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 Enforcement/3820 project : 1999 – 2001
- 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** (**C**onfederation of **O**rganisations in **R**oad **T**ransport **E**nforcement)

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:

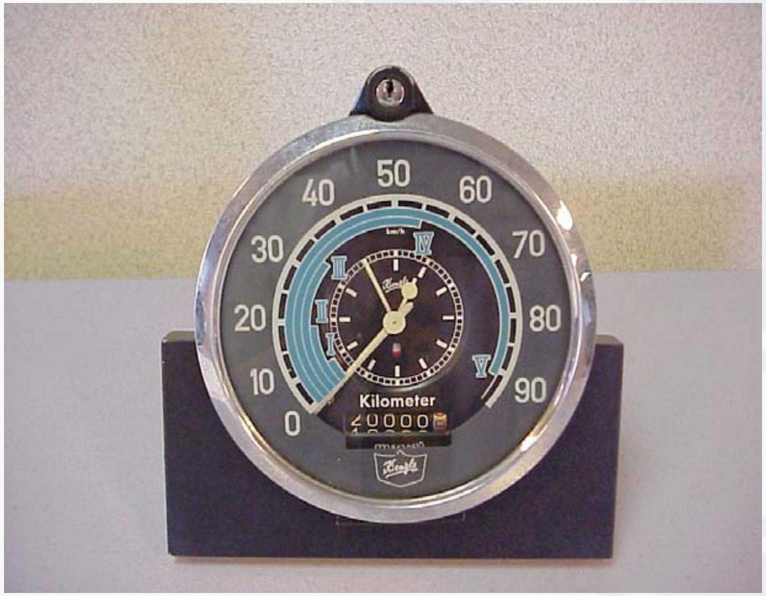
- road traffic congestion
- road traffic accidents
- fatalities and injuries
- the number of heavy vehicles involved in fatalities

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)

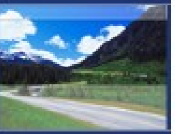
- introduced new obligations for transport operators (in terms of breakdown or faulty operation of their tachograph)

- introduced more stringent requirements for the repair workshops to ensure a proper calibration of these recording equipments

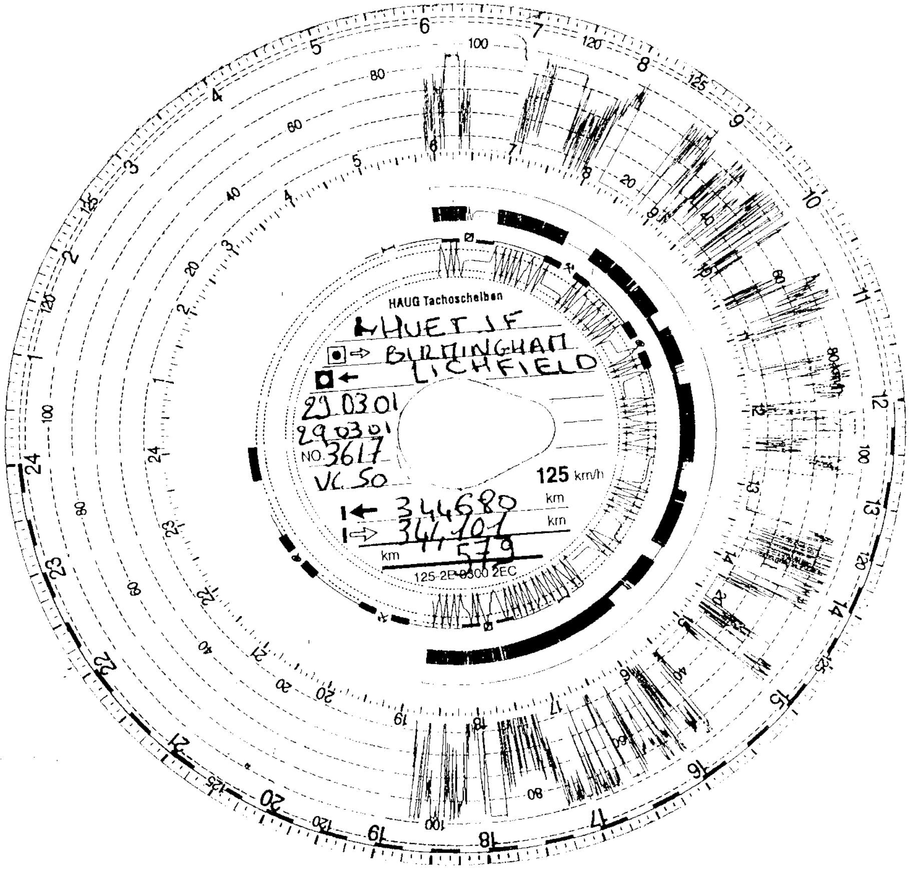
Over the time, the recording equipment evolved and from mechanical became electronic

First generation

Second generation



But both generations are anyway working with paper discs



HAUG Tachoscheiben

HUET J F

BIRMINGHAM

LICHFIELD

29.03.01

29.03.01

NO. 3617

VC 50

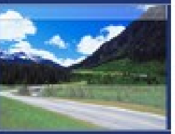
125 km/h

344680 km

344101 km

km 579

125-2E-0300 2EC



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;

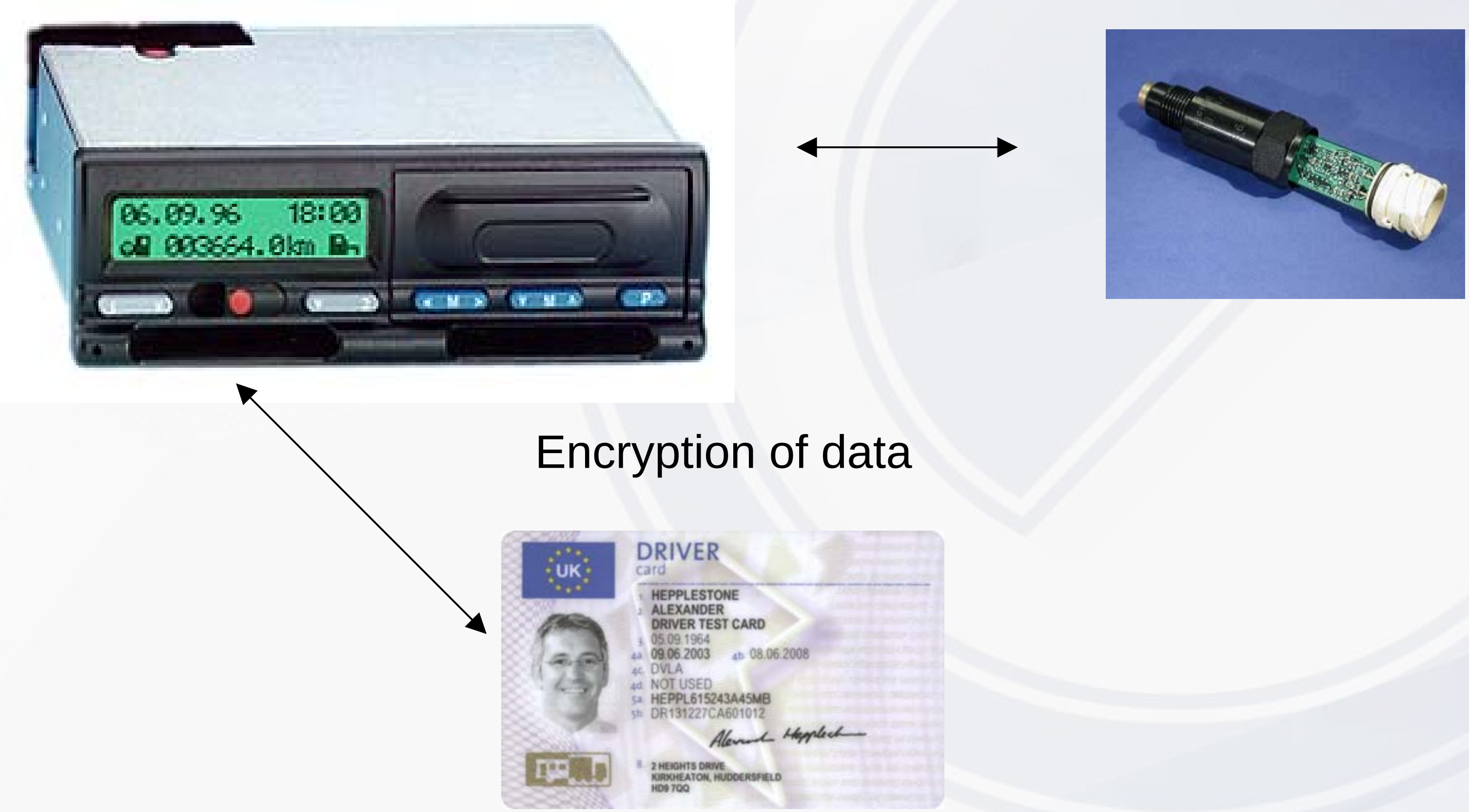
[…]

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

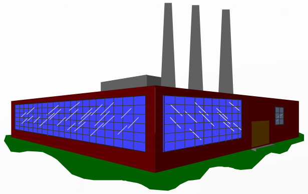
The EU legislator decided therefore to introduce a new kind of recording equipment



Encryption of data

Obligations of the Member States’ authorities

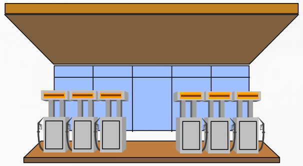
Situation with analogue tachographs



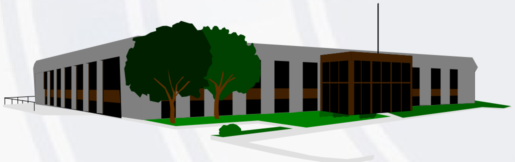
Manufacturers

Type approval

Control bodies



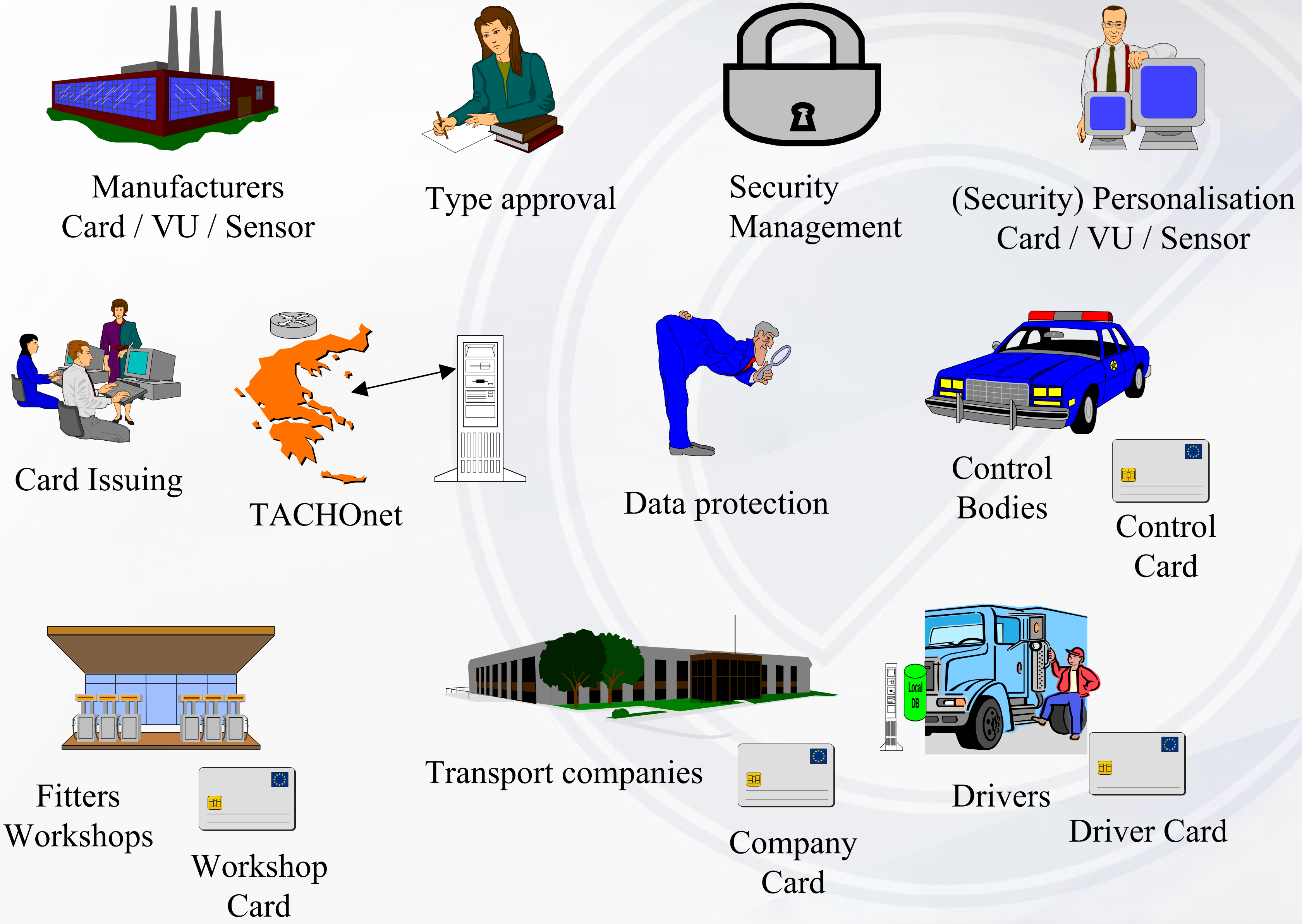
Fitters
Workshops



Transport companies

Drivers

Situation with digital tachographs



Manufacturers
Card / VU / Sensor

Type approval

Security
Management

(Security) Personalisation
Card / VU / Sensor

Card Issuing

TACHOnet

Data protection

Control
Bodies

Control
Card

Fitters
Workshops

Workshop
Card

Transport companies

Company
Card

Drivers

Driver Card

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

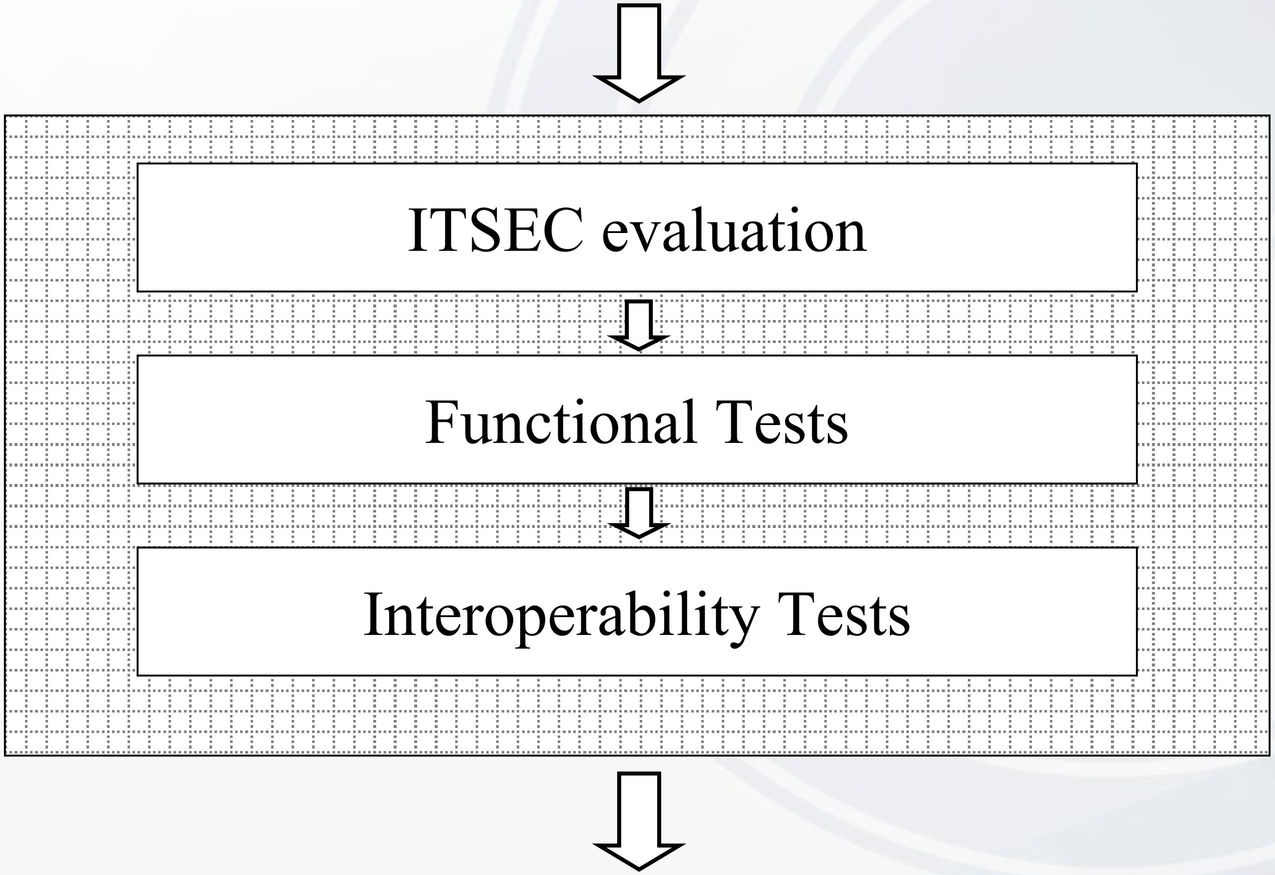
- With analogue tachographs, the situation is different.

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.

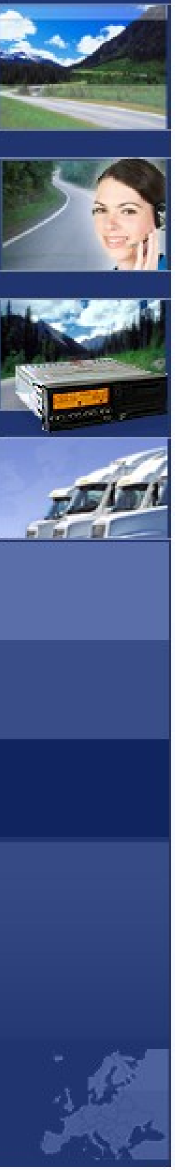
Type Approval Tests



ITSEC evaluation

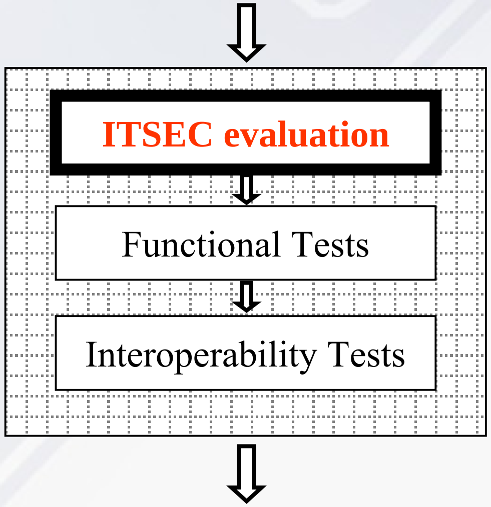
Functional Tests

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**



ITSEC evaluation

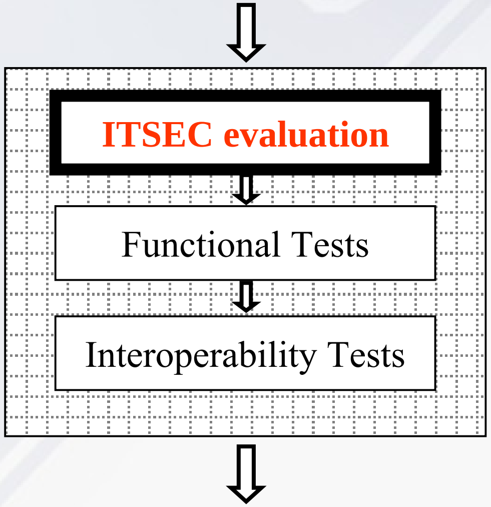
Functional Tests

Interoperability Tests

Card ITSEC evaluation: Result

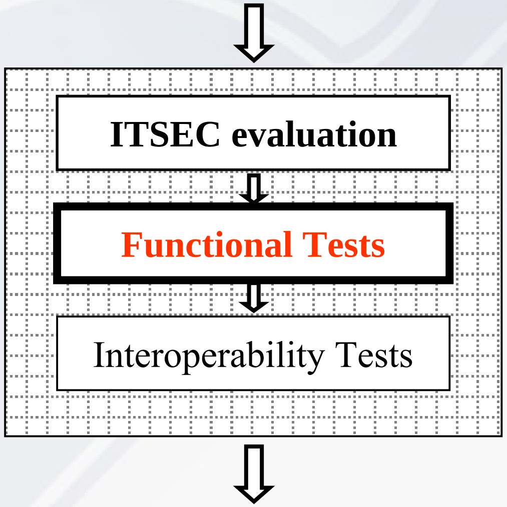
- ITSEC assure that the card manufacturers implement the cards with the specified *target levels*

- The *static characteristics* of the cards and the corresponding manufacturing process are following the requirements



Card Functional Tests: Overview

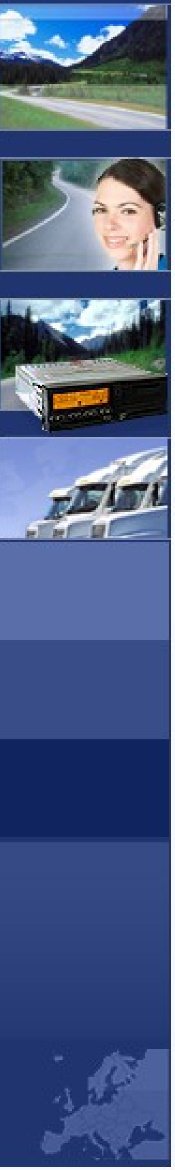
1. Administrative examination
2. Visual inspection
3. Physical tests
4. Protocol tests
5. Card structure
6. Functional tests
7. Environmental Tests



ITSEC evaluation

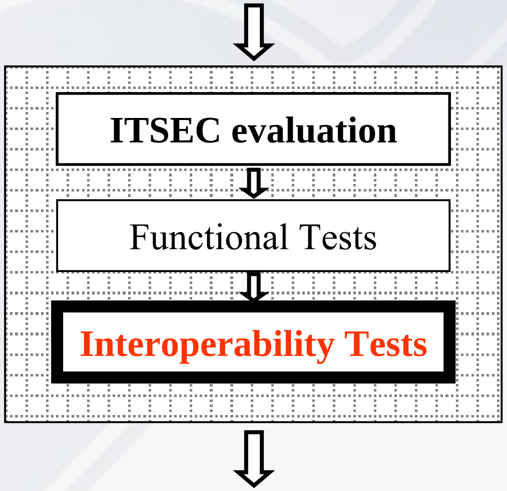
Functional Tests

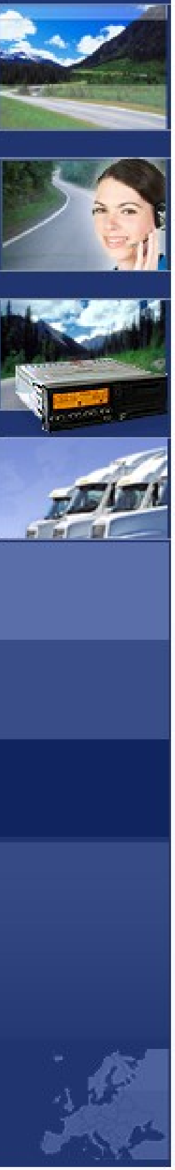
Interoperability Tests



Interoperability Tests

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

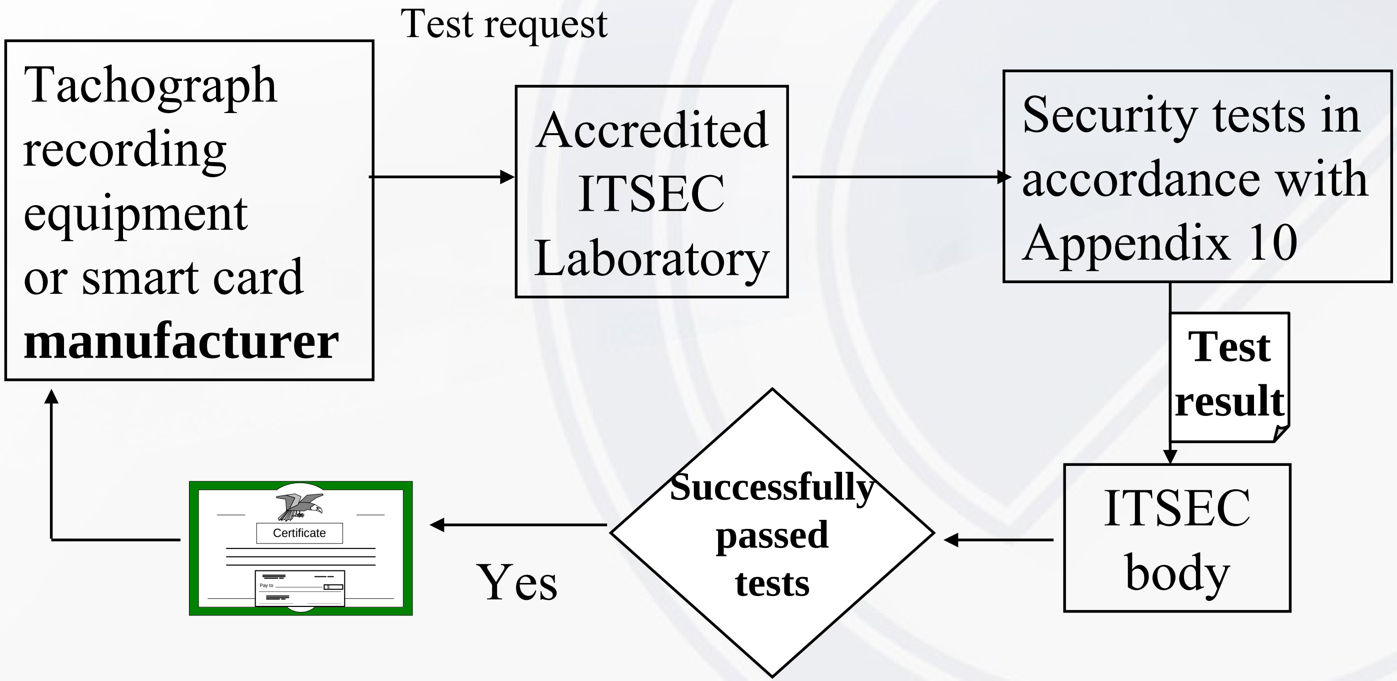




In other words…

TYPE APPROVAL

Security evaluation



Test request

Tachograph recording equipment or smart card **manufacturer**

Accredited ITSEC Laboratory

Security tests in accordance with Appendix 10

Test result

ITSEC body

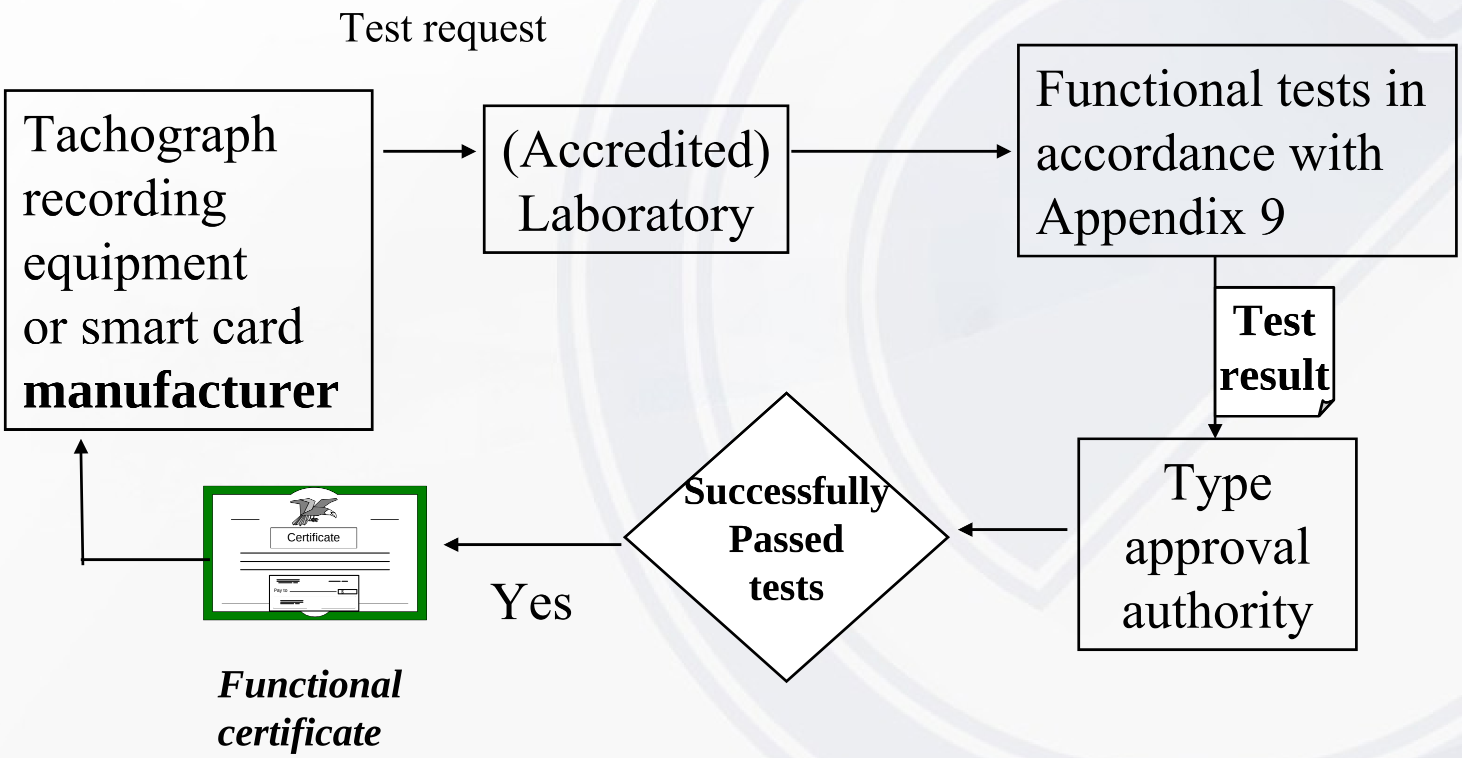
Successfully passed tests

Yes

ITSEC certificate

TYPE APPROVAL

Functional tests



Test request

Tachograph recording equipment or smart card **manufacturer**

(Accredited) Laboratory

Functional tests in accordance with Appendix 9

Test result

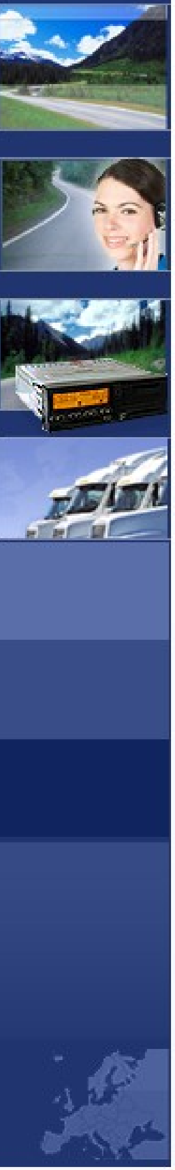
Type approval authority

Successfully Passed tests

Yes

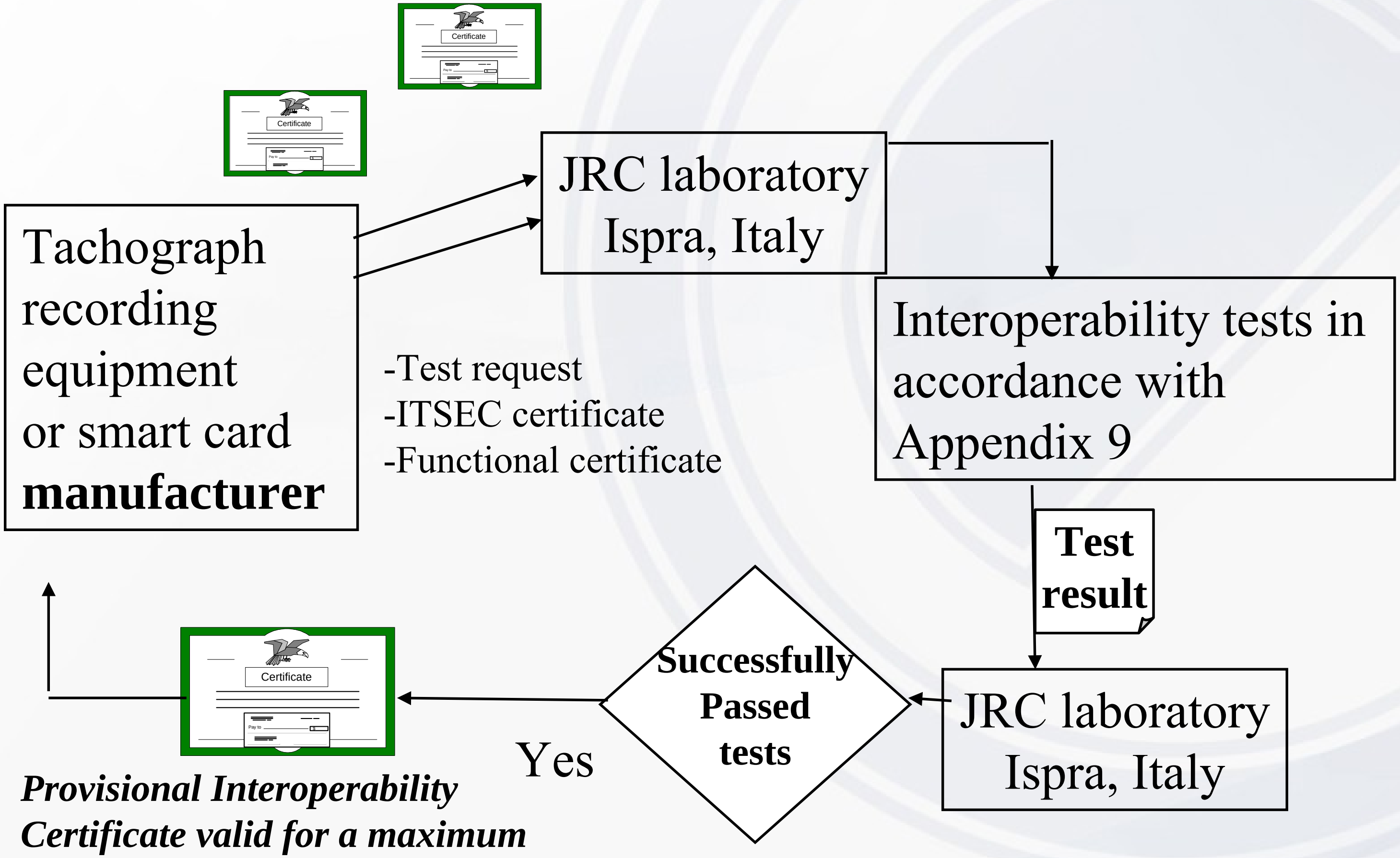
Certificate

Functional certificate



TYPE APPROVAL

Interoperability tests



Tachograph recording equipment or smart card **manufacturer**

-Test request
-ITSEC certificate
-Functional certificate

JRC laboratory
Ispra, Italy

Interoperability tests in accordance with Appendix 9

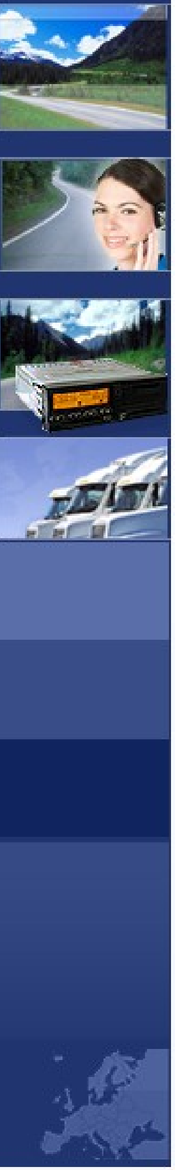
Test result

JRC laboratory
Ispra, Italy

Successfully Passed tests

Yes

Provisional Interoperability Certificate valid for a maximum of 6 months



TYPE APPROVAL

EC Type Approval

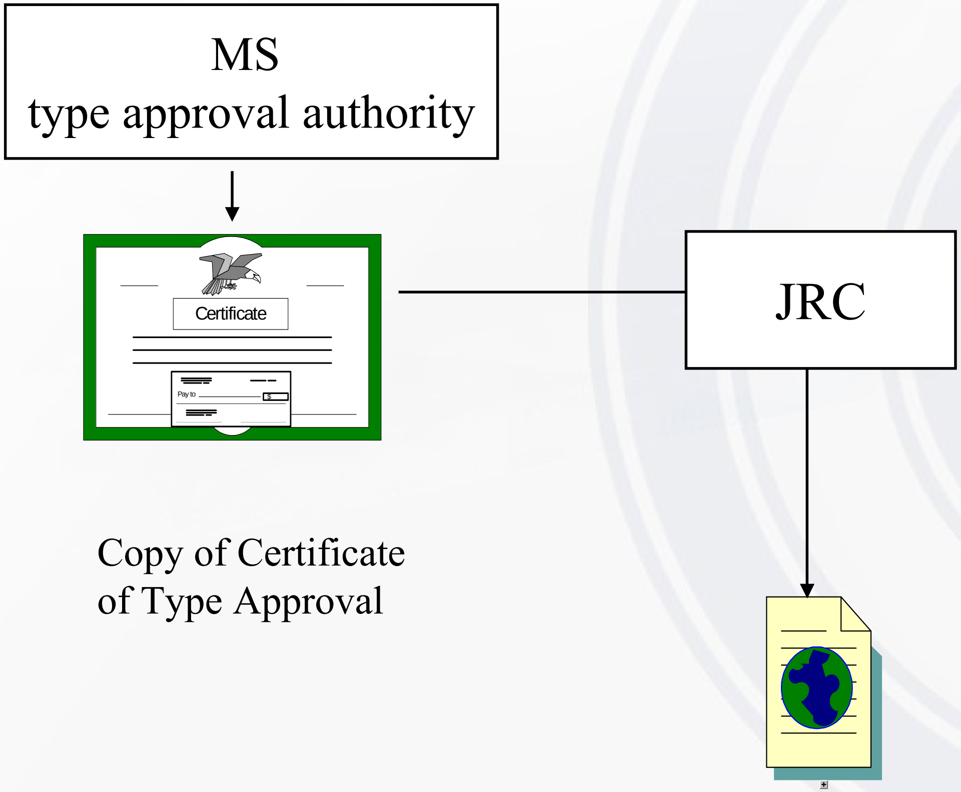
MS type approval authority

- ITSEC certificate
- Functional certificate
- Definitive Interoperability certificate

Certificate of Type Approval

TYPE APPROVAL

Type Approved Tachograph equipment/cards



MS
type approval authority

JRC

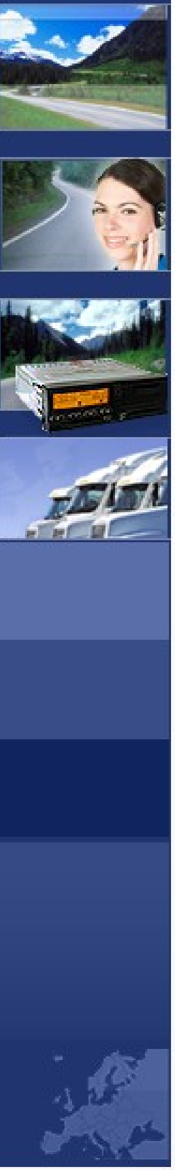
Copy of Certificate
of Type Approval

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

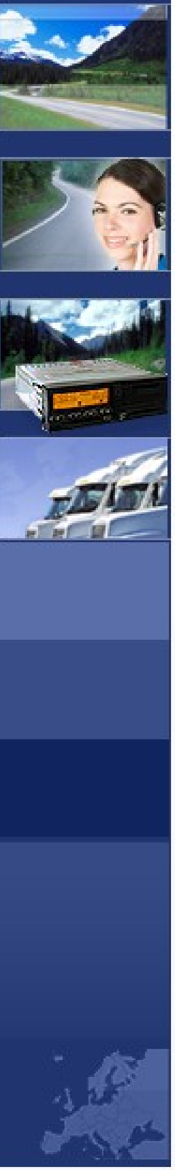
http://dtc.jrc.it/pages/Root%20Certification.htm

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).



Analogue tachographs	Digital tachographs
No type approval required	**Type approval required:** **- either full type approval (functional, security, interoperability and type approval certificates) = develop own cards** **- or simplified procedure = adaptation and type approval of a card already type approved by another Member State**



The list of type approved cards can be found on the following web site:

http://dtc.jrc.it/text/39436108-13.html

Requirement 290 of Appendix 1B of the AETR

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

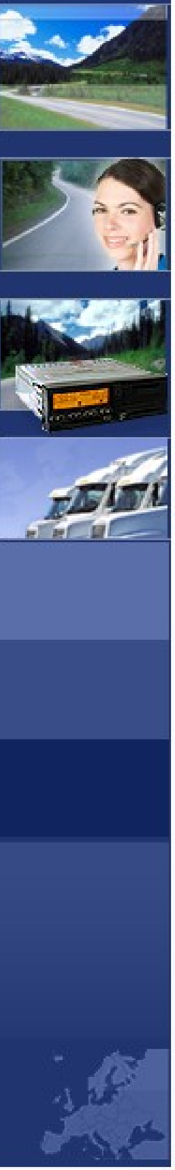
- Kraftfahrt-Bundesamt - Germany
- Ministry of Industry – France
- Swedish Road Administration – Sweden

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/
- CESG (UK): http://www.cesg.gov.uk/
- DCSSI (France): http://www.ssi.gouv.fr/fr/dcssi/index.html



The authority granting interoperability certificates is (only) the following:

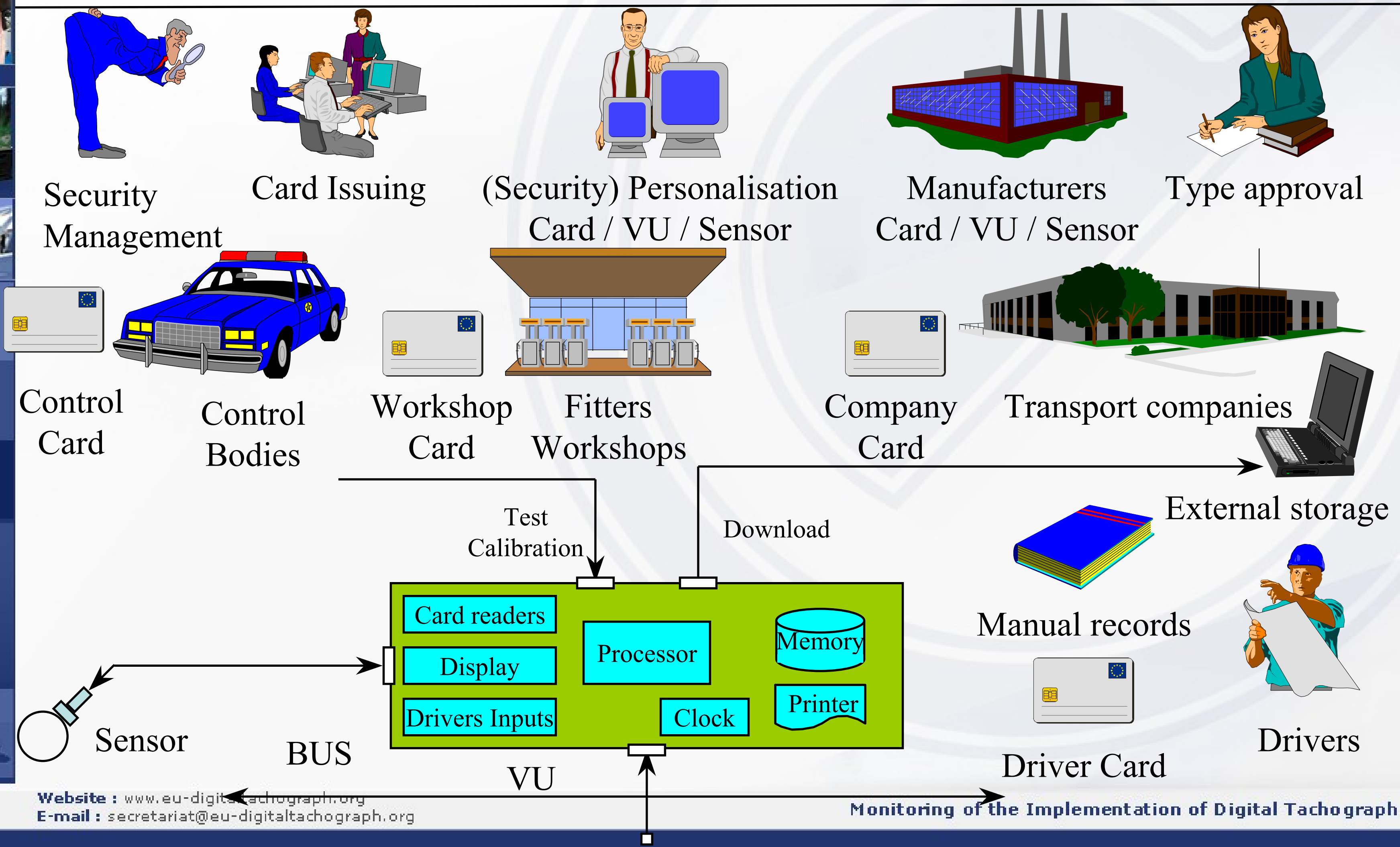
European Commission, DG JRC (Ispra, Italy): http://dtc.jrc.it/text/IOT.html

Requirement 278 of Appendix 1B of the AETR

Questions?

3. Security policy

Global Security Policy
Who / What is involved



Security Management

Card Issuing

(Security) Personalisation
Card / VU / Sensor

Manufacturers
Card / VU / Sensor

Type approval

Control Card

Control Bodies

Workshop Card

Fitters Workshops

Company Card

Transport companies

External storage

Test
Calibration

Download

Card readers

Display

Drivers Inputs

Processor

Memory

Printer

Clock

Manual records

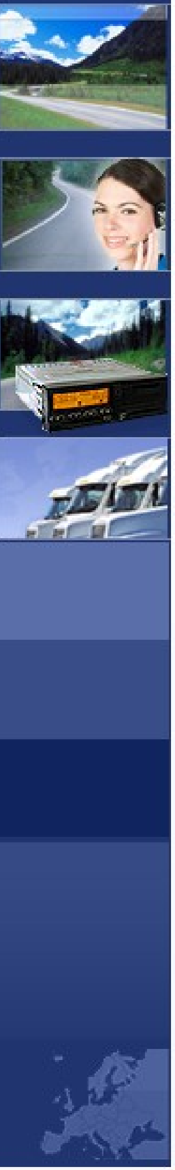
Drivers

Driver Card

Sensor

BUS

VU



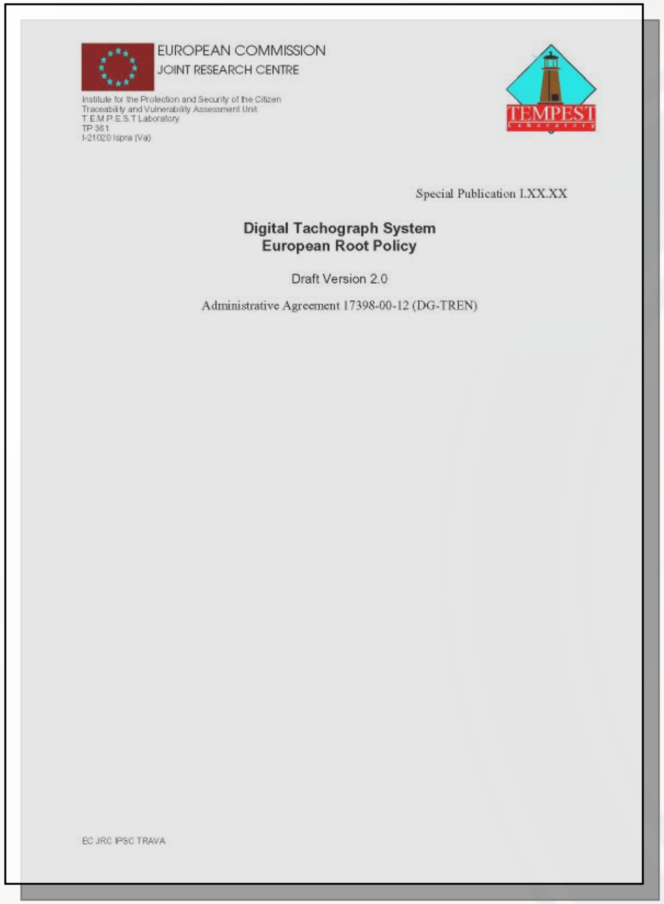
Member States have to ensure the maintenance of the system once deployed in the field.

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.



EUROPEAN COMMISSION
JOINT RESEARCH CENTRE

Institute for the Protection and Security of the Citizen
Traceability and Vulnerability Assessment Unit
T.E.M.P.E.S.T Laboratory
TP 361
I-21020 Ispra (Va)

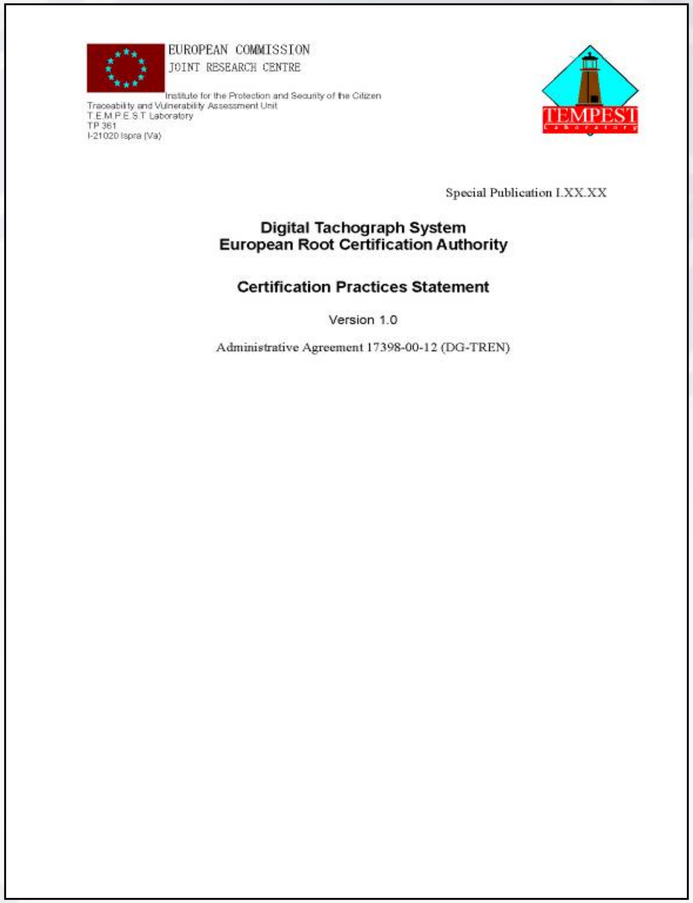
Special Publication I.XX.XX

Digital Tachograph System
European Root Policy

Draft Version 2.0

Administrative Agreement 17398-00-12 (DG-TREN)

EC JRC IPSC TRAVA



EUROPEAN COMMISSION
JOINT RESEARCH CENTRE

Institute for the Protection and Security of the Citizen
Traceability and Vulnerability Assessment Unit
T.E.M.P.E.S.T Laboratory
TP 361
I-21020 Ispra (Va)

Special Publication I.XX.XX

Digital Tachograph System
European Root Certification Authority

Certification Practices Statement

Version 1.0

Administrative Agreement 17398-00-12 (DG-TREN)

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

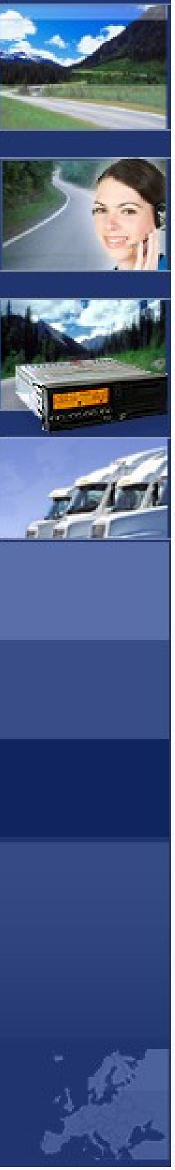
"*the objective of the approval process is to assure comparable levels of security in each Member State*".

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

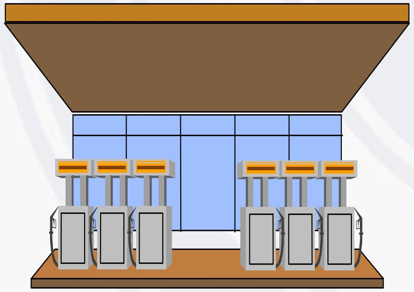
- get it approved by the ERCA

- 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;

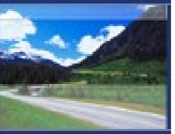
Competent to carry out the work required of them;

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 there 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.

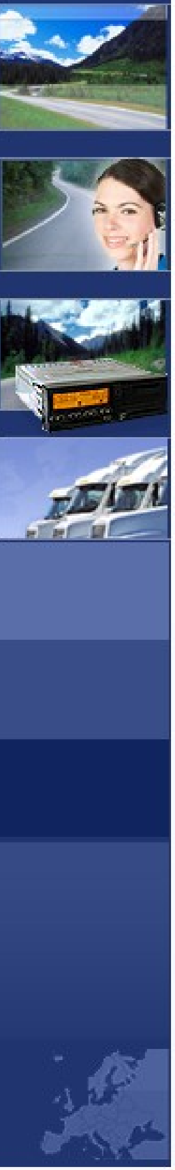
The management of tachograph workshops will need;

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.

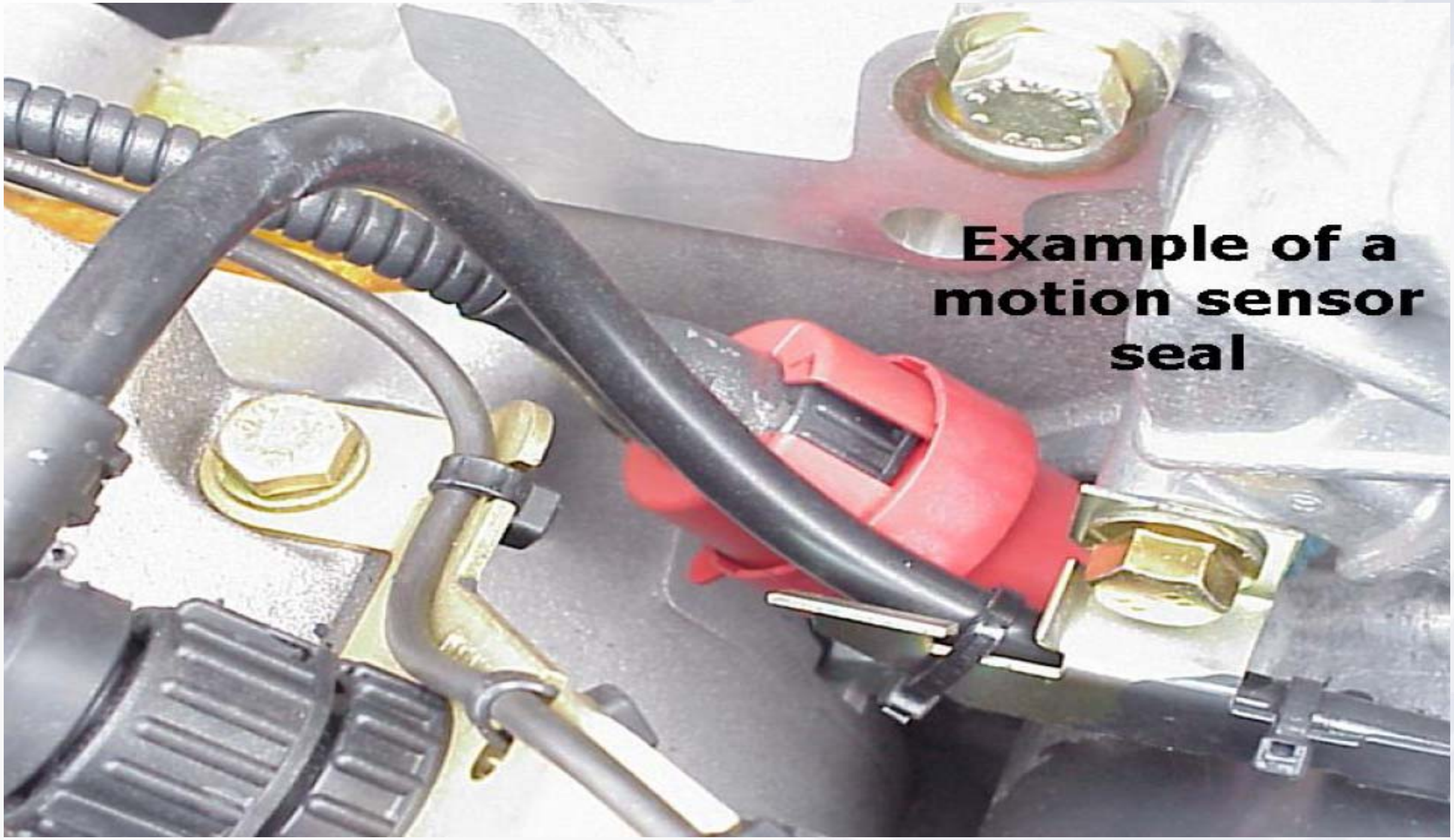
In addition all unused, spoilt, invalid or damaged certificates are retained for audit purposes;



Analogue tachographs	Digital tachographs
Approval of workshops	Approval of workshops
Training of fitters	**(New)** Training of fitters
Equipment	**(New)** Equipment
Honesty	Honesty
Premises	**(New)** Premises
	Security
	Data download
	Workshop card management
Audit	Audit

Today: they check the seals

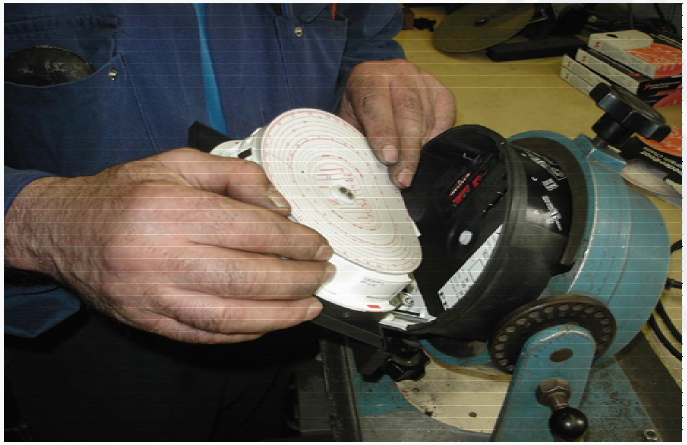
Tomorrow: they check the seals



Today: Data Accuracy

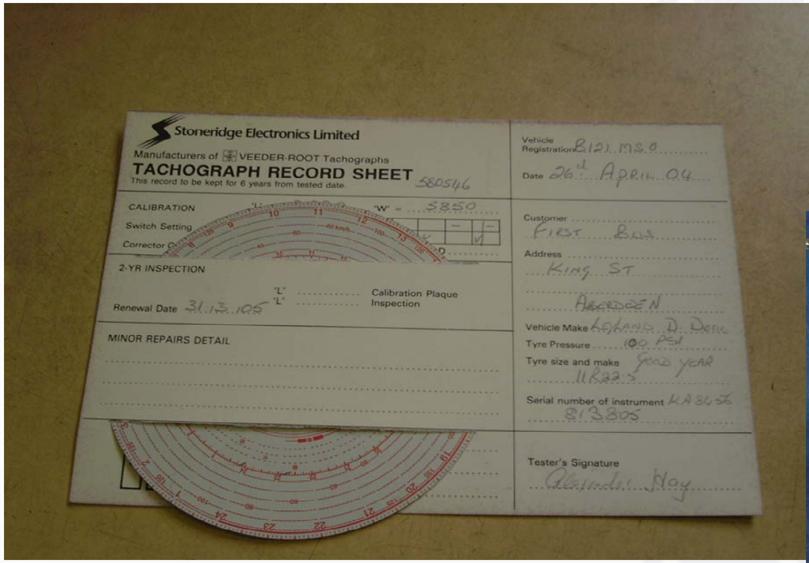
Dates, time, speed, distances, VRN and/or VIN, etc…These data may come from different sources but some of them, at some stages, will need to be calibrated. For example:

- when the recording equipment is installed
- when it is repaired
- when it is regularly checked



Tomorrow: programming

Keep The Records



Stoneridge Electronics Limited
Manufacturers of VEEDER-ROOT Tachographs

TACHOGRAPH RECORD SHEET 580546
This record to be kept for 6 years from tested date.

CALIBRATION 'L' 'W' = 5850
Switch Setting
Corrector G

2-YR INSPECTION
'L' .... Calibration Plaque
Renewal Date 31.13.105 'L' .... Inspection

MINOR REPAIRS DETAIL

Vehicle Registration B121 MSO
Date 26th April 04

Customer
First Bus

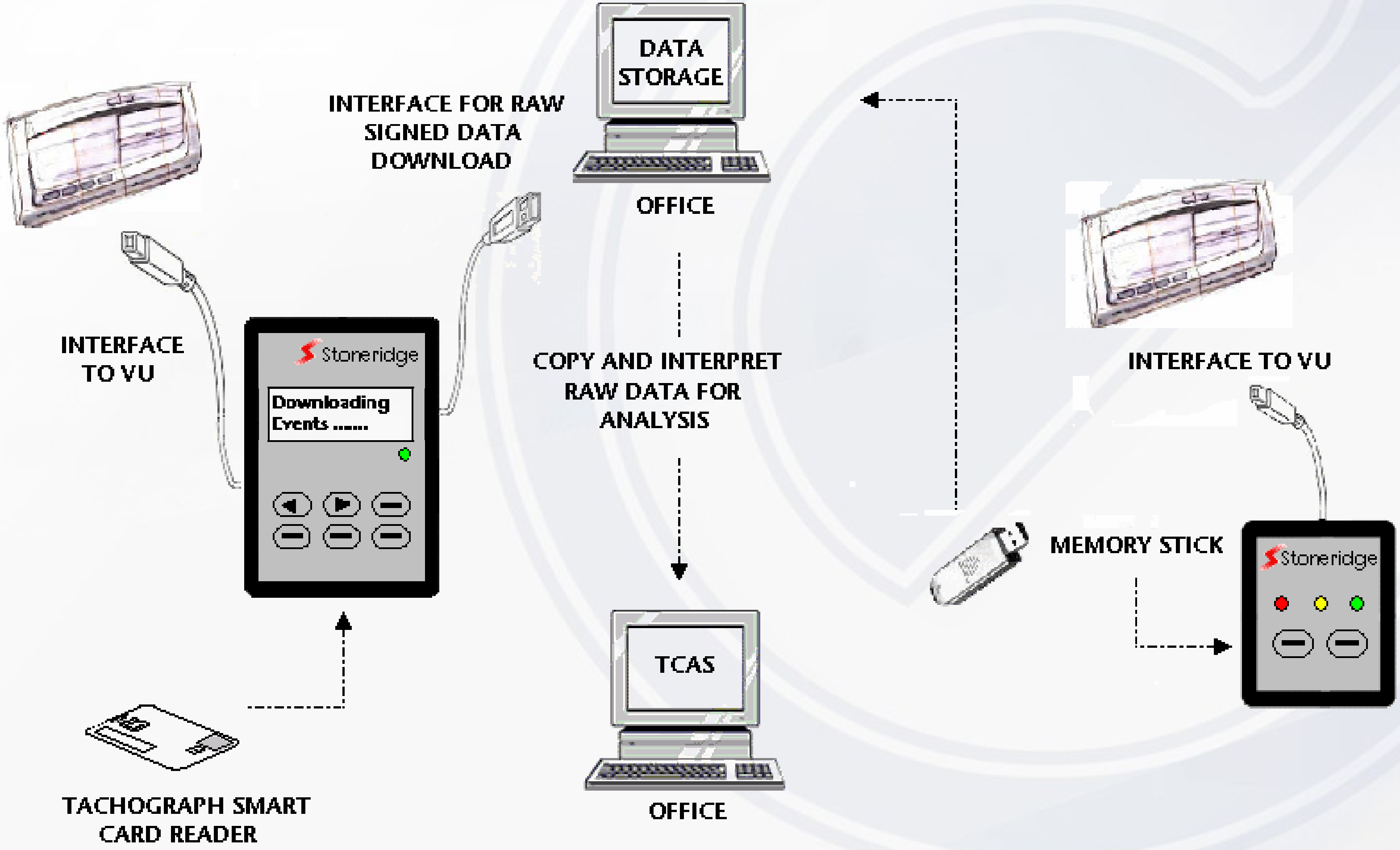
Address
King St
Aberdeen

Vehicle Make Leyland D. Dem
Tyre Pressure 100 PSI
Tyre size and make Good year
11R22.5

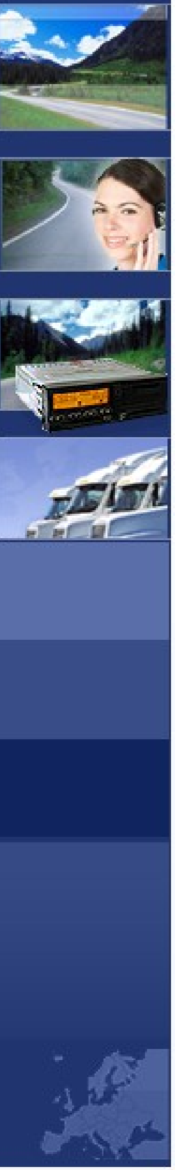
Serial number of instrument KA8456
813805

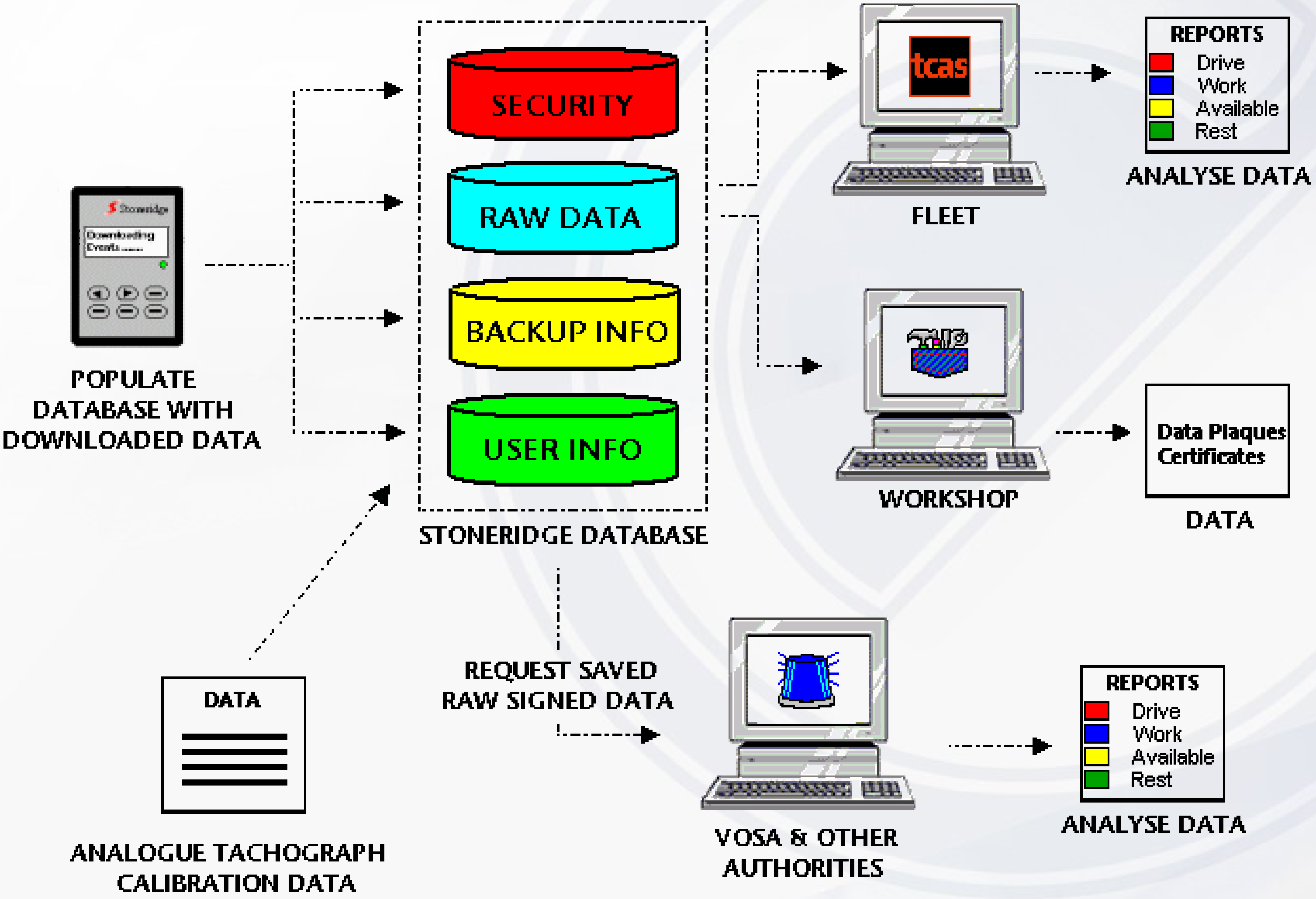
Tester's Signature
Alexander Hay

Keep the data

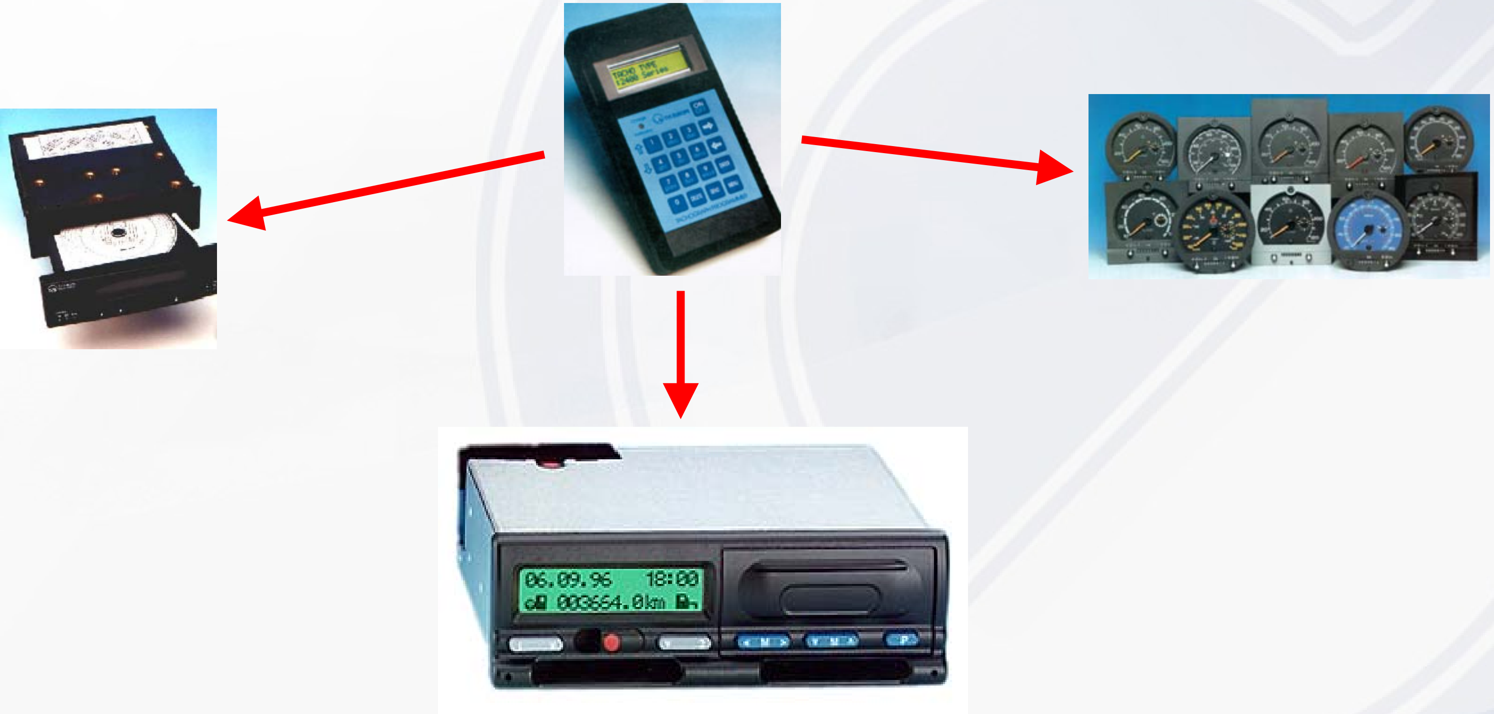

INTERFACE FOR RAW SIGNED DATA DOWNLOAD
DATA STORAGE
OFFICE
INTERFACE TO VU
Storeridge
Downloading Events ......
COPY AND INTERPRET RAW DATA FOR ANALYSIS
INTERFACE TO VU
MEMORY STICK
Storeridge
TCAS
OFFICE
TACHOGRAPH SMART CARD READER

Legal Database





Coexistence of two systems for workshops



National authorities need therefore to:

- issue or amend their national laws on the approval of workshops

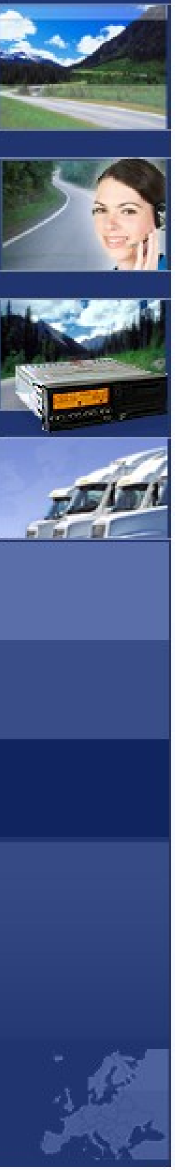
- ensure the proper training of fitters

- ensure to set up a sufficient network of approved workshops at their respective national level

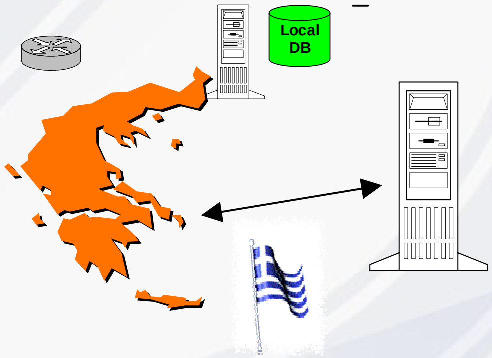
Timing: from 6 up to 16 months

Work to be done in close cooperation with tachograph manufacturers

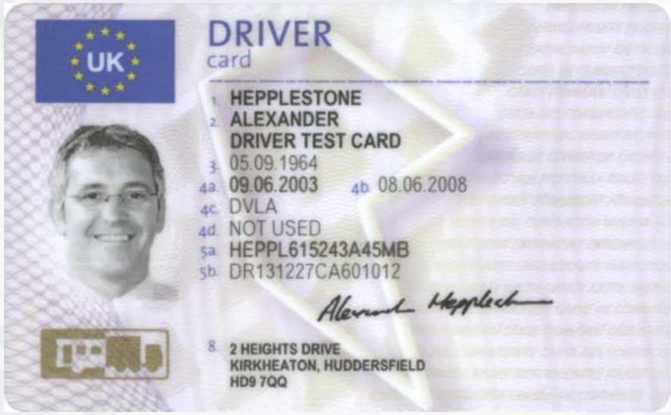
Questions?



5. Card Issuing
TACHOnet



CARD ISSUING



DRIVER
card

UK

1. HEPPLESTONE
2. ALEXANDER
DRIVER TEST CARD
3. 05.09.1964
4a. 09.06.2003 4b. 08.06.2008
4c. DVLA
4d. NOT USED
5a. HEPPL615243A45MB
5b. DR131227CA601012

8. 2 HEIGHTS DRIVE
KIRKHEATON, HUDDERSFIELD
HD9 7QQ

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

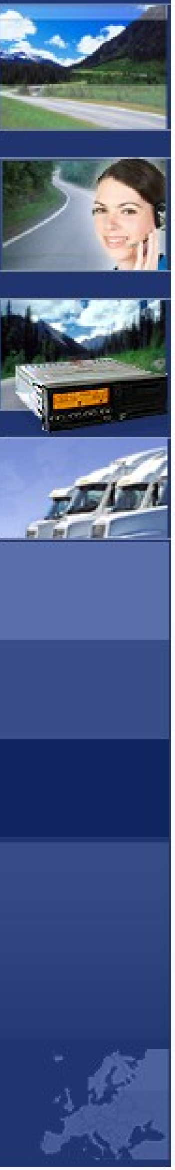
Exchange - Change of administrative data

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

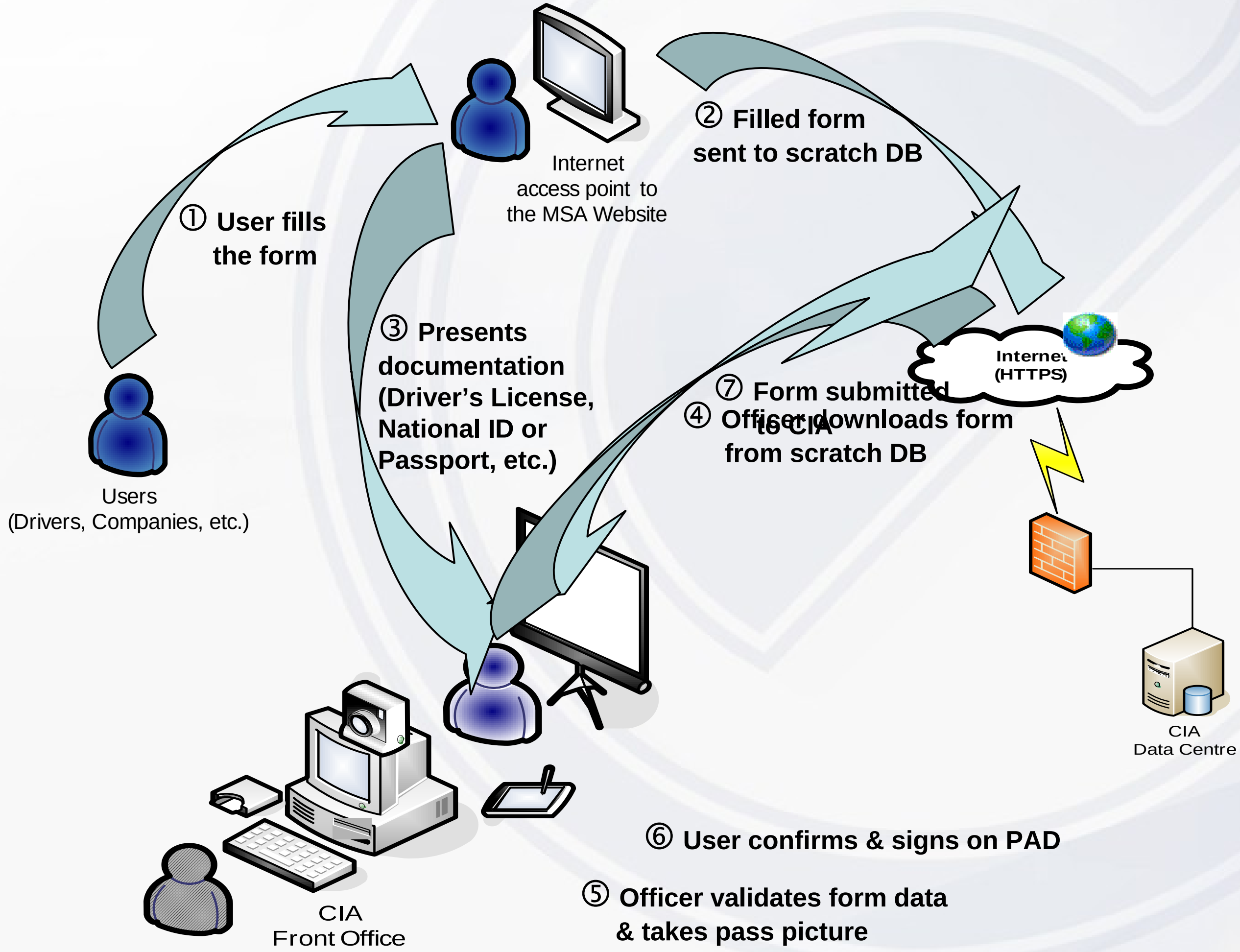
Application processing system

Database to hold & maintain records

Contract with smart card supplier/personaliser

Certification Authority

CIA Front Office
Operational concept



Internet
access point to
the MSA Website

Users
(Drivers, Companies, etc.)

Interne
(HTTPS)

CIA
Data Centre

CIA
Front Office

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

⑦ Form submitted
to CIA

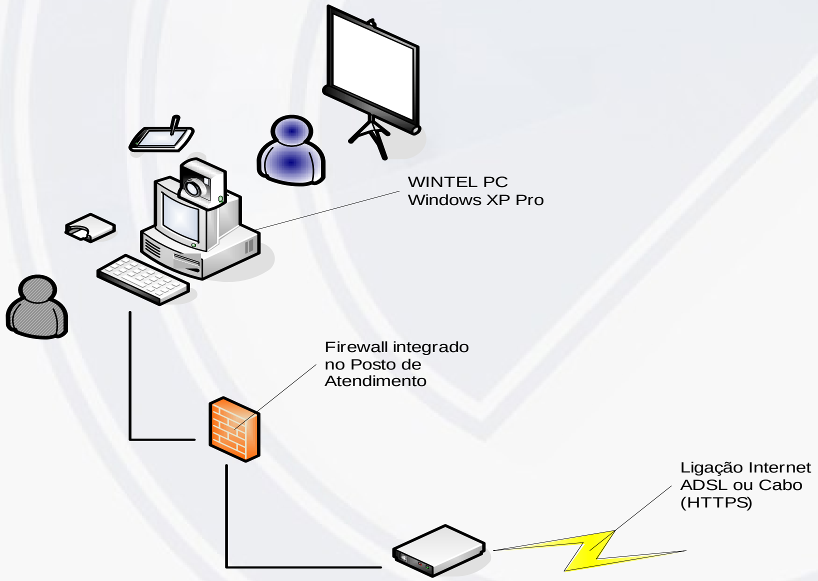
⑥ User confirms & signs on PAD

⑤ Officer validates form data
& takes pass picture

CIA Front Office Architecture

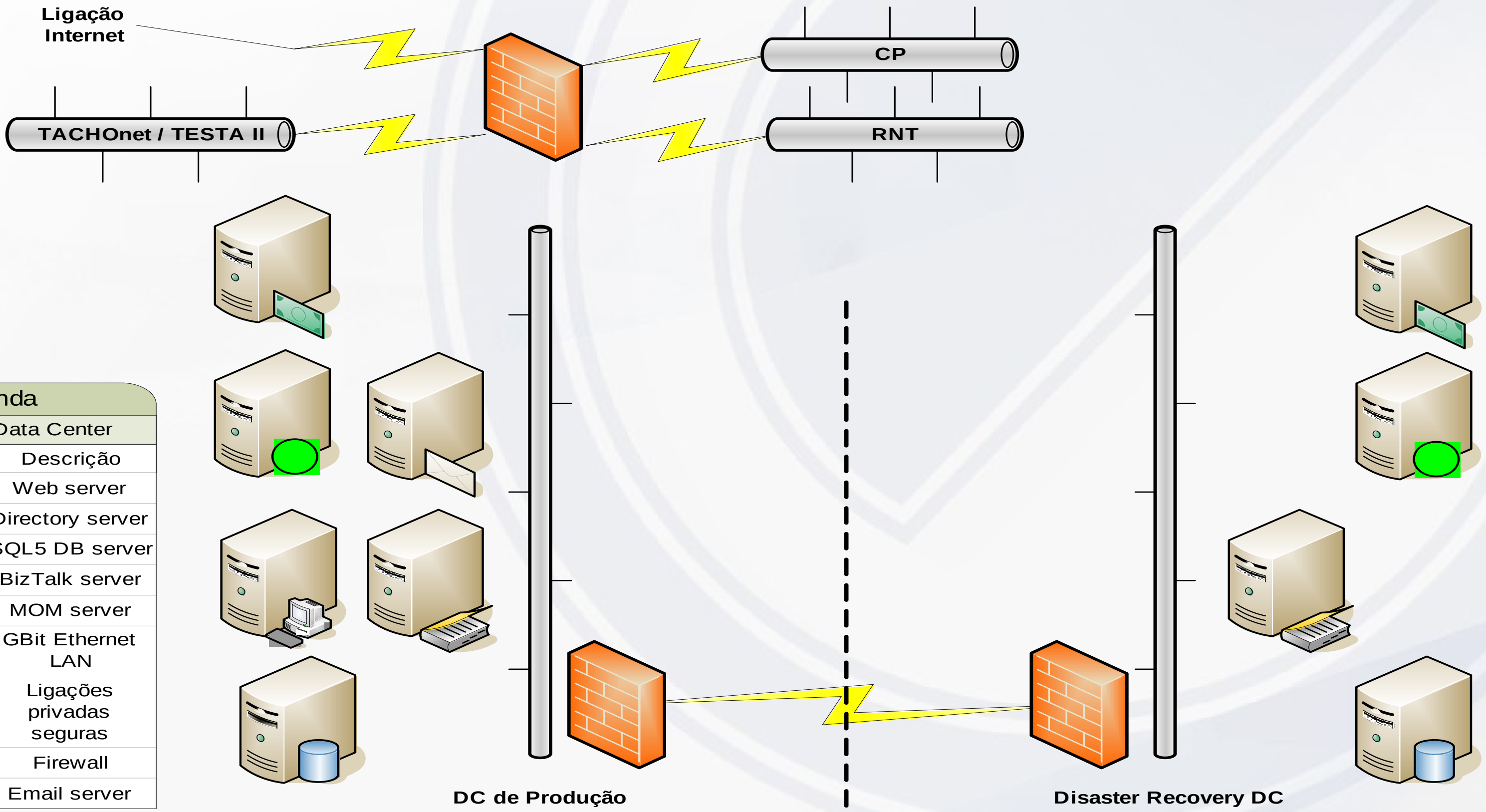
SPTD – CIA
Posto de Atendimento

Legenda		
CIA – Posto de Atendimento		
Símbolo	Qtd	Descrição
▱	1	Modem ADSL/ Cabo
🖥	1	WINTEL PC
📷	1	“Webcam” para recolha de fotografia
👤	2	Agente SPTD e Requerente
▭	1	Ecrã ou superfície clara
▱	1	“Smartcard reader” para autenticação do Agente SPTD
🧱	1	Firewall
✎	1	PAD digital p/ recolha de assinatura
⚡	1	Ligação Internet segura



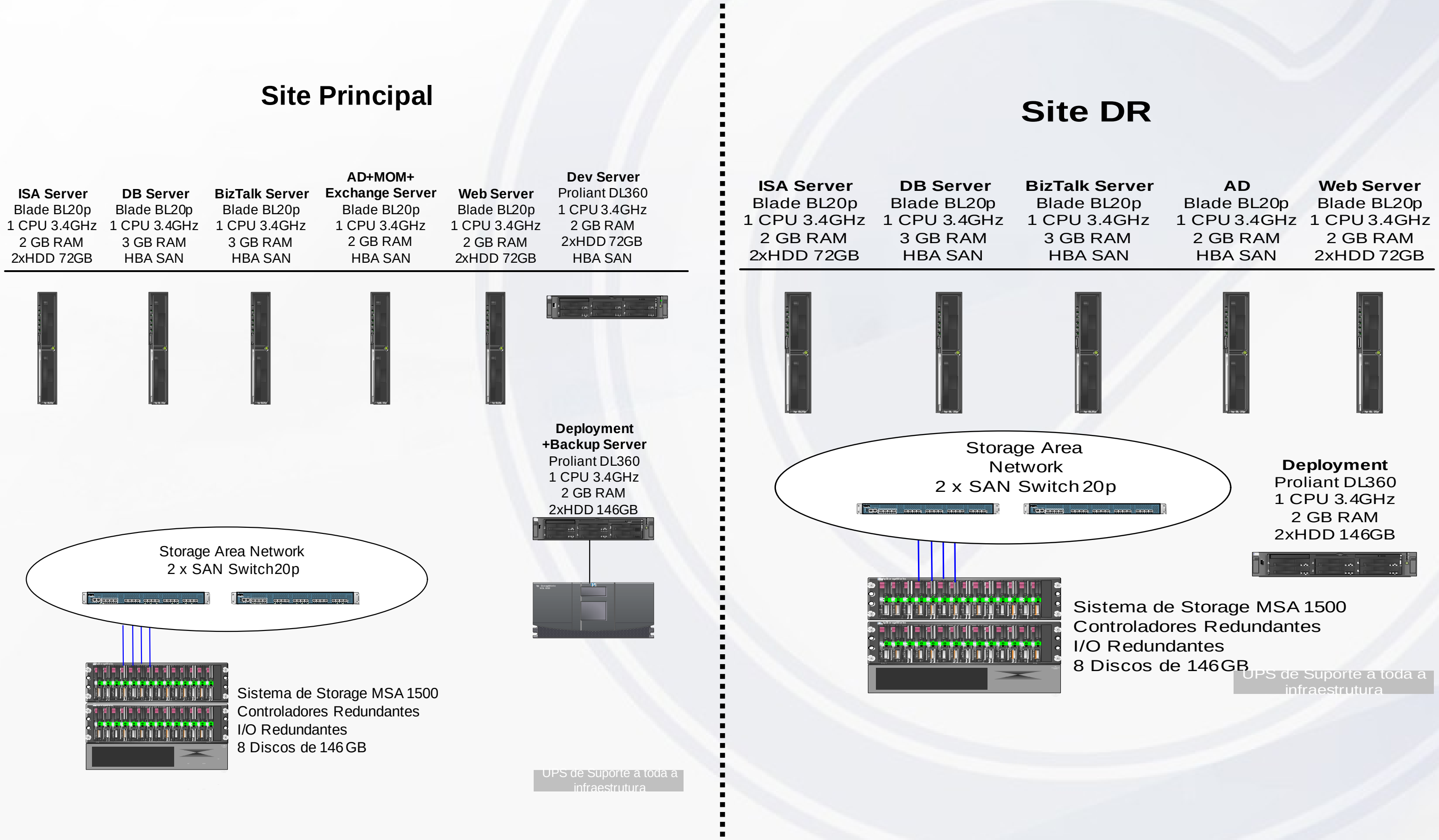
CIA Data Centre Functional Architecture

SPTD – CIA
Data Center



Legenda		
SPTD – CIA Data Center		
Símbolo	Qtd	Descrição
🖥	2	Web server
🖥	2	Directory server
🖥	2	SQL5 DB server
🖥	2	BizTalk server
🖥	1	MOM server
╪	5	GBit Ethernet LAN
⚡	5	Ligações privadas seguras
▨	3	Firewall
🖥	1	Email server

CIA Data Centre
Systems Architecture



Site Principal

ISA Server
Blade BL20p
1 CPU 3.4GHz
2 GB RAM
2xHDD 72GB

DB Server
Blade BL20p
1 CPU 3.4GHz
3 GB RAM
HBA SAN

BizTalk Server
Blade BL20p
1 CPU 3.4GHz
3 GB RAM
HBA SAN

AD+MOM+
Exchange Server
Blade BL20p
1 CPU 3.4GHz
2 GB RAM
HBA SAN

Web Server
Blade BL20p
1 CPU 3.4GHz
2 GB RAM
2xHDD 72GB

Dev Server
Proliant DL360
1 CPU 3.4GHz
2 GB RAM
2xHDD 72GB
HBA SAN

Deployment
+Backup Server
Proliant DL360
1 CPU 3.4GHz
2 GB RAM
2xHDD 146GB

Storage Area Network
2 x SAN Switch20p

Sistema de Storage MSA 1500
Controladores Redundantes
I/O Redundantes
8 Discos de 146 GB

UPS de Suporte a toda a infraestrutura

Site DR

ISA Server
Blade BL20p
1 CPU 3.4GHz
2 GB RAM
2xHDD 72GB

DB Server
Blade BL20p
1 CPU 3.4GHz
3 GB RAM
HBA SAN

BizTalk Server
Blade BL20p
1 CPU 3.4GHz
3 GB RAM
HBA SAN

AD
Blade BL20p
1 CPU 3.4GHz
2 GB RAM
HBA SAN

Web Server
Blade BL20p
1 CPU 3.4GHz
2 GB RAM
2xHDD 72GB

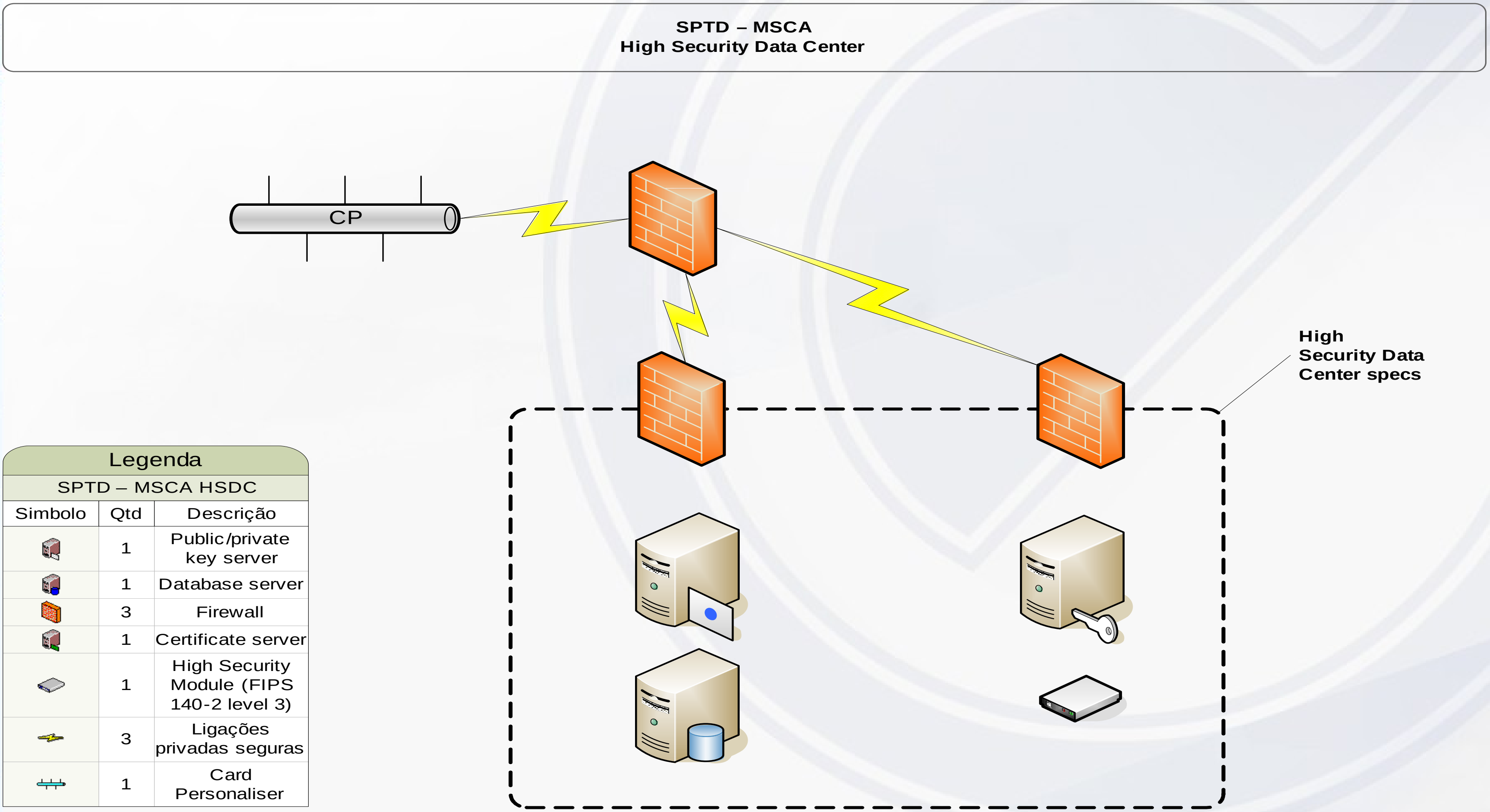
Storage Area
Network
2 x SAN Switch 20p

Deployment
Proliant DL360
1 CPU 3.4GHz
2 GB RAM
2xHDD 146GB

Sistema de Storage MSA 1500
Controladores Redundantes
I/O Redundantes
8 Discos de 146GB

UPS de Suporte a toda a infraestrutura

MSCA Data Centre Functional Architecture



Legenda

SPTD – MSCA HSDC

Simbolo	Qtd	Descrição
🖥	1	Public/private key server
🖥	1	Database server
▨	3	Firewall
🖥	1	Certificate server
▭	1	High Security Module (FIPS 140-2 level 3)
⚡	3	Ligações privadas seguras
╪	1	Card Personaliser

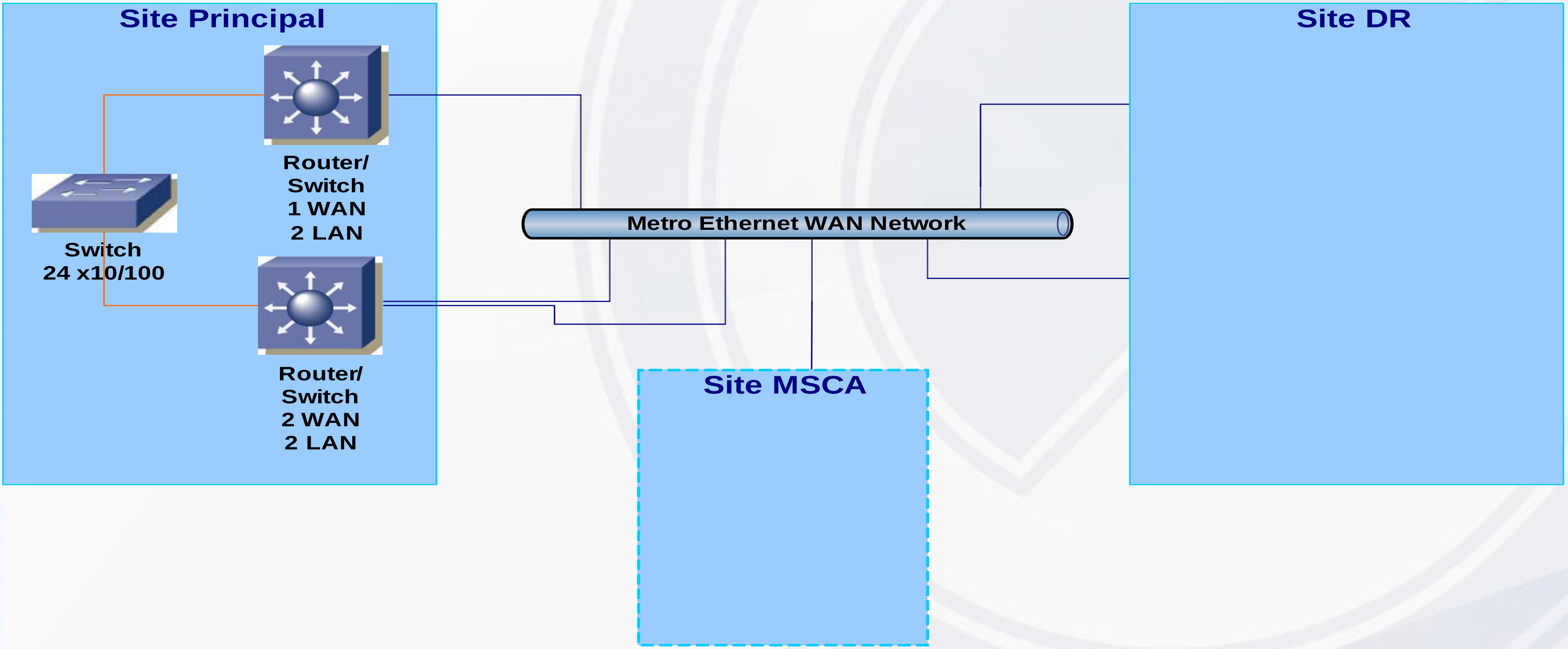
MSCA Data Centre Systems Architecture

2 Servidores de Geração de Chaves/Certificados

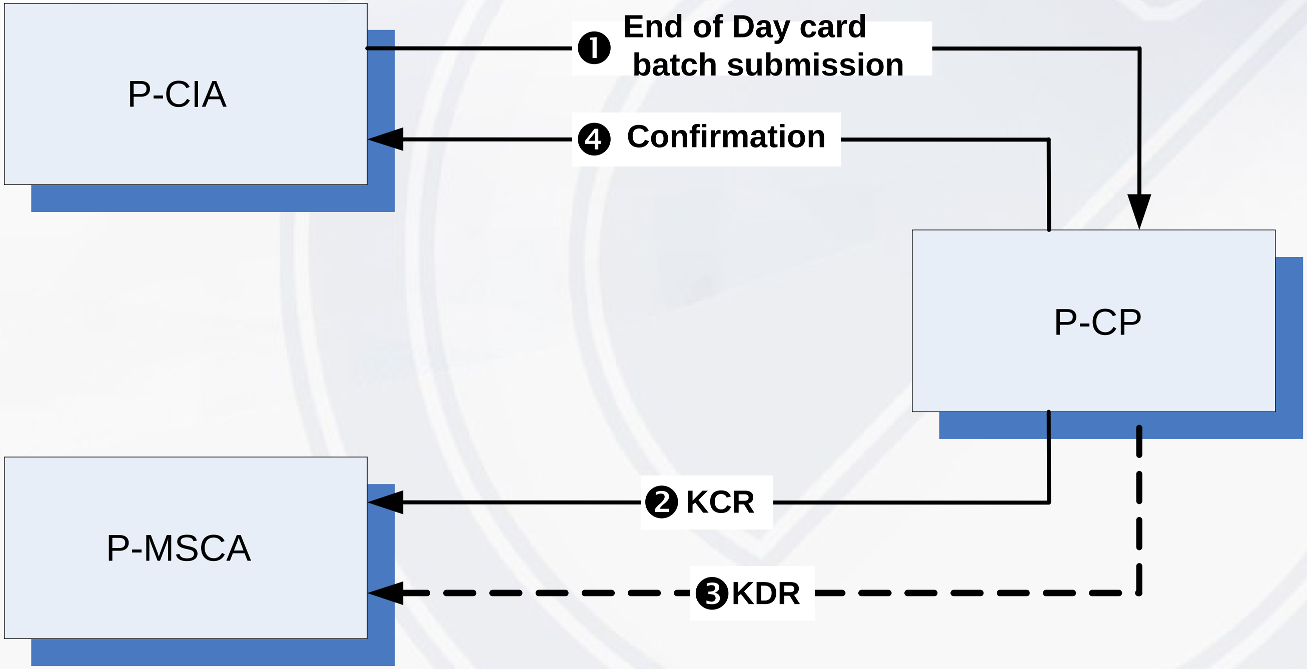
Proliant ML310
1 CPU p640
1 GB RAM
2xHDD 160GB SATA
Bastidor de 14U's em opção

HSM from nCipher
Model "nShield F3 PCI"
FIPS 140-2 level 3 Cert # 527

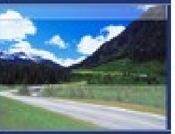
CIA-MSCA
Networking Architecture

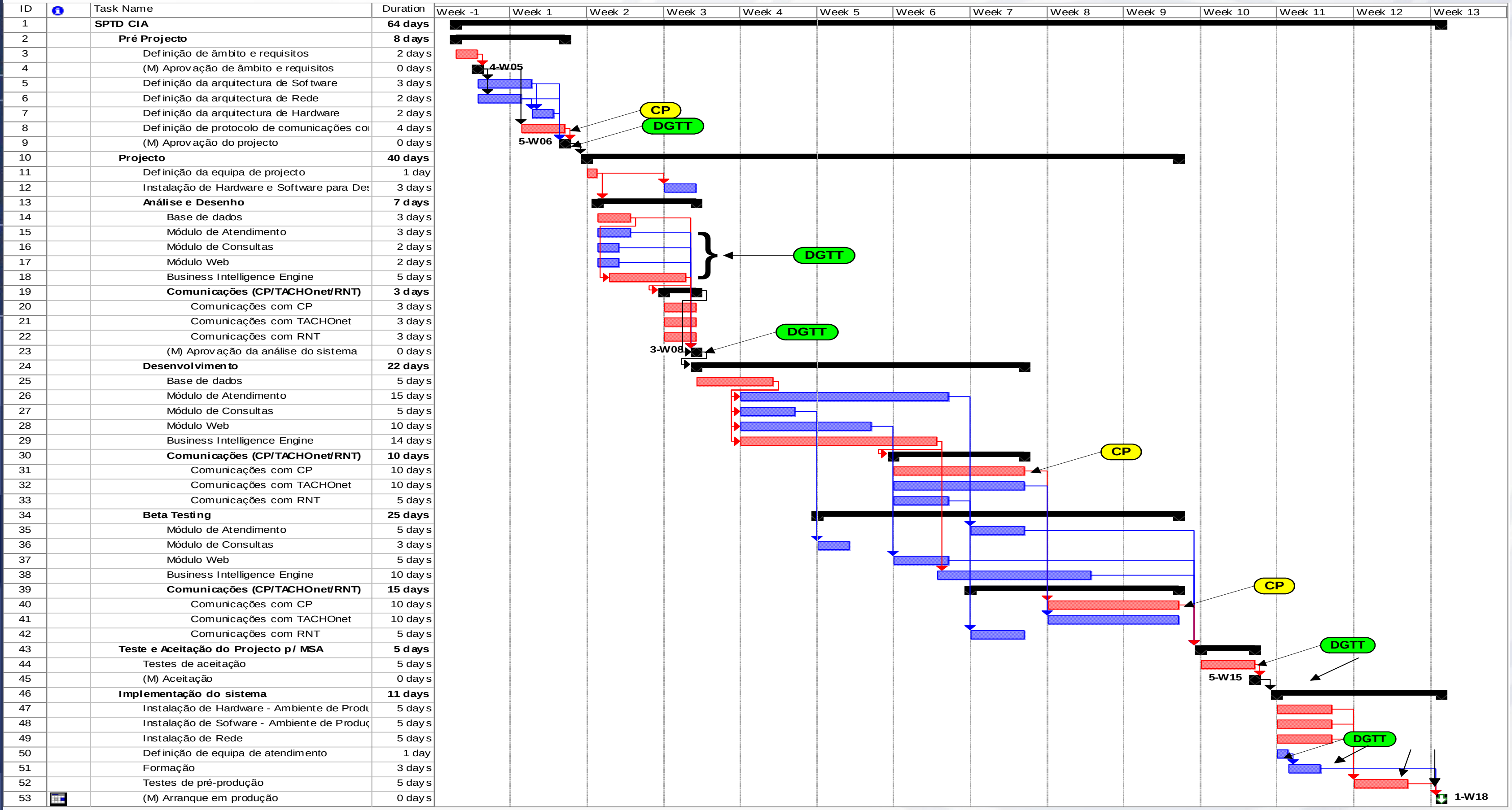


Communication Protocols

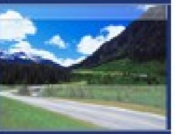


CIA Planning

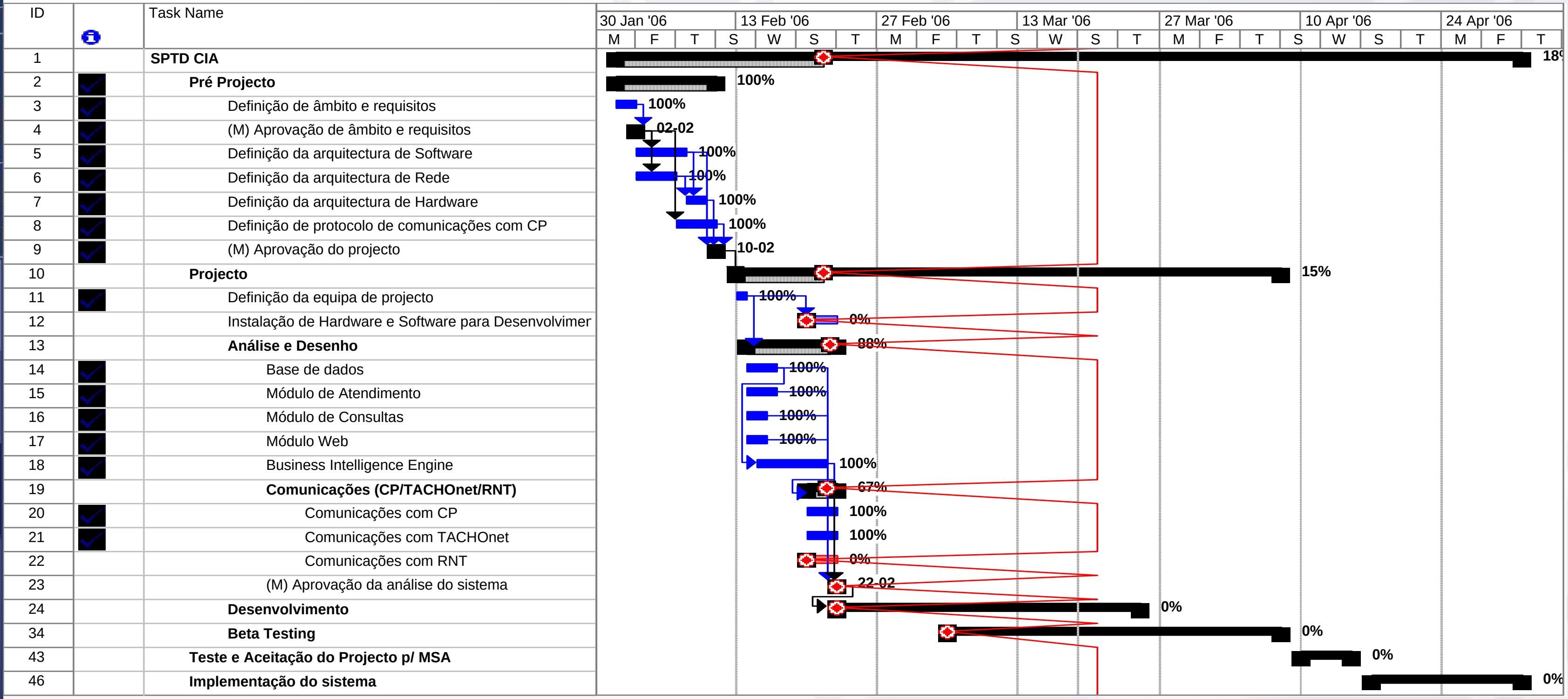




ID	ℹ	Task Name	Duration
1		**SPTD CIA**	**64 days**
2		**Pré Projecto**	**8 days**
3		Definição de âmbito e requisitos	2 days
4		(M) Aprovação de âmbito e requisitos	0 days
5		Definição da arquitectura de Software	3 days
6		Definição da arquitectura de Rede	2 days
7		Definição da arquitectura de Hardware	2 days
8		Definição de protocolo de comunicações coı	4 days
9		(M) Aprovação do projecto	0 days
10		**Projecto**	**40 days**
11		Definição da equipa de projecto	1 day
12		Instalação de Hardware e Software para Des	3 days
13		**Análise e Desenho**	**7 days**
14		Base de dados	3 days
15		Módulo de Atendimento	3 days
16		Módulo de Consultas	2 days
17		Módulo Web	2 days
18		Business Intelligence Engine	5 days
19		**Comunicações (CP/TACHOnet/RNT)**	**3 days**
20		Comunicações com CP	3 days
21		Comunicações com TACHOnet	3 days
22		Comunicações com RNT	3 days
23		(M) Aprovação da análise do sistema	0 days
24		**Desenvolvimento**	**22 days**
25		Base de dados	5 days
26		Módulo de Atendimento	15 days
27		Módulo de Consultas	5 days
28		Módulo Web	10 days
29		Business Intelligence Engine	14 days
30		**Comunicações (CP/TACHOnet/RNT)**	**10 days**
31		Comunicações com CP	10 days
32		Comunicações com TACHOnet	10 days
33		Comunicações com RNT	5 days
34		**Beta Testing**	**25 days**
35		Módulo de Atendimento	5 days
36		Módulo de Consultas	3 days
37		Módulo Web	5 days
38		Business Intelligence Engine	10 days
39		**Comunicações (CP/TACHOnet/RNT)**	**15 days**
40		Comunicações com CP	10 days
41		Comunicações com TACHOnet	10 days
42		Comunicações com RNT	5 days
43		**Teste e Aceitação do Projecto p/ MSA**	**5 days**
44		Testes de aceitação	5 days
45		(M) Aceitação	0 days
46		**Implementação do sistema**	**11 days**
47		Instalação de Hardware - Ambiente de Produ	5 days
48		Instalação de Sofware - Ambiente de Produç	5 days
49		Instalação de Rede	5 days
50		Definição de equipa de atendimento	1 day
51		Formação	3 days
52		Testes de pré-produção	5 days
53	📅	(M) Arranque em produção	0 days

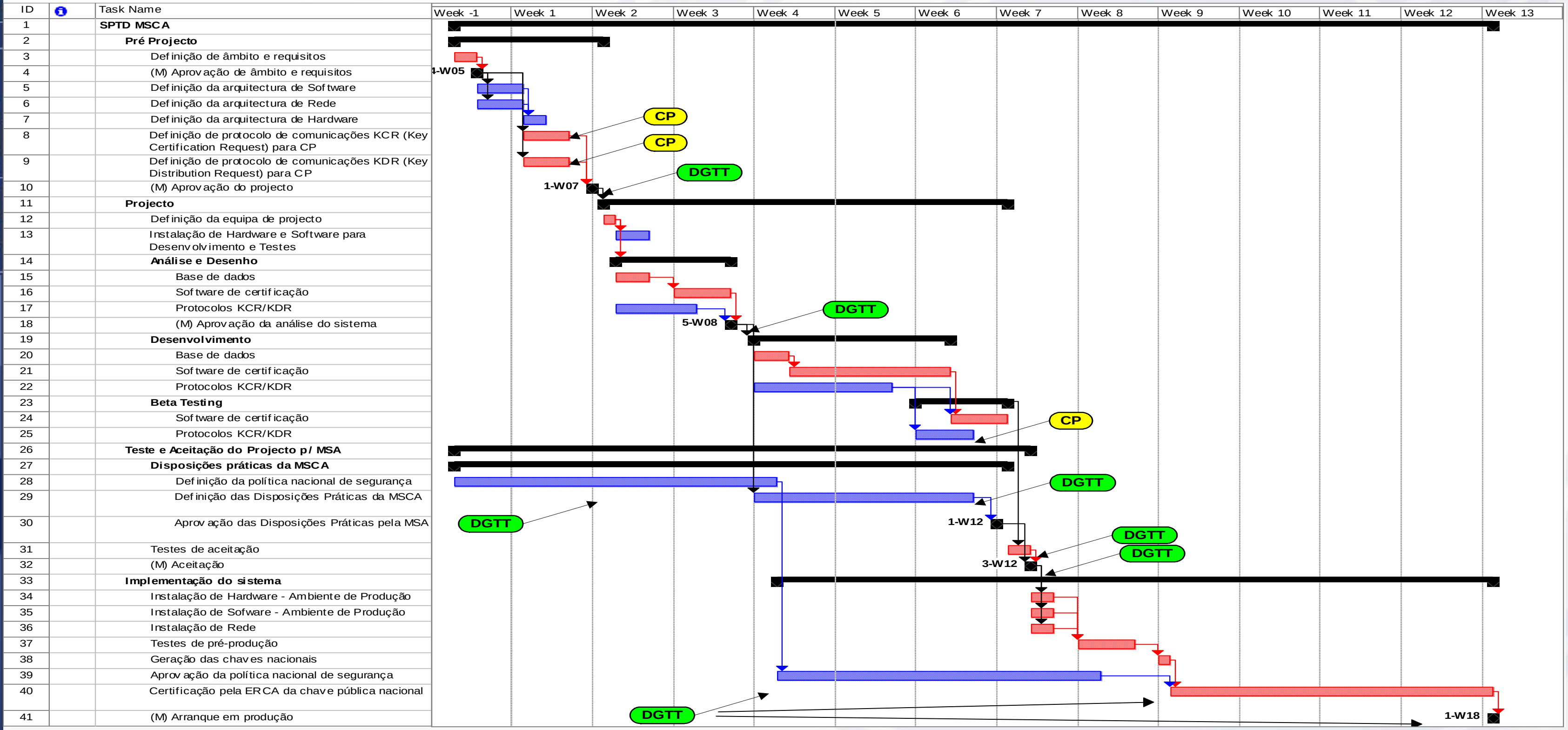


CIA
Tracking Gantt To Date



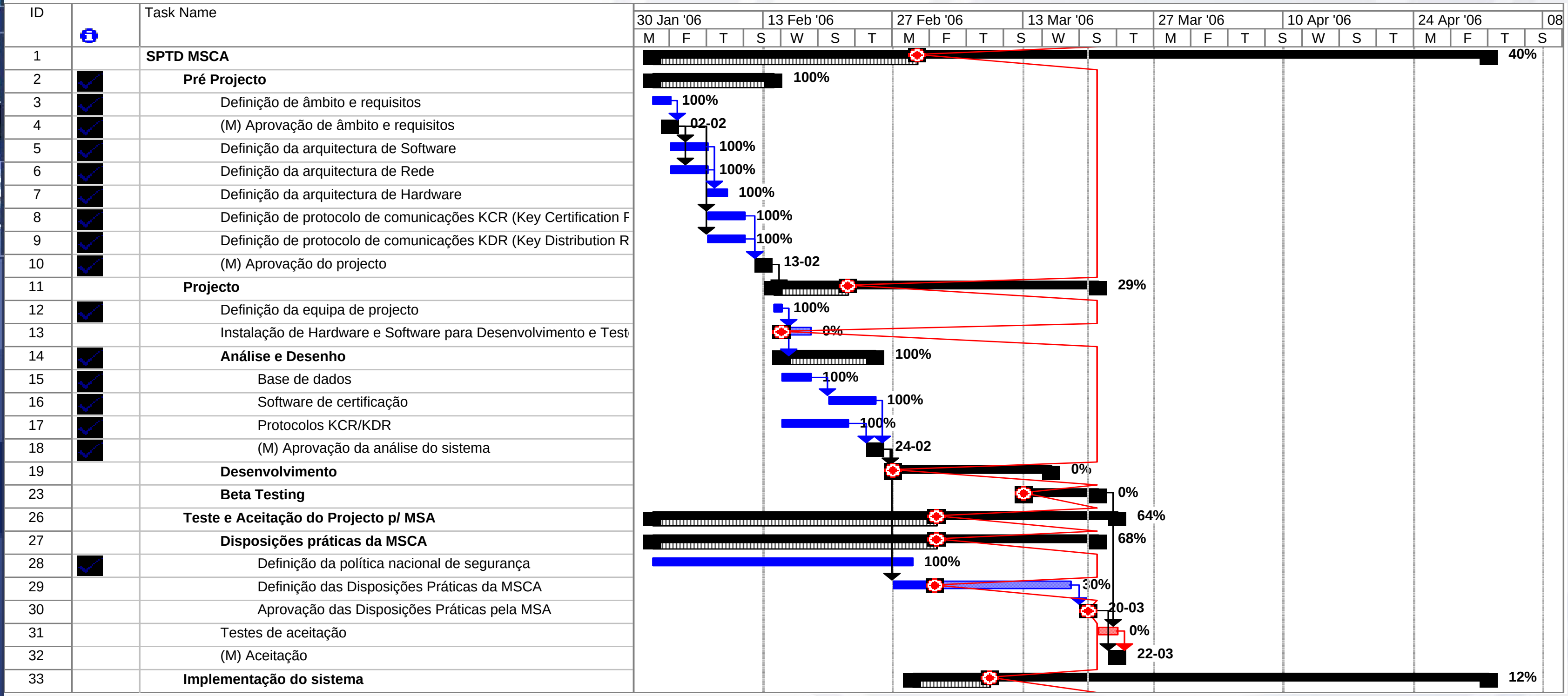
ID	ℹ	Task Name
1		**SPTD CIA**
2	✓	**Pré Projecto**
3	✓	Definição de âmbito e requisitos
4	✓	(M) Aprovação de âmbito e requisitos
5	✓	Definição da arquitectura de Software
6	✓	Definição da arquitectura de Rede
7	✓	Definição da arquitectura de Hardware
8	✓	Definição de protocolo de comunicações com CP
9	✓	(M) Aprovação do projecto
10		**Projecto**
11	✓	Definição da equipa de projecto
12		Instalação de Hardware e Software para Desenvolvimer
13		**Análise e Desenho**
14	✓	Base de dados
15	✓	Módulo de Atendimento
16	✓	Módulo de Consultas
17	✓	Módulo Web
18	✓	Business Intelligence Engine
19		**Comunicações (CP/TACHOnet/RNT)**
20	✓	Comunicações com CP
21	✓	Comunicações com TACHOnet
22		Comunicações com RNT
23		(M) Aprovação da análise do sistema
24		**Desenvolvimento**
34		**Beta Testing**
43		**Teste e Aceitação do Projecto p/ MSA**
46		**Implementação do sistema**

MSCA Planning



ID	ℹ	Task Name
1		**SPTD MSCA**
2		**Pré Projecto**
3		Definição de âmbito e requisitos
4		(M) Aprovação de âmbito e requisitos
5		Definição da arquitectura de Software
6		Definição da arquitectura de Rede
7		Definição da arquitectura de Hardware
8		Definição de protocolo de comunicações KCR (Key Certification Request) para CP
9		Definição de protocolo de comunicações KDR (Key Distribution Request) para CP
10		(M) Aprovação do projecto
11		**Projecto**
12		Definição da equipa de projecto
13		Instalação de Hardware e Software para Desenvolvimento e Testes
14		**Análise e Desenho**
15		Base de dados
16		Software de certificação
17		Protocolos KCR/KDR
18		(M) Aprovação da análise do sistema
19		**Desenvolvimento**
20		Base de dados
21		Software de certificação
22		Protocolos KCR/KDR
23		**Beta Testing**
24		Software de certificação
25		Protocolos KCR/KDR
26		**Teste e Aceitação do Projecto p/ MSA**
27		**Disposições práticas da MSCA**
28		Definição da política nacional de segurança
29		Definição das Disposições Práticas da MSCA
30		Aprovação das Disposições Práticas pela MSA
31		Testes de aceitação
32		(M) Aceitação
33		**Implementação do sistema**
34		Instalação de Hardware - Ambiente de Produção
35		Instalação de Sofware - Ambiente de Produção
36		Instalação de Rede
37		Testes de pré-produção
38		Geração das chaves nacionais
39		Aprovação da política nacional de segurança
40		Certificação pela ERCA da chave pública nacional
41		(M) Arranque em produção

MSCA
Tracking Gantt To Date



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

Questions?

TACHONET

TACHOnet Project Objectives

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

TACHOnet network:

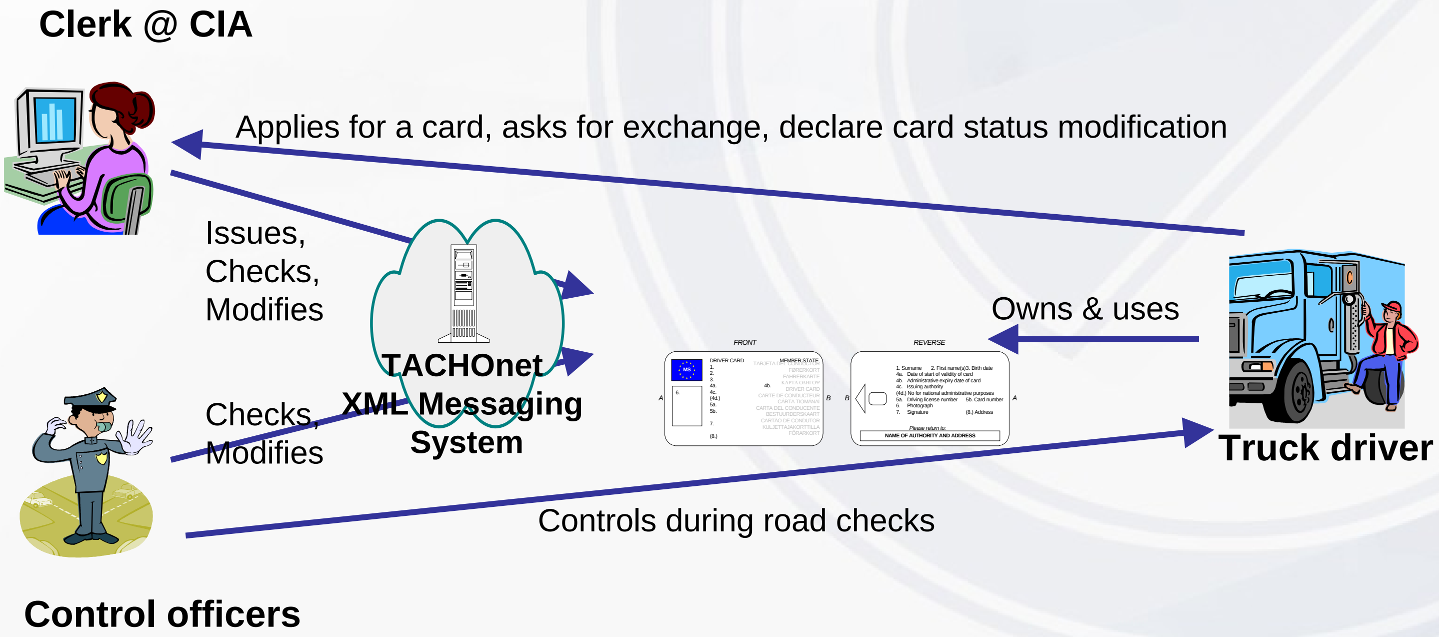
- Ensures a reliable and secure exchange of necessary and sufficient data between States issuing tachograph cards
- Makes sure the exchange is done within the legal constraints stated in the EU-AETR rules
- Imposes only limited constraints on the local systems managing cards in the different States

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

TACHOnet XML Messaging System

Owns & uses

Truck driver

Checks, Modifies

Controls during road checks

Control officers

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

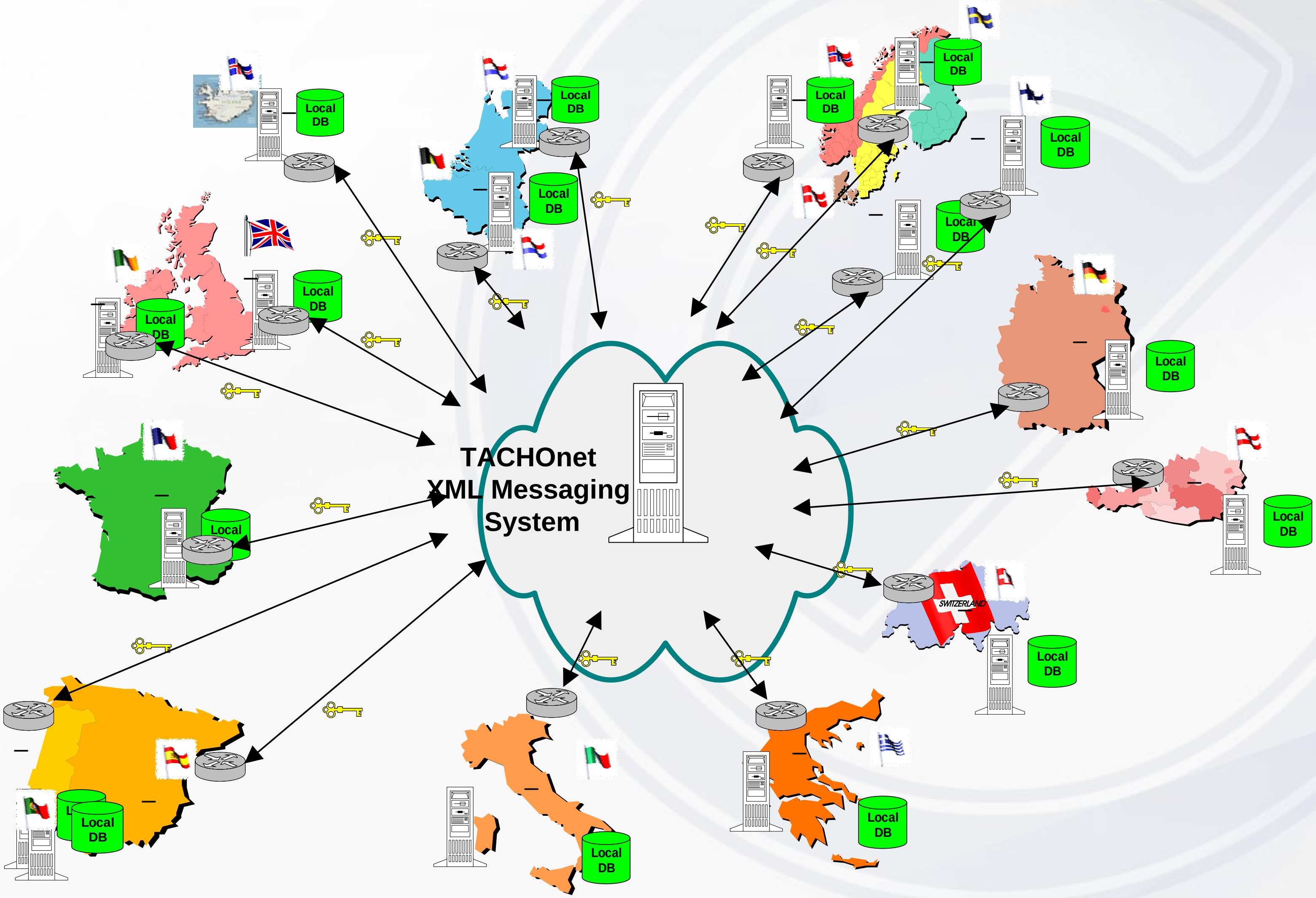
Scope and Exclusions of TACHOnet

Business processes:

2. Not included:

- Check for driver license number by integrating calls to external systems

TACHOnet Architecture



National authorities need therefore to:

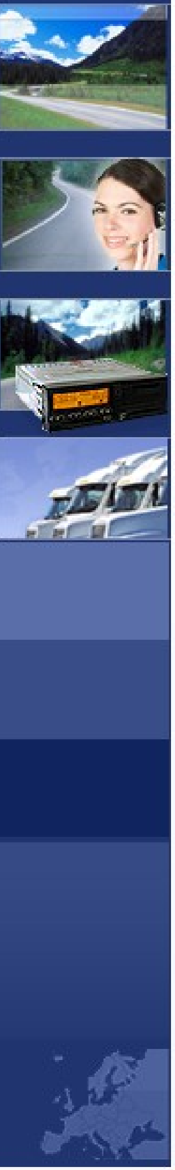
- exchange information making sure that they do not issue a card to an applicant who already holds one

- 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



Analogue tachographs	Digital tachographs
	- Security management **Security policy** **Security audits** **- Issuing of cards** **- Connection to a net or active exchange of information between AETR Contracting Parties**

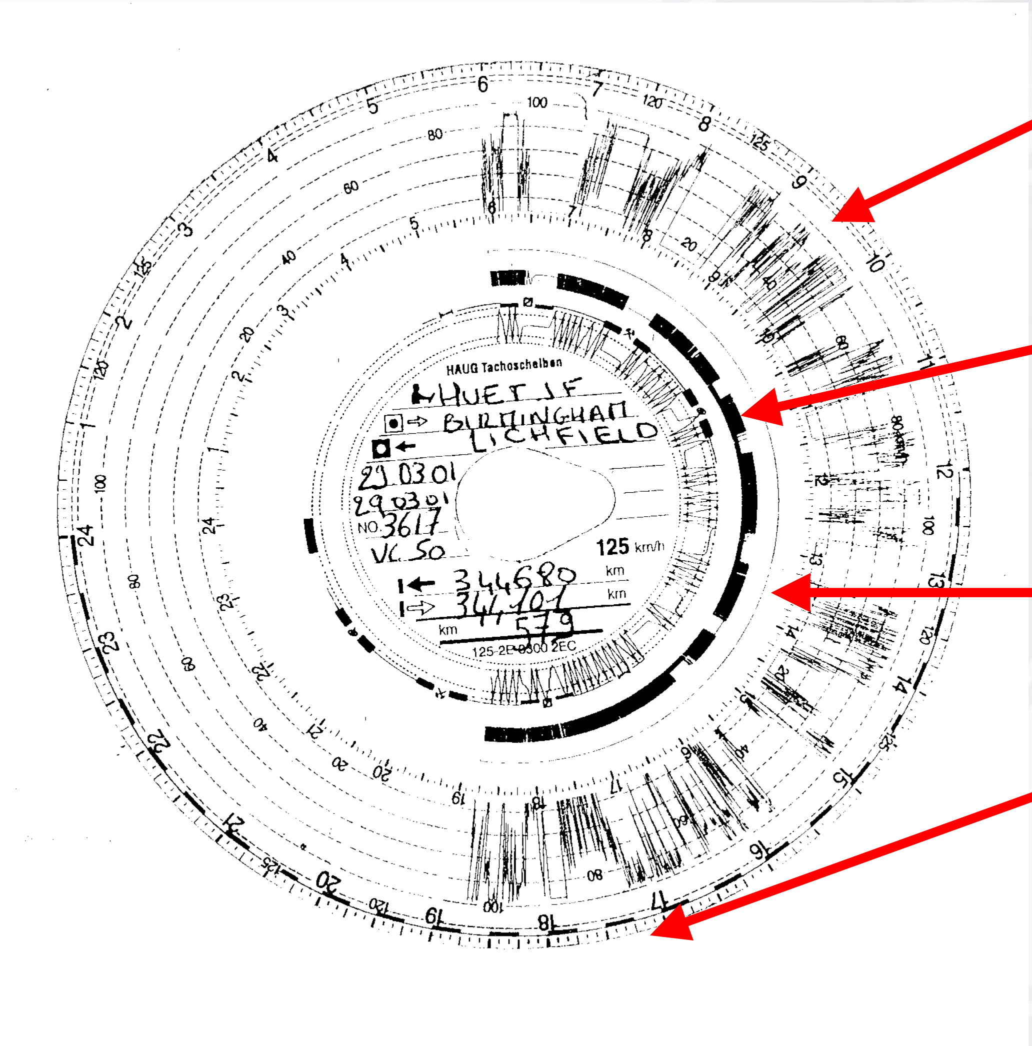
Questions?

6. Enforcement

Enforcement

With analogue tachographs

Are recorded

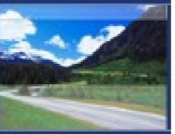


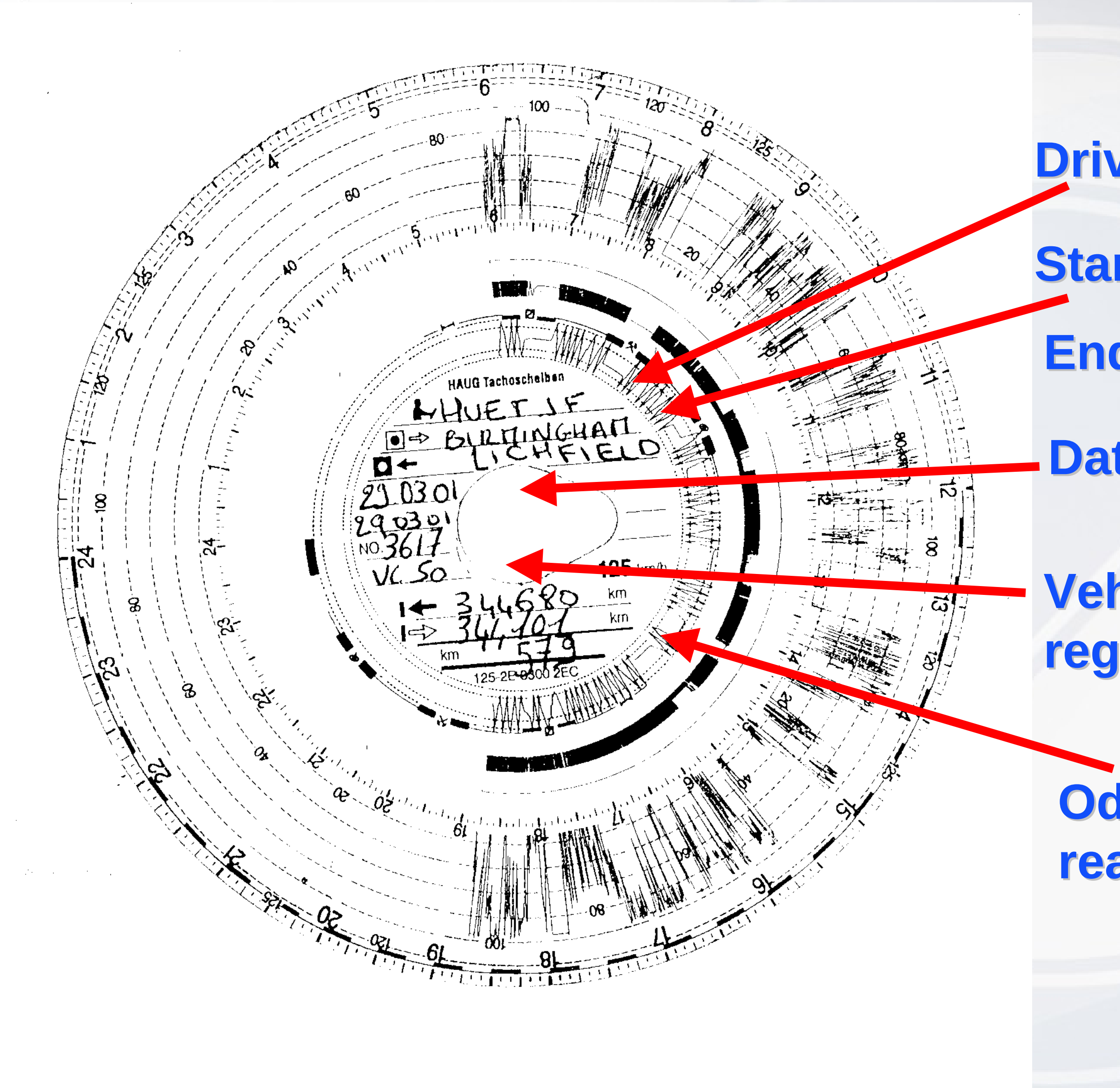
Speed

Distance

Mode of work

Time





HAUG Tachoscheiben
HUET J F
BIRMINGHAM
LICHFIELD
29.03.01
29.03.01
NO 3617
VC 50
344680 km
344101 km
km 579
125 km/h
125-2E-0300 2EC

Drivers name

Start location

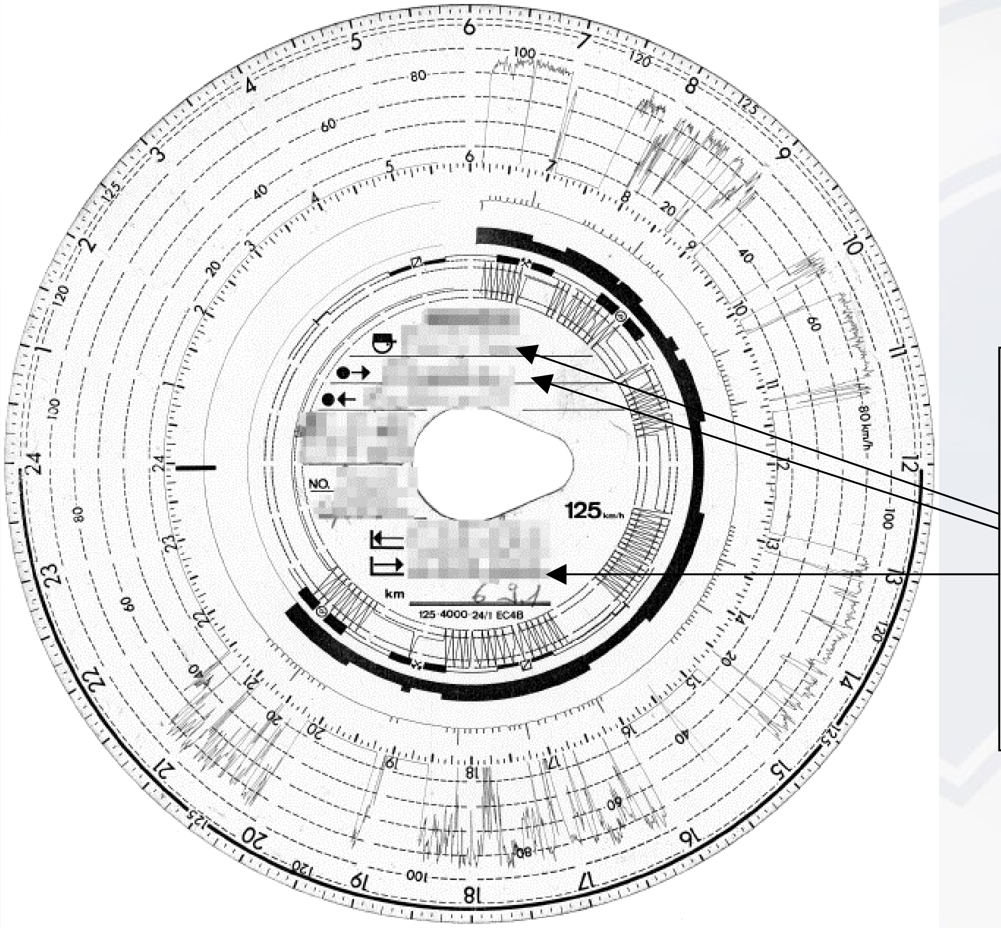
End location

Dates

Vehicle registration

Odometer readings

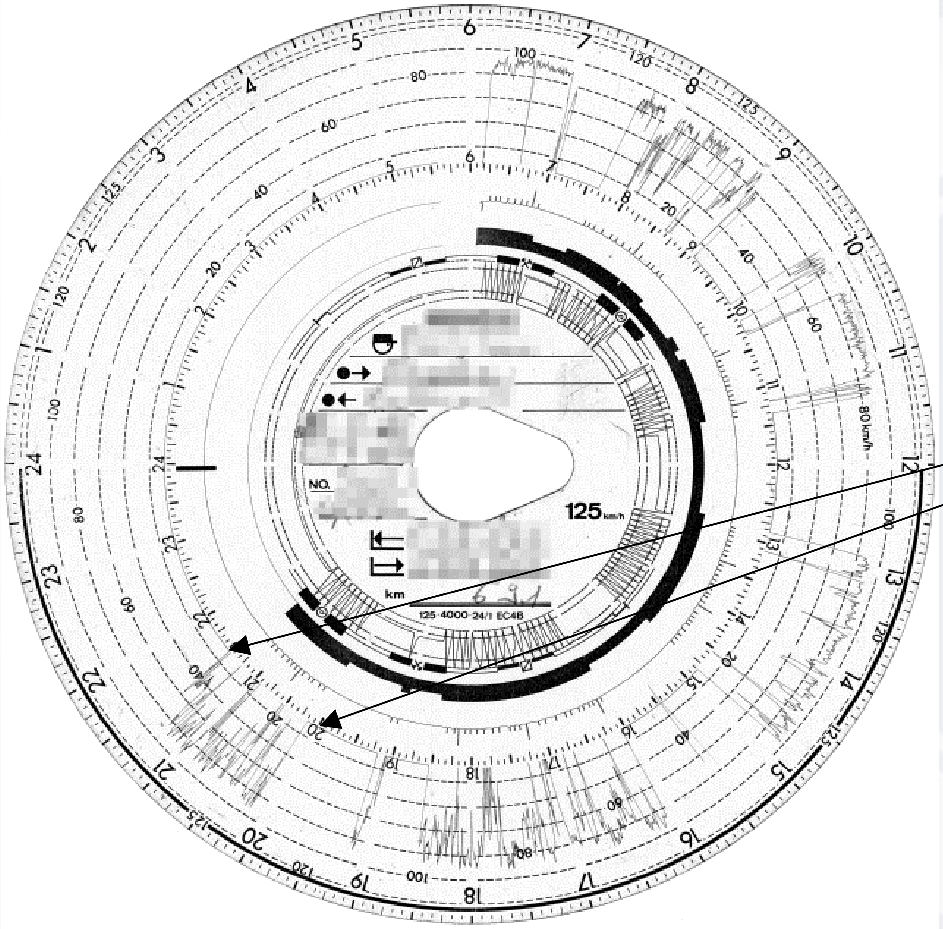
Manipulations can be detected (1)



Odometer Distance is insufficient to match geographical locations

Analogue Distance Trace

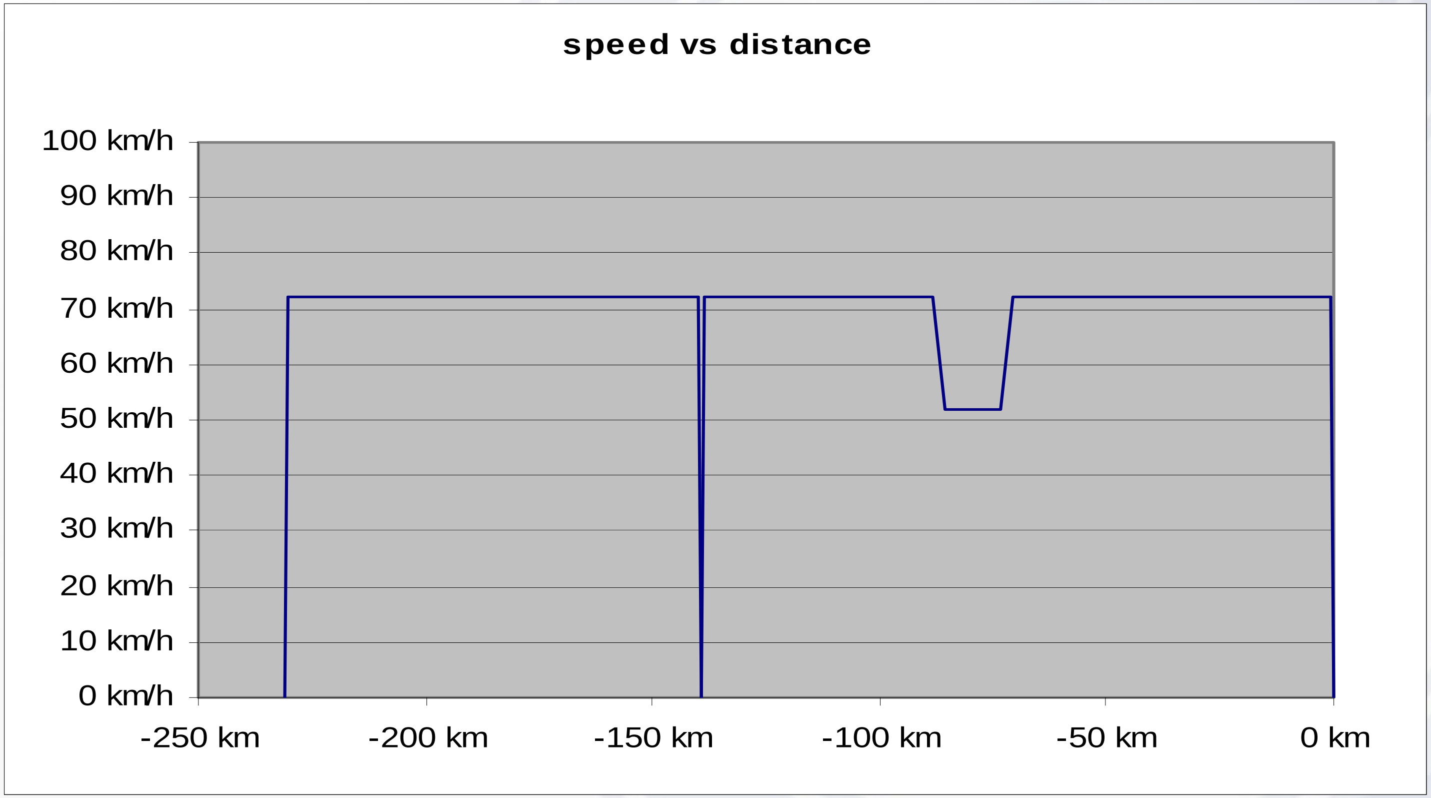
Manipulations can be detected (2)



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

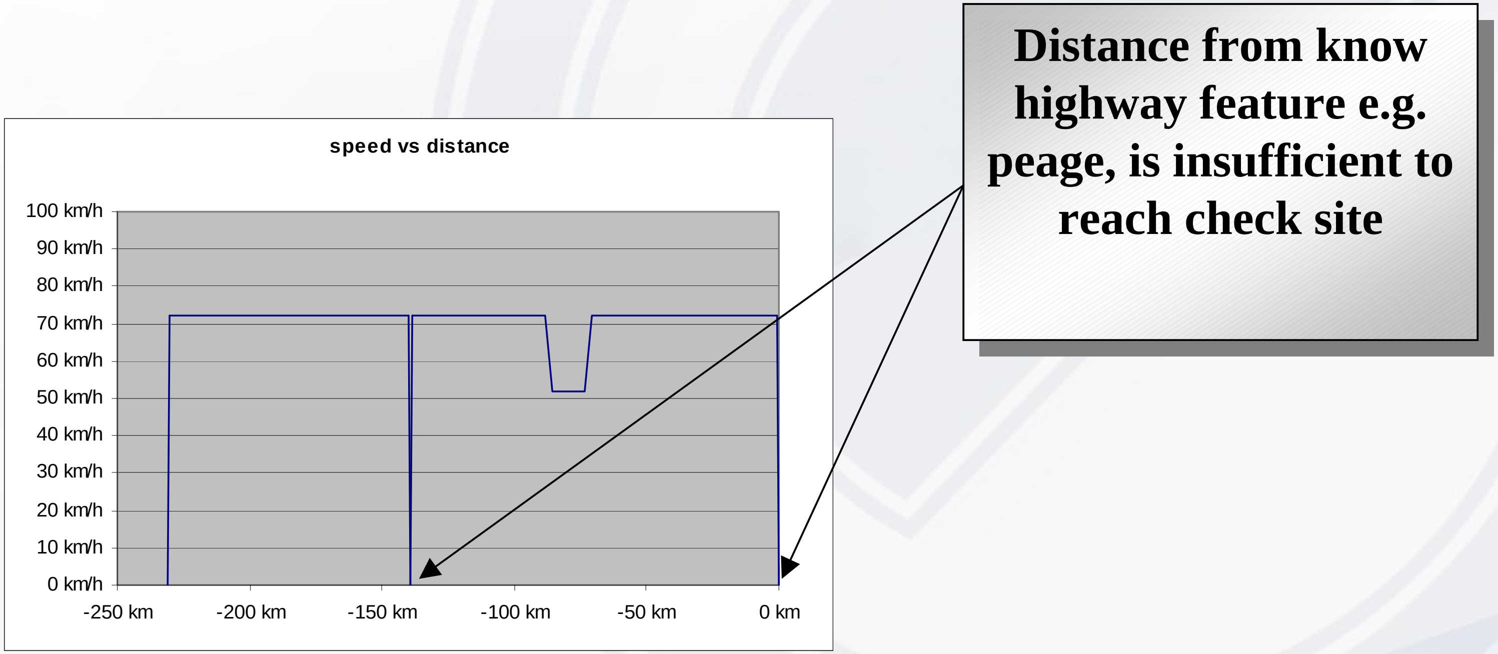
Analogue Distance Trace

Analysis software can also be used one data are scanned (1)



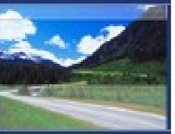
Digital Distance Trace

Analysis software can also be used one data are scanned (2)



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

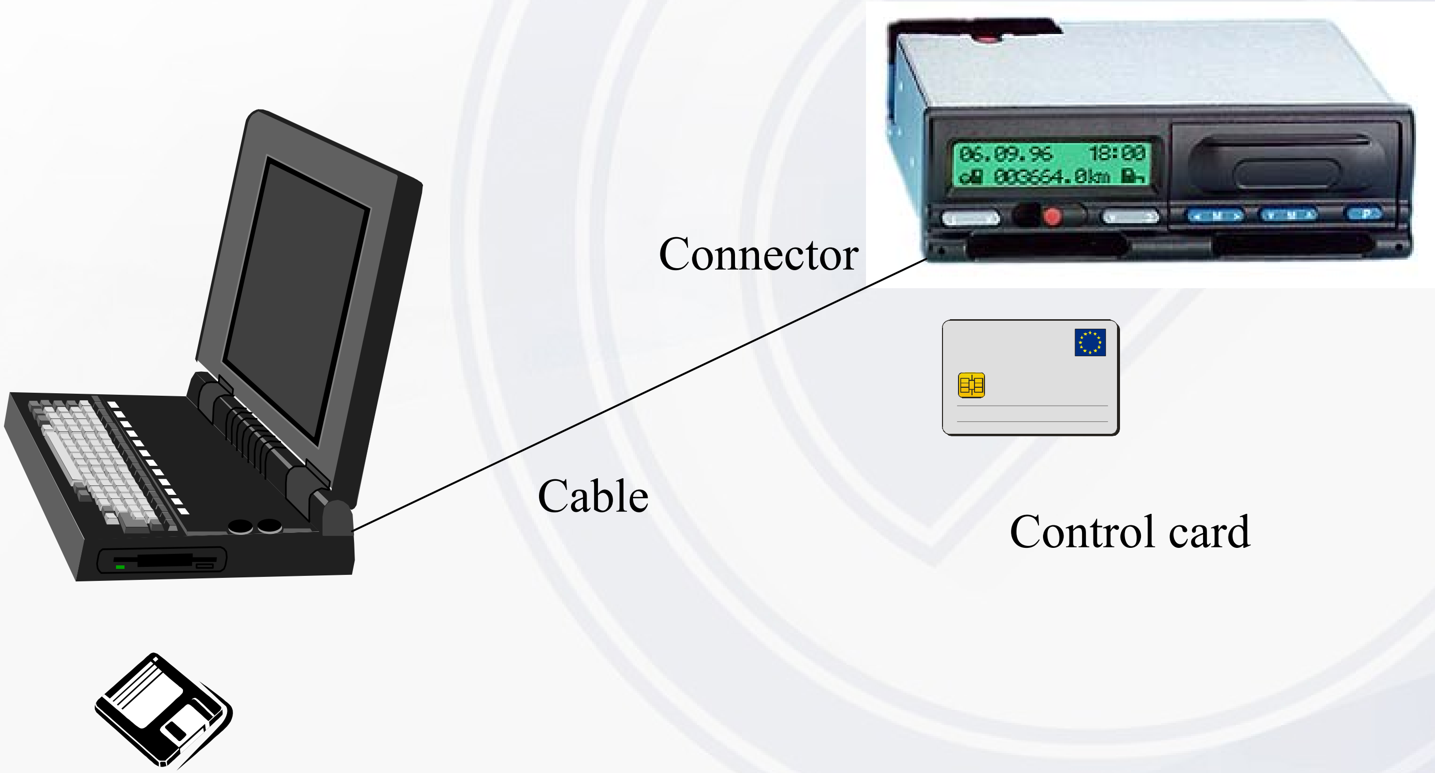
Digital Distance Trace



Enforcement

With digital tachographs

Data can be downloaded by control officers if issued with control cards



Connector

Cable

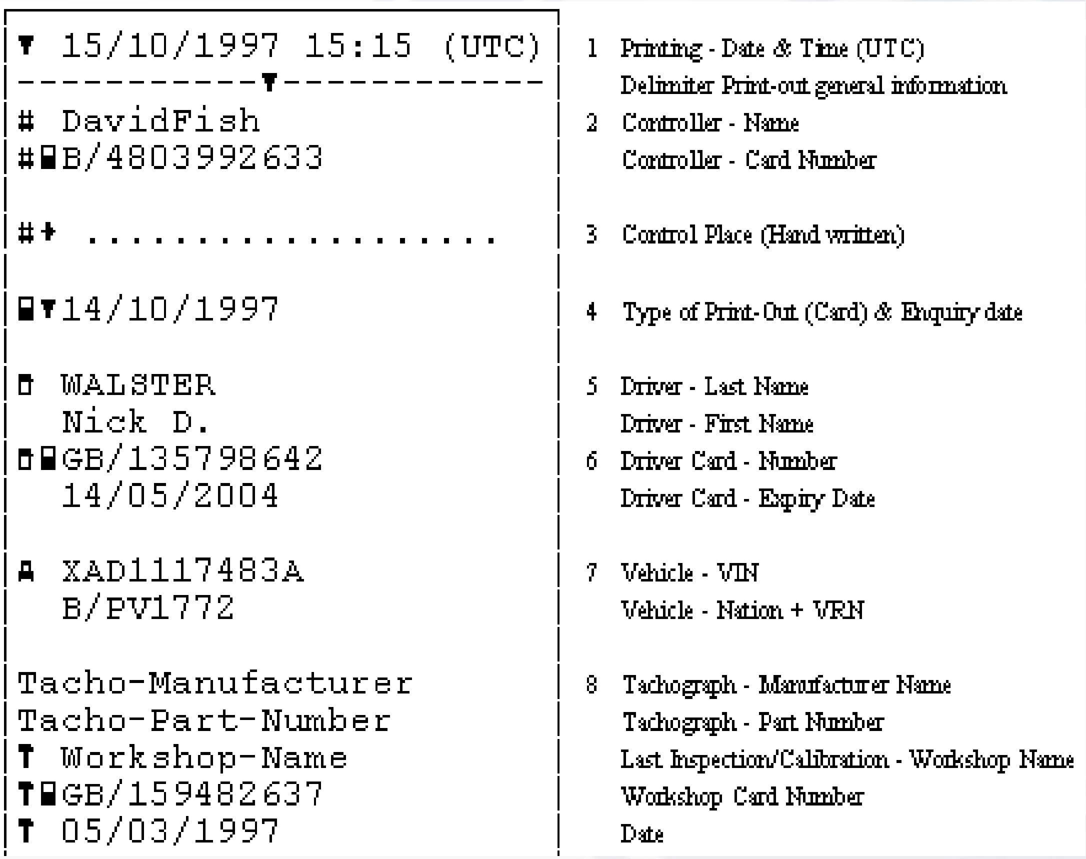
Control card

Alternative for the control officers to get access to the recording equipment's and card's data : printouts

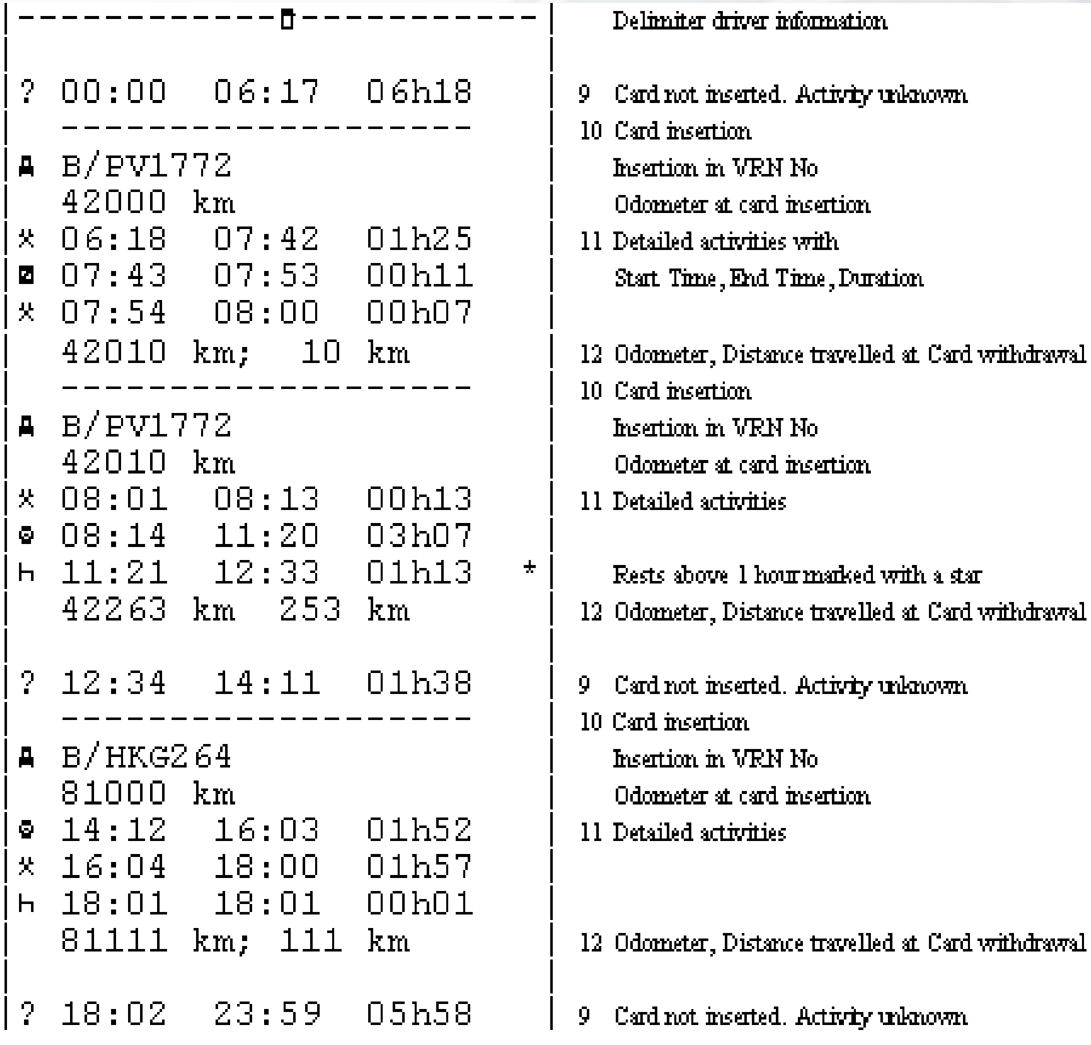
6 types of print-outs, which can be selected through the recording equipment :

- 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.

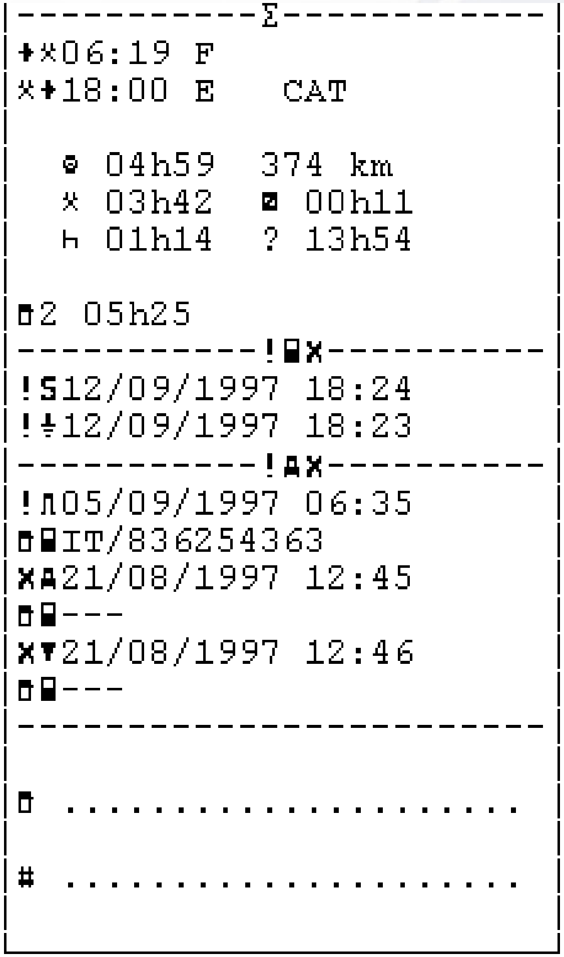
Example: drivers’ activities stored on the driver’s card



▼ 15/10/1997 15:15 (UTC)	1 Printing - Date & Time (UTC)
-----------▼-----------	Delimiter Print-out general information
# DavidFish	2 Controller - Name
#▮B/4803992633	Controller - Card Number
#✚	3 Control Place (Hand written)
▮▼14/10/1997	4 Type of Print-Out (Card) & Enquiry date
☐ WALSTER	5 Driver - Last Name
Nick D.	Driver - First Name
☐▮GB/135798642	6 Driver Card - Number
14/05/2004	Driver Card - Expiry Date
🚚 XAD117483A	7 Vehicle - VIN
B/PV1772	Vehicle - Nation + VRN
Tacho-Manufacturer	8 Tachograph - Manufacturer Name
Tacho-Part-Number	Tachograph - Part Number
T Workshop-Name	Last Inspection/Calibration - Workshop Name
T▮GB/159482637	Workshop Card Number
T 05/03/1997	Date



```
|------------▯-----------|    Delimiter driver information
|                         |
|? 00:00  06:17  06h18    |  9  Card not inserted. Activity unknown
|  -------------------    |  10 Card insertion
|🚚 B/PV1772              |     Insertion in VRN No
|  42000 km               |     Odometer at card insertion
|⚒ 06:18  07:42  01h25    |  11 Detailed activities with
|⊠ 07:43  07:53  00h11    |     Start Time, End Time, Duration
|⚒ 07:54  08:00  00h07    |
|  42010 km;  10 km       |  12 Odometer, Distance travelled at Card withdrawal
|  -------------------    |  10 Card insertion
|🚚 B/PV1772              |     Insertion in VRN No
|  42010 km               |     Odometer at card insertion
|⚒ 08:01  08:13  00h13    |  11 Detailed activities
|⊙ 08:14  11:20  03h07    |
|h 11:21  12:33  01h13   *|     Rests above 1 hour marked with a star
|  42263 km  253 km       |  12 Odometer, Distance travelled at Card withdrawal
|                         |
|? 12:34  14:11  01h38    |  9  Card not inserted. Activity unknown
|  -------------------    |  10 Card insertion
|🚚 B/HKG264              |     Insertion in VRN No
|  81000 km               |     Odometer at card insertion
|⊙ 14:12  16:03  01h52    |  11 Detailed activities
|⚒ 16:04  18:00  01h57    |
|h 18:01  18:01  00h01    |
|  81111 km; 111 km       |  12 Odometer, Distance travelled at Card withdrawal
|                         |
|? 18:02  23:59  05h58    |  9  Card not inserted. Activity unknown
```



```
|------------Σ-------------|
|▸⚒06:19 F                 |
|⚒▸18:00 E   CAT           |
|                          |
|  ⊙ 04h59  374 km         |
|  ⚒ 03h42  ⊠ 00h11        |
|  ⊢ 01h14  ? 13h54        |
|                          |
|▯2 05h25                  |
|------------!▮✖-----------|
|!S12/09/1997 18:24        |
|!⏚12/09/1997 18:23        |
|------------!▲✖-----------|
|!⎍05/09/1997 06:35        |
|▯▮IT/836254363            |
|✖▲21/08/1997 12:45        |
|▯▮---                     |
|✖▼21/08/1997 12:46        |
|▯▮---                     |
|--------------------------|
|                          |
|▯ ......................  |
|                          |
|# ......................  |
|                          |
```

Summary information

13 Start daily work time Country/Region Odometer

End daily work time Country/Region Odometer

14 Activity totals

15 Duration of crew status

16 Delimiter Cards Events and Faults

Event Security breach attempt

Event Power supply interruption

17 Delimiter Vehicle Unit Events and Faults

Event Sensor interruption

Driver Card Number

Fault VU

No card inserted

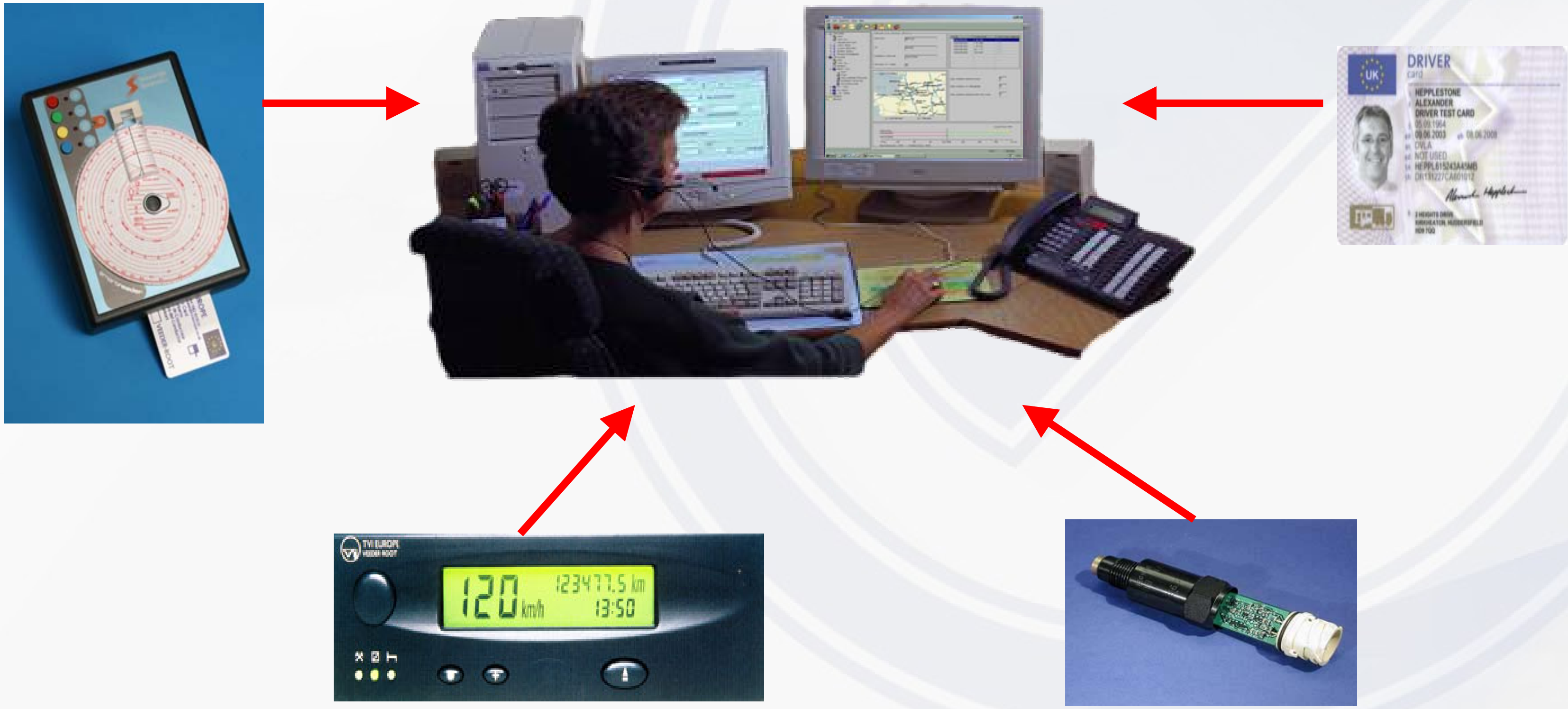
Fault Printer

No card inserted

18 Driver's signature

19 Controller's signature

Data analysis



Analogue tachographs	Digital tachographs
- Roadside checks	- Roadside checks
- Company checks	- Company checks
based on paper discs	based on paper discs **based on print-outs** **based on digital data**
	New equipments required **Control cards to be issued** **Specific training to be supplied**

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 **<u>records and stores digital data</u>** 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

- **<u>These data are accessible</u>** 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”

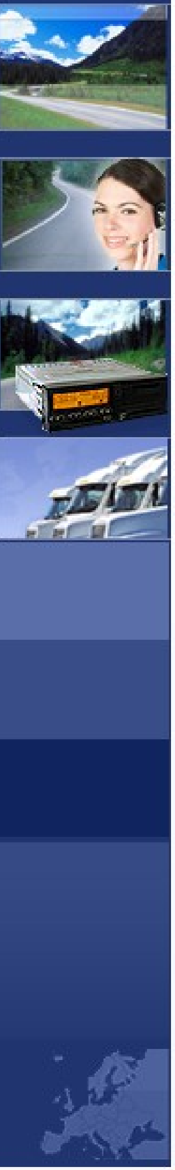
With his/her control card, a control officer can display, print, download ALL data,

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

	No Card	Driver Card	Control Card	Company Card
Print Display	All data with personal identifiers blinded	All own data + Idem No Card	All data	All data except for periods locked by other companies + Idem No Card
Download	Forbidden	Forbidden	All data	All data except for periods locked by other companies



Analogue tachographs	Digital tachographs
Data protection	Data protection
No or few requirements	**Digital tachograph's and tachograph cards' data are submitted to data protection rules (if any)**

8. Risk management

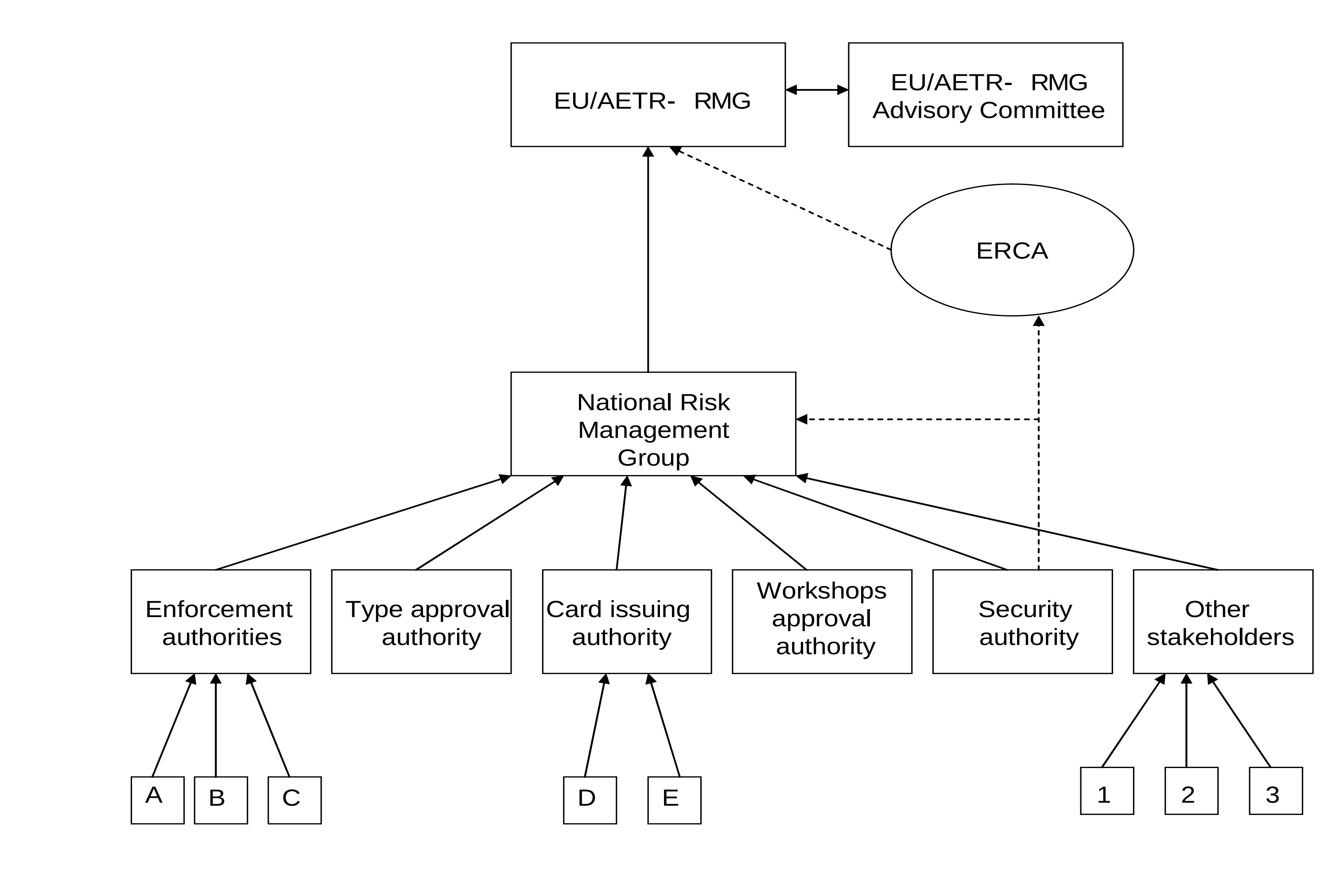
Point 5.3.38 of the ERCA policy states that:

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

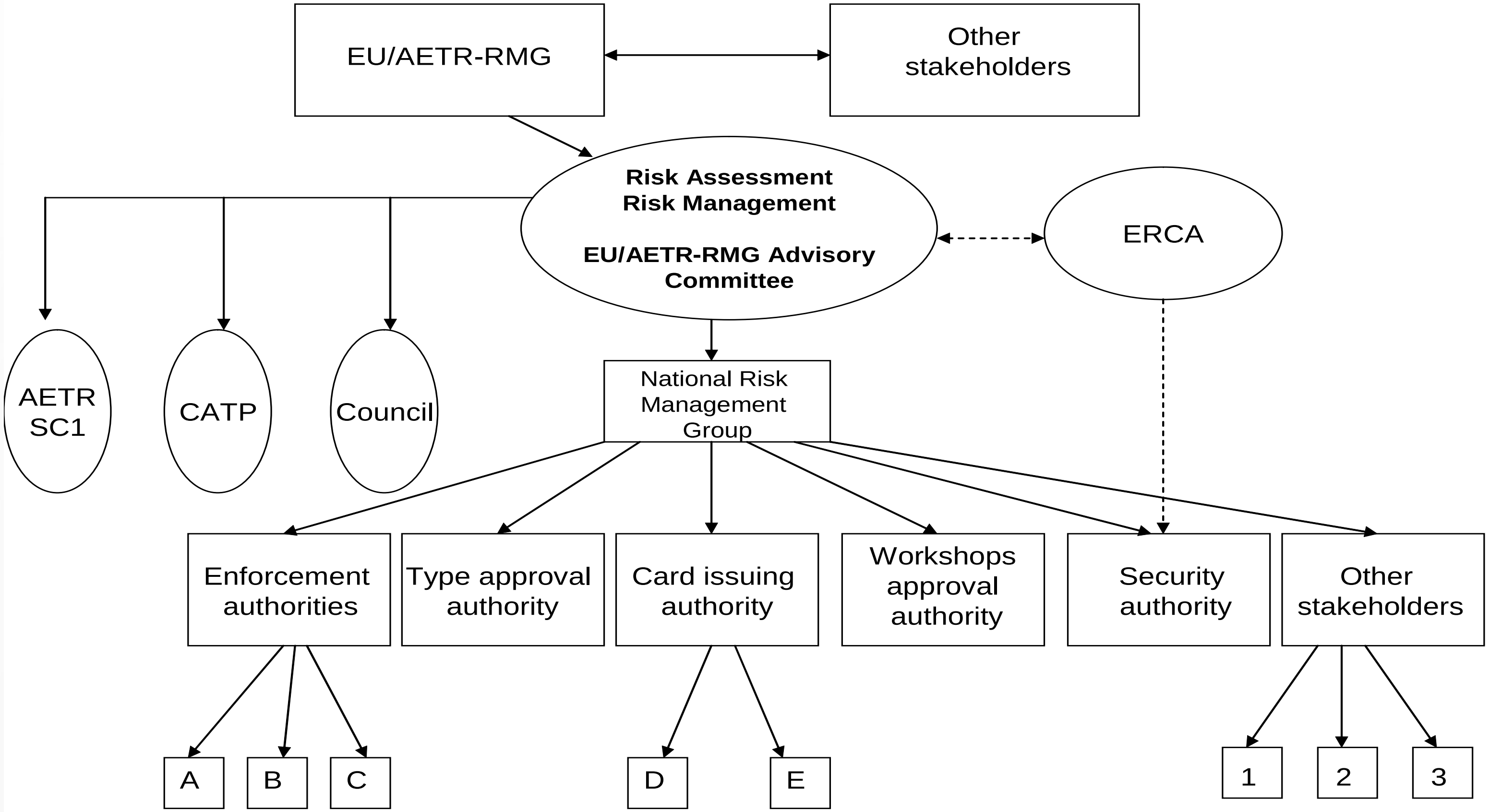
The ERCA does not cover the overall security of the digital tachograph system

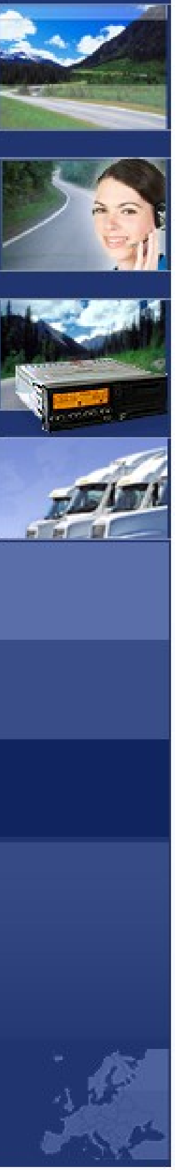
Risk management

From national authorities to the EU/AETR-RMG



From the EU/AETR-RMG to national authorities





Analogue tachographs	Digital tachographs
Risk management	Risk management
No requirement	**Policy to be implemented and maintained**

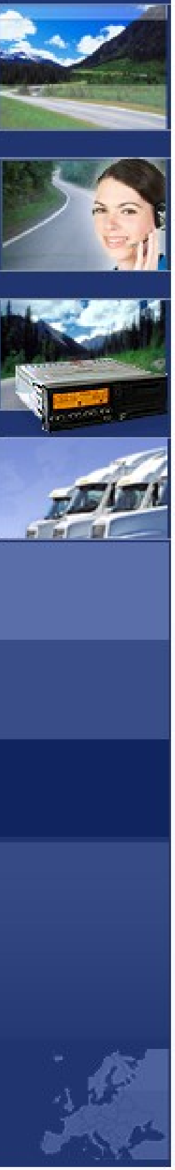
National authorities need therefore to:

- put in place a national risk management policy

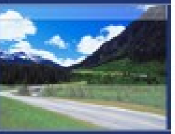
- nominate responsible bodies/persons

- maintain this policy

Timing: (2 to 6 months)

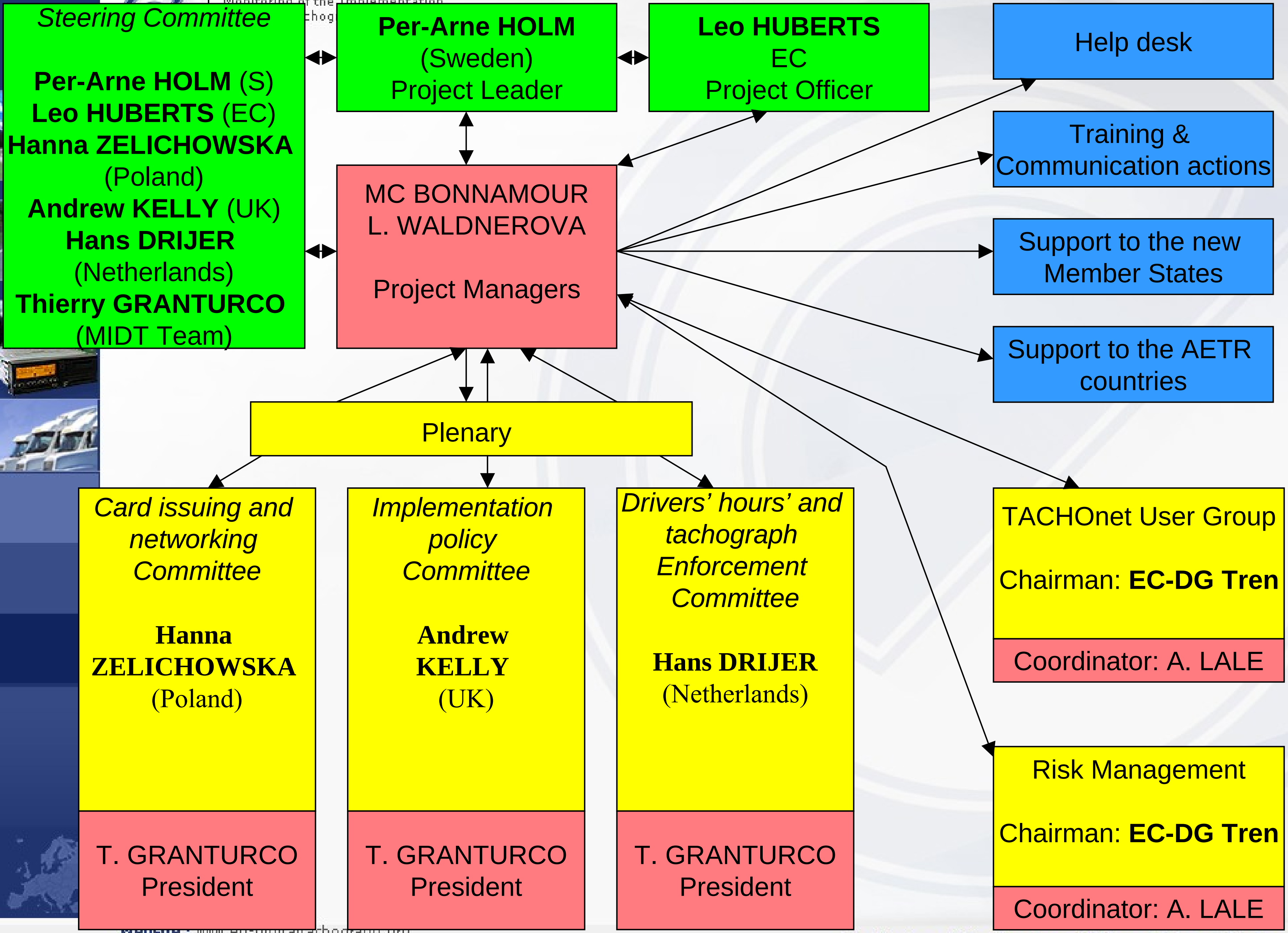


Questions?



9. Conclusion

Overview
# of the Project Organisation



Steering Committee

Per-Arne HOLM (S)
Leo HUBERTS (EC)
Hanna ZELICHOWSKA (Poland)
Andrew KELLY (UK)
Hans DRIJER (Netherlands)
Thierry GRANTURCO (MIDT Team)

Per-Arne HOLM
(Sweden)
Project Leader

Leo HUBERTS
EC
Project Officer

MC BONNAMOUR
L. WALDNEROVA

Project Managers

Help desk

Training & Communication actions

Support to the new Member States

Support to the AETR countries

Plenary

Card issuing and networking Committee

Hanna ZELICHOWSKA
(Poland)

T. GRANTURCO
President

Implementation policy Committee

Andrew KELLY
(UK)

T. GRANTURCO
President

Drivers' hours' and tachograph Enforcement Committee

Hans DRIJER
(Netherlands)

T. GRANTURCO
President

TACHOnet User Group

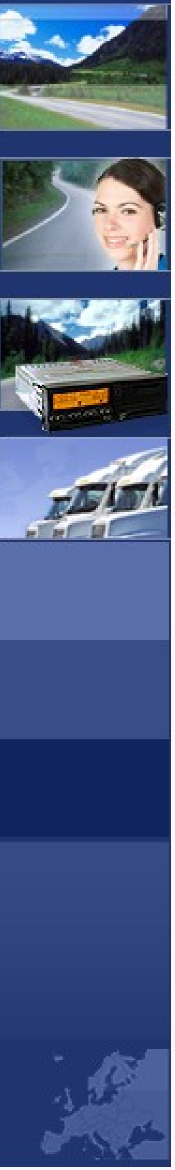
Chairman: **EC-DG Tren**

Coordinator: A. LALE

Risk Management

Chairman: **EC-DG Tren**

Coordinator: A. LALE



Tachograph life cycle	=▶	EU-MIDT/PLE/008-2006
Approval of workshops	=▶	EU-MIDT/PLE/004-2006
Roadside checks	=▶	EU-MIDT/PLE/003-2005 rev 3
Company checks	=▶	EU-MIDT/PLE/005-2006
Data management	=▶	EU-MIDT/IPC/030-2005
Card issuing	=▶	EU-MIDT/CINC/028-2005
TACHOnet	=▶	EU-MIDT/PLE/009-2006
Data protection	=▶	EU-MIDT/PLE/007-2006
Risk management	=▶	EU-MIDT/RMG/004-2006
Security	=▶	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