Introduction of the digital tachograph

Meeting Geneva
14 May 2007
The speaker
Thierry GRANTURCO
GRANTURCO & Partners
French

- Legal adviser in the digital tachograph project : 1997 – 1999
- Legal adviser in the CEECs/digital tachograph project : 2000 – 2002
- Legal adviser in the IDT project : 2002 – 2004
- Legal adviser in the MIDT project : 2005 - …

Barrister at the Bar of Paris and at the Bar of Brussels

Phd in European Law
Phd in Political science
Phd in International relations

Professor of Law

Secretary General of CORTE (Confederation of Organisations in Road Transport Enforcement)
The agenda
1 – Introduction by the AETR/UNECE Secretariat and the European Commission

2 – Type approval

3 – Security policy

4 – Workshop approval

5 – Issuing of tachograph cards

6 – Enforcement

7 – Data protection

8 – Risk management

9 - Conclusion
1. Introduction
Considering the constant increase of:

- registration of passenger cars
- registration of commercial vehicles

as a consequence of this, the constant increase of:

- road traffic congestion
- road traffic accidents
- fatalities and injuries
- the number of heavy vehicles involved in fatalities

the EU legislator has decided in 1969 to regulate the professional drivers’ activities for the very first time.

Regulation (EEC) n° 543/69, Official Journal L 77, page 49
(see http://europa.eu.int/eur-lex/lex/en/index.htm)
This Regulation aimed mainly at:

- limiting driving time allowed by day and by week
- obliging professional drivers to record their activities through a recording equipment called “tachograph” or, alternatively, to use a kind of booklet

First generation of recording equipment in the EU
In the meantime, the EU signed in 1970 under the auspices of the United Nations an agreement called AETR extending the use of the recording equipment to the European but non EU Members (former Eastern countries, former Soviet republics, Balkan countries, etc…)

For EU drivers, the use of recording equipment became mandatory including outside the EU whilst for non EU AETR drivers, the use of recording equipment became mandatory for international journeys only

The UNO-AETR agreement foresees that each change of the recording equipment decided by the EU has to be implemented at AETR level so that each generation of recording equipment, as presented hereinafter, has also been the one used at AETR level
This Regulation changed considerably the drivers’ behaviour

But the recording equipment was not yet mandatory in the sense that booklets could be used instead

Therefore, to avoid any distortion of competition between transport operators, the EU legislator decided to amend the 1969 Regulation in 1985 and to introduce a recording equipment on a mandatorily basis for every professional driver

Except for very few exceptions
Regulation (EEC) n° 3821/85, Official Journal L 370, page 8
See http://europa.eu.int/eur-lex/lex/en/repert/0720.htm#07204020
This new Regulation:

• was much more demanding with drivers (in terms of driving, working, availability and rest times)

• increased the number of data collected by the tachograph through the charts used to record data (speed, time, distances, names of drivers/co-drivers, locations, vehicle registration numbers, etc… have to be recorded and stored)

• introduced new obligations for transport operators (in terms of breakdown or faulty operation of their tachograph)

• introduced more stringent requirements for the repair workshops to ensure a proper calibration of these recording equipments
Over the time, the recording equipment evolved and from mechanical became electronic.

First generation

Second generation
But both generations are anyway working with paper discs
Nevertheless, it became rapidly clear that analogue tachographs were tampered (paper discs not used, destroyed, withdrawn during journeys, parameters mechanically or electromagnetically altered, etc…).

Whereas experience has shown that the economic pressures and competition in road transport have led some drivers employed by road haulage companies to flout certain rules, particularly those concerning the driving and rest times laid down in Council Regulation (EEC) n° 3820/85 of 20 December 1985 on the harmonisation of certain social legislation relating to road transport;

Whereas blatant infringements and fraud present a road safety hazard and are unacceptable for reasons of competition for the individual driver who does respect the rules;

[...]  

Whereas to put an end to the most common abuses of the present system, it is therefore necessary to introduce new advanced equipment [...] ;

Whereas the total security of the system and its components is essential if recording equipment is to function efficiently;

Recitals 2, 3, 6 and 7 of Regulation (EC) n° 2135/98
The EU legislator decided therefore to introduce a new kind of recording equipment.
Obligations of the Member States’ authorities
Situation with analogue tachographs

- Manufacturers
- Type approval
- Control bodies
- Fitters
- Transport companies
- Workshops
- Drivers
2. Type approval
• Digital tachographs and tachograph cards are not type approved if they cannot work with all types of tachograph and of tachograph cards already type approved

• With analogue tachographs, the situation is different.

They are type approved with a particular type of paper disc.
Therefore, the applicant for a type approval has not anymore to be granted with one certificate, as it is the case with the analogue tachograph, but with four different certificates:

- a functional certificate;
- a security certificate;
- an interoperability certificate;
- a type approval certificate.
Type Approval Tests

↓

ITSEC evaluation

↓

Functional Tests

↓

Interoperability Tests
Card ITSEC evaluation: Requirements Annex I B

- Claimed Minimum Strength of Mechanisms
  - The minimum strength of mechanisms for the Tachograph Card is **High** as defined in ITSEC

- Level of Assurance
  - The target level of assurance for the Tachograph Card is ITSEC level **E3**
Card ITSEC evaluation: Result

• ITSEC assure that the card manufacturers implement the cards with the specified target levels

• The *static characteristics* of the cards and the corresponding manufacturing process are following the requirements
Card Functional Tests: Overview

1. Administrative examination
2. Visual inspection
3. Physical tests
4. Protocol tests
5. Card structure
6. Functional tests
7. Environmental Tests
Interoperability Tests

- Appendix 9 defines the interoperability tests:
- Mutual Authentication between VU and cards
- Read/Write Tests
  - activity scenarios
  - card downloading
  - card printout

ITSEC evaluation

Functional Tests

Interoperability Tests
In other words…
TYPE APPROVAL
Security evaluation

Tachograph recording equipment or smart card manufacturer

Accredited ITSEC Laboratory

Security tests in accordance with Appendix 10

Test result

ITSEC body

Successfully passed tests

Yes

ITSEC certificate

Test request

MICROSOFT CORPORATION
Pay to

Certificate
Test result

ITSEC certificate
TYPE APPROVAL
Functional tests

Test request

Tachograph recording equipment or smart card manufacturer

(Accredited) Laboratory

Functional tests in accordance with Appendix 9

Test result

Type approval authority

Successfully Passed tests

Yes

Functional certificate

Type approval authority

MICROSOFT CORPORATION

PAY TO

Certificate

Yes
TYPE APPROVAL
Interoperability tests

Tachograph recording equipment or smart card manufacturer

JRC laboratory
Ispra, Italy

Interoperability tests in accordance with Appendix 9

Test request
- ITSEC certificate
- Functional certificate

Successfully Passed tests

JRC laboratory
Ispra, Italy

Provisional Interoperability Certificate valid for a maximum of 6 months

Yes

MICROSOFT CORPORATION
Pay to

MICROSOFT CORPORATION
Pay to

MICROSOFT CORPORATION
Pay to

MICROSOFT CORPORATION
Pay to
TYPE APPROVAL

EC Type Approval

- ITSEC certificate
- Functional certificate
- Definitive Interoperability certificate

Certificate of Type Approval
TYPE APPROVAL
Type Approved Tachograph equipment/cards

MS
type approval authority

Certificate

JRC
Public web site with list of type approved recording equipment and tachograph cards models

http://dtc.jrc.it/pages/Root%20Certification.htm

Copy of Certificate of Type Approval
With analogue tachographs, your country had no responsibility whatsoever in type approval matters (tachographs and charts were approved in other Countries).

With digital tachographs, your country will have to require cards (to be issued to drivers, transport companies, workshops and control officers) to be type approved (even if your country decides to opt for another Member State’s cards, already type approved).
<table>
<thead>
<tr>
<th>Analogue tachographs</th>
<th>Digital tachographs</th>
</tr>
</thead>
<tbody>
<tr>
<td>No type approval required</td>
<td>Type approval required:</td>
</tr>
<tr>
<td></td>
<td>- either full type approval (functional, security, interoperability and type approval certificates) = develop own cards</td>
</tr>
<tr>
<td></td>
<td>- or simplified procedure = adaptation and type approval of a card already type approved by another Member State</td>
</tr>
</tbody>
</table>
The list of type approved cards can be found on the following web site:


Requirement 290 of Appendix 1B of the AETR

The main type approval authorities in the EU are the following:

- Kraftfahrt-Bundesamt - Germany
- Ministry of Industry – France
- Swedish Road Administration – Sweden

Their contact details can be found on the following web site:

http://www.eu-digitaltachograph.org/ContactDisplay.asp
The authorities granting security certificates are (only) the following:

- BSI (Germany): [http://www.bsi.bund.de/](http://www.bsi.bund.de/)
The authority granting interoperability certificates is (only) the following:

European Commission, DG JRC (Ispra, Italy): [http://dtc.jrc.it/text/IOT.html](http://dtc.jrc.it/text/IOT.html)

Requirement 278 of Appendix 1B of the AETR
Questions?
3. Security policy
Global Security Policy
Who / What is involved

- Sensor
- Display
- Card readers
- Processor
- Memory
- Printer

- External storage
- Manual records
- Driver Card

- Security Management
- Control Card
- Control Bodies
- Workshop Card
- Fitters Workshops

- (Security) Personalisation
  Card / VU / Sensor

- Manufacturers
  Card / VU / Sensor

- Type approval
- Transport companies

- Company Card
- Download
- Test Calibration

- VU
- BUS
- Drivers Inputs
Member States have to ensure the maintenance of the system once deployed in the field.

Before being issued with Member States keys (to be used to cipher cards before they are issued) Member States have to submit a security policy to the ERCA (European Commission – DG JRC)

Security policy has to be maintained
The European Commission (referred to as the European Authority) is responsible for the European Root Certification Authority (ERCA) of the cryptographic key management infrastructure supporting the digital tachograph system.

An ERCA policy has been approved by the European Authority on 9th 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.
It does not cover, therefore, the overall security of the digital tachograph system

Risk management
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”.
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:

- issuing of tachograph cards, including keys and certificates;
- issuing of vehicle unit keys and certificates;
- issuing of motion sensor keys;
- 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.
In simple terms:

- the EU/AETR key has to be used to certify the AETR Contracting Parties’ keys
- the AETR Contacting Parties’ key has to be used to certify the equipments’ and cards’ keys
- equipments and keys using these cryptographic keys can then exchange encrypted and therefore secure messages

No security policy = no national key = no possibility to issue and use cards
KEY Ceremony – Activation Data

Initial conditions, HSM activation data, HSM key backup custodian PINs, ERCA Boot and Root Passwords, Safe key combination settings and safe settings, Integrity CD passwords
KEY Ceremony – ERCA Workstation Setup

ERCA Boot Password setting, ERCA Software Initialization (copy of physical HD image)
KEY Ceremony – Initial Workstation configuration and hardening

First boot sequence, user account setup and login password setting
user permission setting
KEY Ceremony – ERCA key generation and key back-up

HSM configuration, ERCA slot creation and initialization (setting of HSM security mode), ERCA keys generation, creation of the two sets of key backup (2x2)
KEY Ceremony – Creation of ERCA Integrity CDs

Creation of the baseline integrity check data, creation of 4 copies of the Integrity CD
KEY Ceremony – Creation of ERCA Back-UP CDs, ERCA System First Reference State

Creation of the backup file set, creation of 4 copies of the integrity CD.

Shutdown of the system, start-up with an HD image utility, creation of the system first reference state.
KEY Ceremony – Conclusion

Completion of the logbook entry, sealing of envelopes, item distribution, closure of the Ceremony.
National authorities need therefore to:

- issue a security policy
- get it approved by the ERCA
- once approved, it has to be audited and maintained

**Timing: from 3 up to 6 months**

Work eventually to be done in close cooperation with your smart cards supplier
4. Approval of workshops
The Requirements

All workshops should be approved against two sets of criteria:

- Technical Competence and Facilities
- Suitability of Applicant (Fitters and Workshops)
Technical Competence and Facilities

Appropriate workshop facilities

Appropriate approved equipment

Suitably trained and competent technicians

Other considerations (e.g. health and safety guidelines).
Suitability of Applicant (Fitters and Workshops)

Repute (Honesty and Integrity)

References (Business and Personal)
Technicians Qualifications

Properly trained and understand the duties required of them;

Competent to carry out the work required of them;

Meet acceptable standards of reliability, honesty and integrity.
Control of Workshop Technicians

It remains for individual States, dependent on their individual administrative systems, to determine how to ensure that staff working for workshops, in particular the technicians, maintain standards and conduct their duties satisfactorily.

Control could be carried out by the Competent Authority, the Workshop Management, another agency or all of these provided that control is effective.
The Competent Authority will need to:

• Decide the period of validity of workshop approvals;

• Decide the fees for approval and/or renewal;

• Undertake (or delegate responsibility for) conducting periodic inspections of workshops, individual technicians, records, equipment and security aspects;

• Ensure that approval criteria are reviewed periodically to reflect changes and experience;

• Ensure that applications for workshop cards are screened and validated and that cards are not issued inappropriately.
The Competent Authority will also need to:

• Ensure that Workshop Cards are issued only for use at workshops within the State’s territorial jurisdiction.

• Ensure PINs are issued securely so as to be known only to the individual technician who will use the workshop card to which it provides access.

• Maintain a list of approved workshop seal code numbers and share this information with the other EU Member States.

• Approve and oversee a training programme for fitters
Workshops are basically approved to carry out:

- Installation (requirement 239)
- Activation (requirement 243)
- Calibration (requirement 248)
- Producing Plaques and Certificates (requirement 249)
- Sealing (electronic) (requirement 251)
- Periodic inspections (requirement 256)
- Downloading (requirement 260)
- Issue Undownloadability Certificates (requirement 261)
Monitoring and Control of Workshops

To work effectively and keep its integrity it is vital that workshops are properly monitored and controlled.

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

States shall have to determine the appropriate level of resources required to monitor the workshops to prevent the security elements of the scheme being compromised and to ensure that downloaded tachograph data is adequately safeguarded.
Disciplinary Procedures

The Competent Authorities who issue the approval for a workshop will need to take disciplinary action if:

• The workshop has failed to comply with the criteria of its original approval; or if,

• The standard of work falls below an acceptable level; or if,

• Malpractice or criminal activities have been detected.
Security of Workshops and Cards

To meet the EU/AETR vision, accuracy of the recording equipment is imperative.

Workshop cards in the wrong hands or misused, probably represents the highest risk to the integrity of (recorded) drivers hours data.

The individual technicians represent a key link in the security chain.

Essential that all workshop card activities are recorded in such a way that they provide a complete audit trail.
How should workshop cards be issued?

Given the importance workshop cards should be delivered to specific workshops or collected personally and signed for.

PINs will need to be issued to individual technicians under a separate cover completely.

It is for each State to decide exact procedures to ensure secure issue of cards to workshops and the secure issue of the PIN codes to the individual technicians who will use them.
Control of Workshop Cards and PINs

States need to ensure that secure arrangements exist to issue PINs to the individual technicians for whose use the workshop card is authorised;

After issue the PIN shall be the responsibility of the individual technician to whom it has been issued;

Individual technicians need to be aware of the security issues for Workshop Cards and PINs and to take responsibility for them whilst in their care.
Records and records keeping

In order to exercise control over the tachograph workshops and to maintain standards it is necessary to conduct audit.

Key to effective audit is the availability of accurate records.

For enforcement purposes it is important that a vehicle is found with an incorrectly set tachograph checks can be made at the workshop against whom the last inspection or calibration is attributed.
The management of tachograph workshops will need;

A register recording vehicle identity and VU details for all tachographs installed, activated, calibrated, inspected, repaired and decommissioned at the workshop.

As above for downloads from workshop cards to ensure a continuous and verifiable record of calibrations.

A record of all undownloadability certificates issued.

In addition all unused, spoilt, invalid or damaged certificates are retained for audit purposes;
<table>
<thead>
<tr>
<th>Analogue tachographs</th>
<th>Digital tachographs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval of workshops</td>
<td>Approval of workshops</td>
</tr>
<tr>
<td>Training of fitters</td>
<td>(New) Training of fitters</td>
</tr>
<tr>
<td>Equipment</td>
<td>(New) Equipment</td>
</tr>
<tr>
<td>Honesty</td>
<td>Honesty</td>
</tr>
<tr>
<td>Premises</td>
<td>(New) Premises</td>
</tr>
<tr>
<td>Audit</td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td>Data download</td>
</tr>
<tr>
<td></td>
<td>Workshop card management</td>
</tr>
</tbody>
</table>

Audit
Today: they check the seals
Tomorrow: they check the seals

Example of a motion sensor seal
Today: Data Accuracy

Dates, time, speed, distances, VRN and/or VIN, etc… These data may come from different sources but some of them, at some stages, will need to be calibrated. For example:

- when the recording equipment is installed
- when it is repaired
- when it is regularly checked
Tomorrow: programming
Keep The Records
Keep the data

INTERFACE FOR RAW SIGNED DATA DOWNLOAD

DATA STORAGE

COPY AND INTERPRET RAW DATA FOR ANALYSIS

OFFICE

INTERFACE TO VU

TCAS

OFFICE

MEMORY STICK

INTERFACE TO VU
Coexistence of two systems for workshops
National authorities need therefore to:

- issue or amend their national laws on the approval of workshops
- ensure the proper training of fitters
- ensure to set up a sufficient network of approved workshops at their respective national level

Timing: from 6 up to 16 months

Work to be done in close cooperation with tachograph manufacturers
Questions?
5. Card Issuing

TACHOnet
CARD ISSUING
Driver card

Personalised for use by the Driver

• 5 Year Validity Period

• Holds an average of 28 days data

• Driver must hold one card only
Workshop card

Used by approved tachograph fitters to install, activate, calibrate and download the recording equipment.

- One year validity period
- Personalisation recommended
- Issued with a PIN
Company card

Allows the company to ‘Lock and Download Data’ recorded in the vehicle unit.
Control card

Used by enforcers to carry out roadside compliance checks.

• Personalisation recommended
Card Application Types

**First Issue** - First application for a tachograph card

**Replacement** - Issued when a card is lost, stolen or malfunctions

**Exchange** - Change of administrative data

**Renewal** - Issued when a card is renewed after 5 years
Card Issuing Authority (CIA) Organisation

Centralised - database, application processing system, card personalisation & issue

De-Centralised - administrative desks for application processing with centralised database. Card personalisation either from central office or at administrative desks
Considerations for setting up a CIA

Application processing system

Database to hold & maintain records

Contract with smart card supplier/personaliser

Certification Authority
CIA Front Office
Operational concept

1. User fills the form
2. Filled form sent to scratch DB
3. Presents documentation (Driver's License, National ID or Passport, etc.)
4. Officer downloads form from scratch DB
5. User confirms & signs on PAD
6. Officer validates form data & takes pass picture
7. Form submitted to CIA

- CIA Front Office
- Users (Drivers, Companies, etc.)
- CIA Data Centre
- Internet (HTTPS)
CIA Front Office Architecture

<table>
<thead>
<tr>
<th>Símbolo</th>
<th>Qtde</th>
<th>Descrição</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌐</td>
<td>1</td>
<td>Modem ADSL/Cabo</td>
</tr>
<tr>
<td>🖥️</td>
<td>1</td>
<td>WINTEL PC</td>
</tr>
<tr>
<td>📷</td>
<td>1</td>
<td>“Webcam” para recolha de fotografia</td>
</tr>
<tr>
<td>🧑‍🌐</td>
<td>2</td>
<td>Agente SPTD e Requerente</td>
</tr>
<tr>
<td>📋</td>
<td>1</td>
<td>Ecrã ou superfície clara</td>
</tr>
<tr>
<td>🤖</td>
<td>1</td>
<td>“Smartcard reader” para autenticação do Agente SPTD</td>
</tr>
<tr>
<td>🔒</td>
<td>1</td>
<td>Firewall</td>
</tr>
<tr>
<td>📦</td>
<td>1</td>
<td>PAD digital p/ recolha de assinatura</td>
</tr>
<tr>
<td>🌐</td>
<td>1</td>
<td>Ligação Internet segura</td>
</tr>
</tbody>
</table>

WINTEL PC
Windows XP Pro

Firewall integrado no Posto de Atendimento

Ligação Internet ADSL ou Cabo (HTTPS)
CIA Data Centre
Functional Architecture

Legend

<table>
<thead>
<tr>
<th>SPTD – CIA Data Center</th>
<th>Qtd</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web server</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Directory server</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>SQL5 DB server</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>BizTalk server</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>MOM server</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>GBit Ethernet LAN</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Ligações privadas seguras</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Email server</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Monitoring of the Implementation of Digital Tachograph

Website: www.eu-digitaltachograph.org
E-mail: secretariat@eu-digitaltachograph.org
MSCA Data Centre
Functional Architecture

SPTD – MSCA
High Security Data Center

<table>
<thead>
<tr>
<th>Simbolo</th>
<th>Qty</th>
<th>Descrição</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>Public/private key server</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Database server</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Firewall</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Certificate server</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>High Security Module (FIPS 140-2 level 3)</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Ligasções privadas seguras</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Card Personaliser</td>
</tr>
</tbody>
</table>

High Security Data Center specs
MSCA Data Centre
Systems Architecture

2 Servidores de Geração de Chaves/Certificados
Proliant ML310
1 CPU p640
1 GB RAM
2xHDD 160GB SATA
Bastidor de 14U’s em opção

HSM from nCipher
Model “nShield F3 PCI”
FIPS 140-2 level 3 Cert # 527
CIA-MSCA Networking Architecture

Site Principal

Switch
24 x10/100

Router/ Switch
1 WAN
2 LAN

Metro Ethernet WAN Network

Site MSCA

Site DR

Router/ Switch
2 WAN
2 LAN
Communication Protocols

1. End of Day card batch submission
2. KCR
3. KDR
4. Confirmation
CIA Planning
## CIA

### Tracking Gantt To Date

<table>
<thead>
<tr>
<th>ID</th>
<th>Task Name</th>
<th>30 Jan '06</th>
<th>13 Feb '06</th>
<th>27 Feb '06</th>
<th>13 Mar '06</th>
<th>27 Mar '06</th>
<th>10 Apr '06</th>
<th>24 Apr '06</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SPTD CIA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Pré Projecto</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Definição de âmbito e requisitos</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>(M) Aprovação de âmbito e requisitos</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Definição da arquitectura de Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Definição da arquitectura de Rede</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Definição da arquitectura de Hardware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Definição de protocolo de comunicações com CP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>(M) Aprovação do projecto</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Projecto</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Definição da equipa do projecto</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Instalação de Hardware e Software para Desenvolvimento</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Análise e Desenho</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Base de dados</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Módulo de Atendimento</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Módulo de Consultas</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Módulo Web</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Business Intelligence Engine</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Comunicações (CP/TACHOnet/RNT)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Comunicações com CP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Comunicações com TACHOnet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Comunicações com RNT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>(M) Aprovação da análise do sistema</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Desenvolvimento</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>Beta Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>Teste e Aceitação do Projecto p/ MSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>Implementação do sistema</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Task Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>-----------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Pré Projecto</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Definição de âmbito e requisitos</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Definição da arquitetura de rede</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Definição da arquitetura de software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Definição de protocolo de comunicações KCR (Key Certification Request) para CP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Definição de protocolo de comunicações KDR (Key Distribution Request) para CP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Definição da arquitetura de rede</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Definição da arquitetura de software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Definição de protocolo de comunicações KCR (Key Certification Request) para CP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Definição de protocolo de comunicações KDR (Key Distribution Request) para CP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Aprovação do projecto</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Definição da equipa de projecto</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Instalação de hardware e software para desenvolvimento e testes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Análise e Desenho</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Desenvolvimento</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Teste e Análise do Projecto p/ MSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Definição das Disposições Práticas da MSCA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Aprovação das Disposições Práticas pela MSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Testes de aceitação</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Definição das Disposições Práticas da MSCA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Instalação de hardware e software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Instalação de rede</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Testes de pré-produção</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Implementação do sistema</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Gestão dos canais nacionais</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Implementação do sistema</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Testes de aceitação</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Definição das Disposições Práticas da MSCA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Aprovação das Disposições Práticas pela MSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Monitoring of the Implementation of Digital Tachograph**

Website: [www.eu-digitaltachograph.org](http://www.eu-digitaltachograph.org)
E-mail: secretariat@eu-digitaltachograph.org
## MSCA Tracking Gantt To Date

<table>
<thead>
<tr>
<th>ID</th>
<th>Task Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SPTD MSCA</td>
</tr>
<tr>
<td>2</td>
<td>Pre Project</td>
</tr>
<tr>
<td>3</td>
<td>Definição do âmbito e requisitos</td>
</tr>
<tr>
<td>4</td>
<td>(M) Aprovação do âmbito e requisitos</td>
</tr>
<tr>
<td>5</td>
<td>Definição da arquitectura de Software</td>
</tr>
<tr>
<td>6</td>
<td>Definição da arquitectura de Rede</td>
</tr>
<tr>
<td>7</td>
<td>Definição da arquitectura de Hardware</td>
</tr>
<tr>
<td>8</td>
<td>Definição de protocolo de comunicações KCR (Key Certification R)</td>
</tr>
<tr>
<td>9</td>
<td>Definição de protocolo de comunicações KDR (Key Distribution R)</td>
</tr>
<tr>
<td>10</td>
<td>(M) Aprovação do projecto</td>
</tr>
<tr>
<td>11</td>
<td>Projecto</td>
</tr>
<tr>
<td>12</td>
<td>Definição da equipa do projecto</td>
</tr>
<tr>
<td>13</td>
<td>Instalação de Hardware e Software para Desenvolvimento e Teste</td>
</tr>
<tr>
<td>14</td>
<td>Análise e Desenho</td>
</tr>
<tr>
<td>15</td>
<td>Base de dados</td>
</tr>
<tr>
<td>16</td>
<td>Software de certificação</td>
</tr>
<tr>
<td>17</td>
<td>Protocolos KCR/KDR</td>
</tr>
<tr>
<td>18</td>
<td>(M) Aprovação da análise do sistema</td>
</tr>
<tr>
<td>19</td>
<td>Desenvolvimento</td>
</tr>
<tr>
<td>23</td>
<td>Beta Testing</td>
</tr>
<tr>
<td>26</td>
<td>Teste e Aceitação do Projecto p/ MSA</td>
</tr>
<tr>
<td>27</td>
<td>Disposições práticas da MSCA</td>
</tr>
<tr>
<td>28</td>
<td>Definição da política nacional de segurança</td>
</tr>
<tr>
<td>29</td>
<td>Definição das Disposições Práticas da MSCA</td>
</tr>
<tr>
<td>30</td>
<td>Aprovação das Disposições Práticas pela MSA</td>
</tr>
<tr>
<td>31</td>
<td>Testes de aceitação</td>
</tr>
<tr>
<td>32</td>
<td>(M) Aceitação</td>
</tr>
<tr>
<td>33</td>
<td>Implementação do sistema</td>
</tr>
</tbody>
</table>

### Timeline

- **30 Jan '06**
- **13 Feb '06**
- **27 Feb '06**
- **13 Mar '06**
- **27 Mar '06**
- **10 Apr '06**
- **24 Apr '06**
- **08**

### Progress

- **30 Jan '06**: 40%
- **13 Feb '06**: 29%
- **27 Feb '06**: 0%
- **13 Mar '06**: 0%
- **27 Mar '06**: 22-03
- **10 Apr '06**: 0%
- **24 Apr '06**: 12%

---

Website: [www.eu-digitaltachograph.org](http://www.eu-digitaltachograph.org)
E-mail: secretariat@eu-digitaltachograph.org

Monitoring of the Implementation of Digital Tachograph
Questions?
TACHONET
TACHOnet Project Objectives

Create a telematics network aiming at facilitating data exchange between national administrations in charge of issuing tachographs cards

TACHOnet network:

- Ensures a reliable and secure exchange of necessary and sufficient data between States issuing tachograph cards
- Makes sure the exchange is done within the legal constraints stated in the EU-AETR rules
- Imposes only limited constraints on the local systems managing cards in the different States

TACHOnet project is owned by European Commission DG TREN
TACHOnet Business Actors

Clerks working for National Card Issuing Authorities (CIA)
Control officers working for National Enforcement Authorities

**Clerk @ CIA**
- Applies for a card, asks for exchange, declare card status modification
- Issues, Checks, Modifies

**Control officers**
- Checks, Modifies
- Controls during road checks

**Truck driver**
- Owns & uses

**TACHOnet XML Messaging System**
- Owns & uses

**Monitors & controls**
- During road checks
Scope and Exclusions of TACHOnet

Organisational:

1. Included:

   • Central secure and reliable XML messaging system allowing competent authorities to exchange information about tachograph cards based on well defined interfaces
   • Intelligent router between States (hub & spoke)
   • Central logging/tracking for non-repudiation & statistics
   • Access granted at State level using digital certificates handled by IDA PKI services.
Scope and Exclusions of TACHOnet

Organisational:

2. Not included:

  • Establishment of card holders data bases is the responsibility of each State

  • Access to the TACHOnet network within each State is under the responsibility of each State
Scope and Exclusions of TACHOnet

Business processes:

1. Included:
   
   • Check that an applicant for a card in a State does not already hold a valid card in another State

   • Check the actual status of a tachograph card based on its number/index (useful for control authorities)

   • Information about lost, stolen, defective cards, as well as about exchange of driver cards
Scope and Exclusions of TACHOnet

Business processes:

1. Included:
   - Information interchange about the usage of a driving license number for an issued card
   - Provide a central Greek or Latin to US/Ascii transliteration service
   - Provide a central service for getting the Phonex search keys of a driver’s surname and first of first names
   - Produce irrefutable statistics about activities (response by request, average response time/delay,...) for every State
Scope and Exclusions of TACHOnet

Business processes:

2. Not included:

- Check for driver license number by integrating calls to external systems
National authorities need therefore to:

- exchange information making sure that they do not issue a card to an applicant who already holds one
- connect to TACHOnet?
- set up an AETR net to be connected to TACHOnet?

**Timing:** ?

Coordination between the EC and the UN/AETR Secretariat highly recommended
<table>
<thead>
<tr>
<th>Analogue tachographs</th>
<th>Digital tachographs</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Security management</td>
<td>- Security management</td>
</tr>
<tr>
<td>Security policy</td>
<td>Security policy</td>
</tr>
<tr>
<td>Security audits</td>
<td>Security audits</td>
</tr>
<tr>
<td>- Issuing of cards</td>
<td>- Issuing of cards</td>
</tr>
<tr>
<td>- Connection to a net or active exchange of information between AEKR Contracting Parties</td>
<td>- Connection to a net or active exchange of information between AEKR Contracting Parties</td>
</tr>
</tbody>
</table>
Questions?
6. Enforcement
Enforcement

With analogue tachographs
Are recorded

Speed
Distance
Mode of work
Time
Manipulations can be detected (1)

Analogue Distance Trace

Odometer Distance is insufficient to match geographical locations
Manipulations can be detected (2)

Distance from known highway feature e.g. peage, is insufficient to reach check site

Analogue Distance Trace
Analysis software can also be used once data are scanned (1).
Analysis software can also be used one data are scanned (2)

Digital Distance Trace

Distance from known highway feature e.g. peage, is insufficient to reach check site
Enforcement

With digital tachographs
Data can be downloaded by control officers if issued with control cards
Alternative for the control officers to get access to the recording equipment’s and card’s data: printouts

6 types of print-outs, which can be selected through the recording equipment:

• 2 relate to the drivers’ activities: one comes from the recording equipment, the other one from the driver card;

• 2 relate to the events and faults: one from the recording equipment, the other one from the driver card;

• 1 concerns the technical data (vehicle, recording equipment, etc…);

• 1 concerns the over speeding.
Example: drivers’ activities stored on the driver’s card

```
<table>
<thead>
<tr>
<th>▼ 15/10/1997 15:15 (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td># DavidFish</td>
</tr>
<tr>
<td># GB/4803992633</td>
</tr>
<tr>
<td>#</td>
</tr>
<tr>
<td>▼ 14/10/1997</td>
</tr>
<tr>
<td># WALSTER</td>
</tr>
<tr>
<td>Nick D.</td>
</tr>
<tr>
<td># GB/13579642</td>
</tr>
<tr>
<td>14/05/2004</td>
</tr>
<tr>
<td># XAD1117483A</td>
</tr>
<tr>
<td>B/RV1772</td>
</tr>
<tr>
<td><strong>Tacho-Manufacturer</strong></td>
</tr>
<tr>
<td><strong>Tacho-Part-Number</strong></td>
</tr>
<tr>
<td><strong>Workshop-Name</strong></td>
</tr>
<tr>
<td># GB/159482637</td>
</tr>
<tr>
<td># 05/03/1997</td>
</tr>
<tr>
<td>1 Printing - Date &amp; Time (UTC)</td>
</tr>
<tr>
<td>2 Controller - Name</td>
</tr>
<tr>
<td>3 Control Place (Hand written)</td>
</tr>
<tr>
<td>4 Type of Print-Out (Card) &amp; Enquiry date</td>
</tr>
<tr>
<td>5 Driver - Last Name</td>
</tr>
<tr>
<td>6 Driver Card - Number</td>
</tr>
<tr>
<td>7 Vehicle - VIN</td>
</tr>
<tr>
<td>8 Tachograph - Manufacturer Name</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
```

Website: www.eu-digitaltachograph.org
E-mail: secretariat@eu-digitaltachograph.org
### Delimiter driver information

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00:00</td>
<td>06:17</td>
<td>06h18</td>
</tr>
<tr>
<td>9</td>
<td>Card not inserted. Activity unknown.</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Card insertion</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Detailed activities with</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Odometer, Distance travelled at Card withdrawal</td>
<td></td>
</tr>
</tbody>
</table>

#### B/PV1772

- **42000 km**

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>06:18</td>
<td>07:42</td>
<td>01h25</td>
</tr>
<tr>
<td>07:43</td>
<td>07:53</td>
<td>00h11</td>
</tr>
<tr>
<td>07:54</td>
<td>08:00</td>
<td>00h07</td>
</tr>
<tr>
<td>42010 km; 10 km</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### B/PV1772

- **42010 km**

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:01</td>
<td>08:13</td>
<td>00h13</td>
</tr>
<tr>
<td>08:14</td>
<td>11:20</td>
<td>03h07</td>
</tr>
<tr>
<td>11:21</td>
<td>12:33</td>
<td>01h13</td>
</tr>
<tr>
<td>42263 km; 253 km</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### B/HKG264

- **81000 km**

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:12</td>
<td>16:03</td>
<td>01h52</td>
</tr>
<tr>
<td>16:04</td>
<td>18:00</td>
<td>01h57</td>
</tr>
<tr>
<td>18:01</td>
<td>18:01</td>
<td>00h01</td>
</tr>
<tr>
<td>81111 km; 111 km</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### B/HKG264

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>18:02</td>
<td>23:59</td>
<td>05h58</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Facts above 1 hour marked with a star.

---

**Website:** [www.eu-digitaltachograph.org](http://www.eu-digitaltachograph.org)

**E-mail:** secretariat@eu-digitaltachograph.org

---

**Monitoring of the Implementation of Digital Tachograph**
<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
<th>Odometer</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>06:19</td>
<td>F</td>
<td>04h59</td>
<td>374 km</td>
</tr>
<tr>
<td>18:00</td>
<td>E CAT</td>
<td>03h42</td>
<td>00h11</td>
</tr>
<tr>
<td>01h14</td>
<td>?</td>
<td>13h54</td>
<td></td>
</tr>
<tr>
<td>05:25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12/09/1997 18:24</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12/09/1997 18:23</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>05/09/1997 06:35</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BIT/836254363</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21/08/1997 12:45</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21/08/1997 12:46</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Data analysis
<table>
<thead>
<tr>
<th>Analogue tachographs</th>
<th>Digital tachographs</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Roadside checks</td>
<td>- Roadside checks</td>
</tr>
<tr>
<td>- Company checks</td>
<td>- Company checks</td>
</tr>
<tr>
<td>based on paper discs</td>
<td>based on paper discs</td>
</tr>
<tr>
<td></td>
<td>based on print-outs</td>
</tr>
<tr>
<td></td>
<td>based on digital data</td>
</tr>
<tr>
<td></td>
<td>New equipments required</td>
</tr>
<tr>
<td></td>
<td>Control cards to be issued</td>
</tr>
<tr>
<td></td>
<td>Specific training to be supplied</td>
</tr>
</tbody>
</table>
National authorities need therefore to:

- issue laws to allocate control officers with new powers, to regulate data download, to define under which conditions electronic data can be used before Courts, etc…

- train their control officers

- equip them appropriately

**Timing: (6 to 24 months)**

National authorities should seek support from EU Member States and manufacturers
Questions?
7. Data protection
Data protection

- The digital tachograph falls under the scope of data protection rules for different reasons:
  - The digital tachograph **records and stores digital data** concerning individuals (mainly drivers) as well as legal persons (transport companies and approved workshops)

See requirements 73 to 105 b of AETR Appendix 1B
Data protection

• **These data are accessible** in different ways, depending on whether or not tachograph cards are used, and in case tachograph cards are used, depending on the type of cards that is used (driver, company, control or workshop cards) and of the mode of operation of the tachograph.

See requirements 007 to 11 of the AETR Appendix 1B
Data protection

• These data are also **downloaded** and can also be **transferred** for freight and fleet management, but also for enforcement purposes

See requirements 149 to 151 of AETR Appendix 1B
Data protection

- 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 the AETR Appendix 1B
• Each tachograph card contains data, that are accessible in different ways regulated notably and mainly by the AETR as far as enforcement is concerned

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

  See requirements 213 to 230 a of the AETR Appendix 1B for the workshop card

  See requirements 231 to 234 of the AETR Appendix 1B for the control card

  See requirements 235 to 238 of the AETR Appendix 1B for the company card
Data protection

• These data, their recording, their storage, the way they can be accessed, their transfer and their use fall under the scope of the data protection rules (if any in the non EU-AETR Contracting Parties)

• Therefore, Contracting Parties which have to implement the amendments to the AETR shall make sure that their implementation scheme does not contradict their data protection rules
Operational Modes
Data Read Access Rights

With his/her driver card, a driver can display, print all data related to him/herself, the other ones being “anonymous”

With his/her control card, a control officer can display, print, download ALL data,

With its company card, a company can display and print all data not locked by another company,

Without card, all data can be displayed or printed except personal identification (Names and Card numbers) which is blinded. Access limited to 8 days.
# Operational Modes
## Data Read Access Rights

<table>
<thead>
<tr>
<th>Print Display</th>
<th>No Card</th>
<th>Driver Card</th>
<th>Control Card</th>
<th>Company Card</th>
</tr>
</thead>
<tbody>
<tr>
<td>All data with personal identifiers blinded</td>
<td>All own data</td>
<td>All data</td>
<td>All data except for periods locked by other companies + Idem No Card</td>
<td></td>
</tr>
<tr>
<td>Forbidden</td>
<td>Forbidden</td>
<td>All data</td>
<td>All data except for periods locked by other companies</td>
<td></td>
</tr>
<tr>
<td>Download</td>
<td>Idem No Card</td>
<td>Idem No Card</td>
<td>Idem No Card</td>
<td>Idem No Card</td>
</tr>
</tbody>
</table>

**Monitoring of the Implementation of Digital Tachograph**

Website: [www.eu-digitaltachograph.org](http://www.eu-digitaltachograph.org)

E-mail: secretariat@eu-digitaltachograph.org
<table>
<thead>
<tr>
<th>Analogue tachographs</th>
<th>Digital tachographs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data protection</td>
<td>Data protection</td>
</tr>
<tr>
<td>No or few requirements</td>
<td>Digital tachograph’s and tachograph cards’ data are submitted to data protection rules (if any)</td>
</tr>
</tbody>
</table>
8. Risk management
Point 5.3.38 of the ERCA policy states that:

_The MSA shall establish an information security management system (ISMS) based on risk assessment for all the operations involved._

The ERCA does not cover the overall security of the digital tachograph system
From national authorities to the EU/AETR-RMG

- Enforcement authorities
- Type approval authority
- Card issuing authority
- Workshops approval authority
- Security authority
- Other stakeholders
- National Risk Management Group

EU/AETR-RMG
EU/AETR-RMG Advisory Committee
ERCA

From national authorities to the EU/AETR-RMG...
From the EU/AETR-RMG to national authorities

- EU/AETR-RMG
- Other stakeholders

Risk Assessment
Risk Management
EU/AETR-RMG Advisory Committee

ERCA

AETR SC1
CATP
Council

National Risk Management Group

Enforcement authorities
Type approval authority
Card issuing authority
Workshops approval authority
Security authority
Other stakeholders

A B C
D E

1 2 3
<table>
<thead>
<tr>
<th>Analogue tachographs</th>
<th>Digital tachographs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk management</td>
<td>Risk management</td>
</tr>
<tr>
<td>No requirement</td>
<td><strong>Policy to be implemented and maintained</strong></td>
</tr>
</tbody>
</table>
National authorities need therefore to:

- put in place a national risk management policy
- nominate responsible bodies/persons
- maintain this policy

**Timing:** (2 to 6 months)
Questions?
9. Conclusion
Overview of the Project Organisation
Tachograph life cycle
Approval of workshops
Roadside checks
Company checks
Data management
Card issuing
TACHOnet
Data protection
Risk management
Security

► EU-MIDT/PLE/008-2006
► EU-MIDT/PLE/004-2006
► EU-MIDT/PLE/003-2005 rev 3
► EU-MIDT/PLE/005-2006
► EU-MIDT/IPC/030-2005
► EU-MIDT/CINC/028-2005
► EU-MIDT/PLE/009-2006
► EU-MIDT/PLE/007-2006
► EU-MIDT/RMG/004-2006
► EU-MIDT/PLE/011-2006
Scope of the Project
Four Work Packages

- Help Desk
- Communication and Training Actions
- Support to the new Member States
- Support to the UNO-AETR Secretariat and to the AETR countries

Fora for Member States

- Plenary
- Enforcement Committee
- Implementation Policy Committee
- Card Issuing & Networking Committee
- TACHOnet User Group
- Risk Assessment Group
Support to the AETR Countries
Objectives

Helping the control authorities of AETR Contracting parties to face the digital tachograph and the AETR Contracting parties to introduce the digital tachograph by 2010

Three informative workshops to be organised

Help desk

Specific documentation can be made available (in English – IDT deliverables)
THANK YOU VERY MUCH
FOR YOUR ATTENTION