards to be issued need to be type approved (see point 1) Card issuing process needs to be covered by the security policy (see point 2). With the exception of the legislative and administrative process, all the technical part can be outsourced (tendering procedure)	None	Information Coordination See also points 1 and 4.2	Private companies (tendering procedure)	8 to 18 months	**EU/MIDT/CINC/028-2005** *Card Issuing Best Practises Guidelines*

4-2	**TACHOnet**	Connect their data bases/Card Issuing Authority (CIA) to a network so as to ensure the uniqueness of the cards to be issued. The connection to this network can be outsourced and be considered as one of the elements of the tender for a card issuing system	Ensure the compatibility of the AETR network with TACHOnet.	Information Coordination	Private companies (tendering procedure)	See point 4.1	**EU/MIDT/CINC/009-2006** *TACHOnet XML Messaging Reference Guide* **EU/MIDT/CINC/010-2006** *TACHOnet XML Network and Security Reference Guide* **EU/MIDT/CINC/011-2006** *TACHOnet Test Plan*
5	**Enforcement**	Adoption of the necessary set of rules to cover: - data download and access of data by control officers - eventually use of digital data as evidences before Courts Training of control officers	None	Information Coordination	Tachograph manufacturers (training of control officers) Private companies (equipment of control officers)	6 to 12 months	**EU/MIDT/ENC/003-2005 rev 1** *Guidelines to on Roadside checks* **EU/MIDT/PLE/005-2005** *Guidelines on company checks* **EU/MIDT/IPC/030-2005**

		- Equipment of control officers (can be subject of a tendering procedure)					*Guidelines on data management*
6	**Data protection**	Adoption of the necessary set of rules (or check existing rules) governing the recording, storage, access and use of digital data by transport companies, approved workshops and enforcement agencies	None	Information Coordination		6 to 12 months	**EU/MIDT/PLE/007-2006** *Guidelines on data protection*
7	**Risk Management**	Implement a risk management procedure so as to ensure the maintenance of the digital tachograph system once introduced in the field	AETR-EU Risk Manager	Information Coordination Interface with the AETR-EU Risk Manager as far as the non EU-AETR Contracting Parties are concerned	Can be involved at both national and AETR-EU levels when it comes to risks assessment	6 to 12 months	**EU/MIDT/RMG/003-2006 rev 1** *Guidance for risk management procedures to be implemented at national level* **EU/MIDT/RMG/004-2006** *EU risk management procedure*