EU-MIDT

Plenary

EU-MIDT/PLE/011-2006

Digital Tachograph System

Guidelines on Security at workshops

PREPARED BY: IDT Project
DATE: 24/04/2006
EU-MIDT Plenary – 011-2006

REF : EU-MIDT/PLE/011-2006

EU-MIDT SECRETARIAT DOCUMENT PREPARATION

OPERATION	NAME	ORGANISATION	DATE
PREPARED BY	IDT Project		31/05/2003
CHECKED BY	Marie-Christine BONNAMOUR	Cybele – MIDT Secretariat	24/04/2006
APPROVED BY	Thierry GRANTURCO	Granturco & Partners – MIDT	24/04/2006
ISSUED BY	Secretariat	MIDT	17/05/2006

CHANGE CONTROL LIST

VERSION	DATE	NAME	DESCRIPTION

DIGITAL TACHOGRAPH SECURITY

This document contains the main principles on which the security of the digital tachograph is based.

It also addresses the very important issue of the risks to the digital tachograph scheme posed by workshops.

This second part of the report comes from a study made by Mike LISLE, from LISLE Design.

1 – MAIN PRINCIPLES OF THE SECURITY OF THE DIGITAL TACHOGRAPH

1.1 - SECURITY TARGETS

The three security targets specifying the Security Enforcing Functions (SEF) required for the digital tachograph components (motion sensor, vehicle unit (VU) and tachograph smart cards) have been evaluated by the SYNTEGRA Commercial Evaluation Facility (the SYNTEGRA CLEF is a UK approved laboratory for ITSEC evaluations) in order to provide an independent view on their suitability, completeness and appropriateness for an ITSEC E3 evaluation.

1.2 - SYSTEM-WIDE COMMON MECHANISMS AND ALGORITHMS

The component manufacturers will define most of the security mechanisms needed to fulfil these SEFs. Some security mechanisms, though, needed to be common and specified, in order to allow a full compatibility between any VU and any tachograph card and in order to allow any controller to inspect data downloaded from any VU.

Security mechanisms are closely related with security elements (e.g. cryptographic keys) distribution methods and both need to be defined together.

Therefore, this document describes the common security algorithms and key distribution methods to fulfil the following security requirements:

- Mutual authentication between VUs and cards,
- Integrity and authentication of data transferred between VUs and cards,
- Integrity and authentication of data downloaded to external storage media.

1.3 - PRINCIPLES

1.3.1 – Constraints

The main constraints taken into account in this Annex 1 B are as follows:

- the tachograph components are distributed in the field and are not connected on line to any central register for checks,
- it involves different manufacturers and different issuing authorities,
- it must cope with a step by step introduction (new Member States, new manufacturers,...),
- it must rely on leading edge but currently available and proven Information Technology,
- it must allow to periodically change the security elements.

1.3.2 - Cryptographic system

Cryptographic information technology provides security mechanisms able to fulfil authentication and data integrity requirements.

Public-Key cryptographic system

The authentication requirement implies that any element of the system (VU, card) must be able to prove its belonging to the system to any other element of the system. Each element must therefore be able to prove that it owns some secret element, which only the system (or the organisation) has been able to distribute.

Any symmetrical cryptographic system makes assumption that both entities, which must authenticate each other, share a common secret element or that one owns the secret seed of the other. This would mean, for the tachograph system, that all VUs would contain a common secret. This would be almost as unsafe as no secret.

In a public-key cryptographic system, a common secret must also exist, but without being installed in all elements (it is installed only once at the top level of a certification hierarchy).

The use of a public-key cryptographic system was therefore chosen.

Classical RSA public-key cryptographic system

Public-key cryptographic systems rely on a levelled approach, where each level possesses a pair of private and public key whose acceptability is determined using the public key of the upper level. Such a system imposes to trust the top level whose private key is the master key of the whole system.

In a classical public-key cryptographic system each level, in addition to its pair of keys, possess a certificate, delivered by the upper level, able to prove the authenticity of its public key. The top-level public key must be trusted.

Newer public-key cryptographic systems propose schemes using "implicit keys" that have the advantages of simplifying the key generation process, of requiring less space to store keys and of proposing faster cryptographic algorithms. Those schemes, however, are still in a concept phase. They have not yet been implemented nor evaluated and require algorithms that are not in the public domain.

The classical public-key cryptographic system was therefore chosen.

Three well-known algorithms fall in this category: RSA, DSA and ECDSA.

A classical RSA public-key cryptographic system has been chosen.

1.3.3 - Key distribution

A three level key distribution system has been adopted for the tachograph application:

- European level,
- Member State level,
- Equipment Manufacturer or Card personaliser level.

Those three levels must be understood as three mandatory functional levels, but not necessarily as three organisational levels.

The European level role is to generate the tachograph application master key pair (Europe secret key and Europe public key) and to certify the Member States public keys. A single organisation will soon be appointed by the European Commission to handle this task.

Member State level role is to generate the Member State key pair (Member State secret key and Member State public key), to have its public key certified by the European level, to certify the Public keys that will be inserted in the equipment, and to keep records of all certified keys.

Manufacturer level role is to generate equipment's key pairs, to have the Public keys certified by its Member State, to insert key pairs and certificates in the equipment and to eventually feed back Member State of key/Certificate assignment to equipment (if not done at certificate request time).

Equipment key pairs generation has been placed as a manufacturer responsibility. The Member State authority could also take this responsibility. In this case the transport of the private keys from the Member State authority to the equipment manufacturer must be done in a secure way.

1.3.4 - Certificates

The certificates delivered are of a recoverable type (Public key can be recovered from the certificate).

When requesting certificates, a manufacturer may or may not know the identification of the equipment in which the keys will be inserted.

In the first case, the manufacturer will send the equipment identification with the public key to its Member State authority for certification. The certificate will then contain the equipment identification, and the manufacturer must ensure that keys and certificate are inserted in the intended equipment.

In the later case, the manufacturer must uniquely identify each certificate request and send this identification with the public key to its Member State authority for certification. The certificate will contain the request identification. The manufacturer must feed back its Member State authority with the assignment of key to equipment (i.e. certificate serial number, certificate request identification, equipment identification) after key installation in the equipment.

1.3.5. – Approved Workshops and workshop cards

It is common to say that the main threats to the digital tachograph will probably be committed by some dishonest workshops/fitters using their workshop cards, or by any person who could, by a way or another, simulate the use of a valid workshop card.

We have therefore decided to identify the potential risks and this identification is addressed in the point 2 mentioned below.

2 - RISKS TO THE DIGITAL TACHOGRAPH SCHEME POSED BY WORKSHOPS

Extract from Commission Regulation (EC) n° 1360/2002, Appendix 10 – "Generic Security Targets".

This extract explicitly refers to threats faced by VUs and the related security objectives and means of achieving those objectives. There is an equivalent section which refers to threats faced by motion sensors, and the relevant additional points are also extracted below.

Of the threats etc. listed, some have been marked in italics. Those are the threats which can be influenced by workshop activities. To achieve the security objectives of the tachograph system, each of the threats identified as influenced by workshops must have a satisfactory measure in place to address that point.

2.1.- THREATS

This paragraph describes the threats the VU may face.

2.1.1. Threats to identification and access control policies

T.Access — *Users could try to access functions not allowed to them (e.g. drivers gaining access to calibration function)*

T.Identification — Users could try to use several identifications or no identification.

2.1.2. Design related threats

T.Faults — Faults in hardware, software, communication procedures could place the VU in unforeseen conditions compromising its security

T.Tests — The use of non invalidated test modes or of existing back doors could compromise the VU security

T.Design — Users could try to gain illicit knowledge of design either from manufacturer's material (through theft, bribery, –) or from reverse engineering

2.1.3. Operation oriented threats

T.Calibration_Parameters : Users could try to use mis-calibrated equipment (through calibration data modification, or through organisational weaknesses)

T.Card_Data_Exchange : Users could try to modify data while exchanged between VU and tachograph cards (addition, modification, deletion, replay of signal)

T.Clock *Users could try to modify internal clock*

T.Environment Users could compromise the VU security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical, –)

T.Fake_Devices *Users could try to connect fake devices (motion sensor, smart cards) to the VU*

T.Hardware Users could try to modify VU hardware

T.Motion_Data *Users could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal)*

T.Non_Activated *Users could use non activated equipment*

T.Output_Data Users could try to modify data output (print, display or download)

T.Power_Supply *Users could try to defeat the VU security objectives by modifying (cutting, reducing, increasing) its power supply*

T.Security_Data *Users could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment*

T.Software Users could try to modify VU software

T.Stored_Data Users could try to modify stored data (security or user data).

2.1.4. Security objectives

The main security objective of the digital tachograph system is the following:

O.Main *The data to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed*

Therefore the security objectives of the VU, contributing to the global security objective, are the following:

O.VU_Main *The data to be measured and recorded and then to be checked by control authorities must be available and reflect accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed*

O.VU_Export *The VU must be able to export data to external storage media in such a way as to allow for verification of their integrity and authenticity.*

2.1.5. Information technology security objectives

The specific IT security objectives of the VU contributing to its main security objectives, are the following:

O.Access	The VU must control user access to functions and data
O.Accountability	The VU must collect accurate accountability data
O.Audit	The VU must audit attempts to undermine system security and should trace them to associated users
O.Authentication	The VU should authenticate users and connected entities (when a trusted path needs to be established between entities)
O.Integrity	The VU must maintain stored data integrity
O.Output	The VU must ensure that data output reflects accurately data measured or stored
O.Processing	The VU must ensure that processing of inputs to derive user data is accurate
O.Reliability	The VU must provide a reliable service
O.Secured_Data_Exchange	The VU must secure data exchanges with the motion sensor and with tachograph cards.

2.1.6. Physical, personnel or procedural means

This paragraph describes physical, personnel or procedural requirements that contribute to the security of the VU.

2.1.7. Equipment design

M.Development	VU developers must ensure that the assignment of responsibilities during development is done in a manner which maintains IT security
M.Manufacturing	VU manufacturers must ensure that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security, and that during the manufacturing process the VU is protected from physical attacks which might compromise IT security.

2.1.8. Equipment delivery and activation

M.Delivery	*VU manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of non activated VUs is done in a manner which maintains VU security*

M.Activation *Vehicle manufacturers and fitters or workshops must activate the VU after its installation before the vehicle leaves the premises where installation took place.*

2.1.9. Security data generation and delivery

M.Sec_Data_Generation Security data generation algorithms must be accessible to authorised and trusted persons only

M.Sec_Data_Transport *Security data must be generated, transported, and inserted into the VU, in such a way to preserve its appropriate confidentiality and integrity.*

2.1.10. Cards delivery

M.Card_Availability *Tachograph cards must be available and delivered to authorised persons only*

M.Driver_Card_Uniqueness Drivers must possess, at one time, one valid driver card only

M.Card_Traceability *Card delivery must be traceable (white lists, black lists), and black lists must be used during security audits.*

2.1.11. Recording equipment installation, calibration, and inspection

M.Approved_Workshops *Installation, calibration and repair of recording equipment must be carried by trusted and approved fitters or workshops*

M.Regular_Inpections *Recording equipment must be periodically inspected and calibrated*

M.Faithful_Calibration *Approved fitters and workshops must enter proper vehicle parameters in recording equipment during calibration.*

2.1.12. Equipment operation

M.Faithful_Drivers Drivers must play by the rules and act responsibly (e.g. use their driver cards, properly select their activity for those that are manually selected, –).

2.1.13. Law enforcement control

M.Controls *Law enforcement controls must be performed regularly and randomly, and must include security audits.*

2.1.14. Software upgrades

M.Software_Upgrade Software revisions must be granted security certification before they can be implemented in a VU.

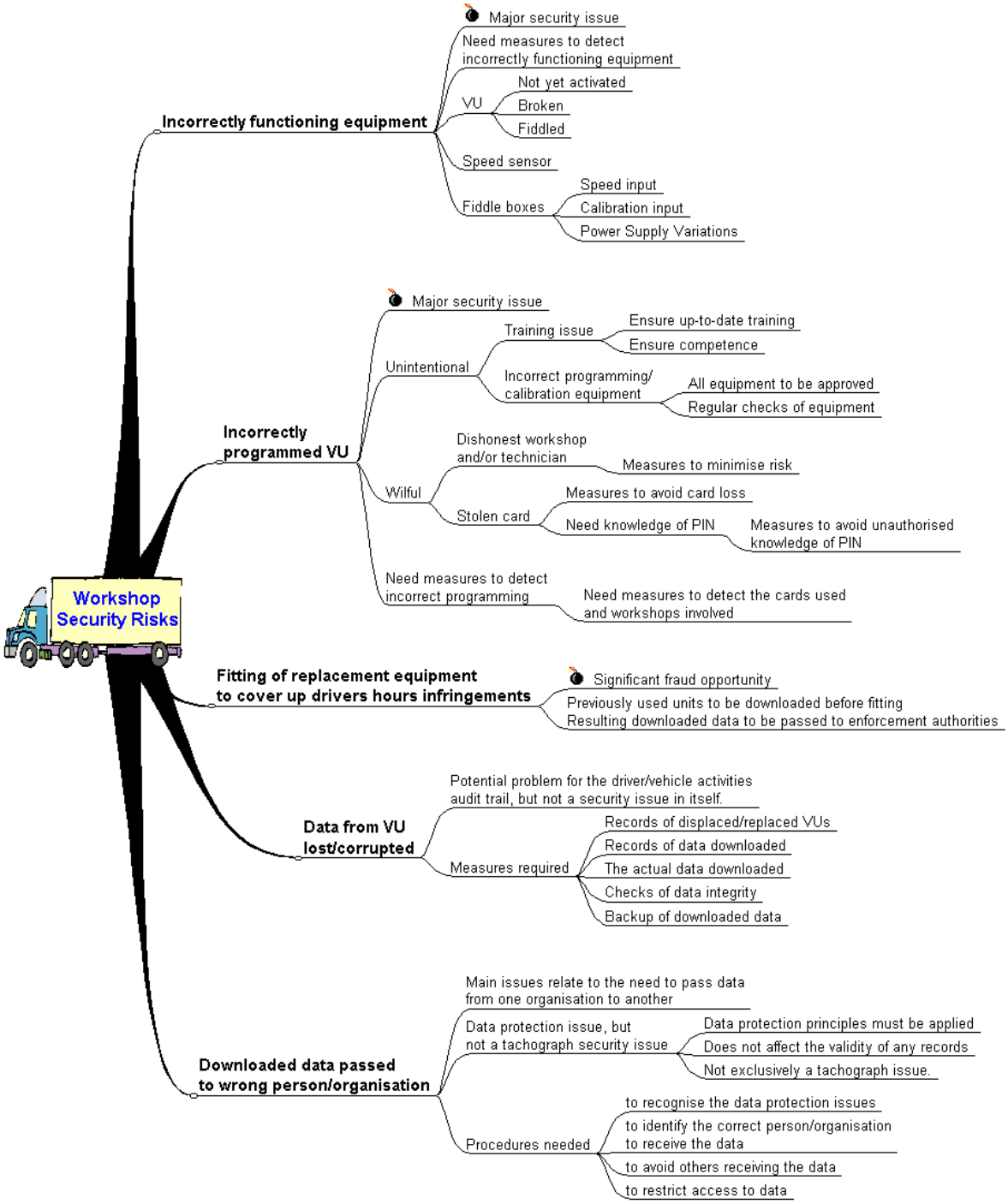
The following additional threats etc… faced by motion sensors are relevant to workshops:

T.Mechanical_Origin Users could try to manipulate the motion sensor input (e.g. unscrewing from gearbox, –)

O.Sensor_Main The data transmitted by the motion sensor must be available to the VU so as to allow the VU to determine fully and accurately the movement of the vehicle in terms of speed and distance traveled.

M.Mechanical_Interface Means of detecting physical tampering with the mechanical interface must be provided (e.g. seals)

2.2 - DIAGRAMATIC REPRESENTATION OF THE RISKS TO THE DIGITAL TACHOGRAPH SCHEME POSED BY WORKSHOPS



Workshop-Related Security Threats and Measures

Note: Throughout the following text, phrases in square brackets refer to the related threat or measure identified in EU Regulation 3821/85 Annex 1B, Appendix 10.

2.3 - SECURITY DATA

Workshops shall not handle any security data during normal workshop activities under normal workshop approval procedures. In the case that it becomes appropriate for a workshop to handle security data, then the procedures for handling of that data and implementation of those procedures shall be the subject of separate approval [T.Security_Data, M.Sec_Data_Transport].

2.4 - INCORRECTLY-FUNCTIONING EQUIPMENT

Tachograph equipment could malfunction. Such malfunctions represent a major security threat.

Malfunctions might be unintentional, as in the case of equipment failure. To counter such situations, tachograph installations must to be checked regularly [M.Regular_Inspections] (i.e. every 2 years or when there has been a significant change to the vehicle which might affect the calibration).

Drivers must betweentimes ensure that the equipment is functioning correctly [M.Faithful_drivers] and have malfunctions corrected.

Malfunctions might otherwise be intentional. To minimise this risk, fitting and calibration etc. of tachograph installations must only be carried out by authorised workshops [M.Approved_Workshops].

The staff working in such workshops that might have any influence on the fitting etc. of tachographs must be suitably vetted and approved both for competence and reliability [M.Approved_Workshops].

Workshop fitters must carry out such checks as will ensure that all components of the tachograph installation (VU, motion sensor, cables, etc.) are functioning correctly.

Motion sensors shall be secured (e.g. sealed to the gearbox) in such a way that tampering with the motion sensor or its fitting will be apparent [T.Mechanical_Origin, M.Mechanical_Interface]. Checks shall be carried out to ensure that they are fitted correctly and that the seals are intact.

As far as possible the checks carried out at workshops shall be such as to identify the existence of fake devices [M.Fake_Devices] which might cause the VU to record incorrectly or similar devices which might interrupt or otherwise modify the speed data received by the VU [M.Motion_Data].

Similarly workshop fitters shall ensure as far as possible that tachograph equipment is connected to the correct power supply (vehicle battery or wherever) without intervening equipment which might affect the supply to the tachograph equipment [T.Power_Supply].

2.5 - INCORRECTLY PROGRAMMED EQUIPMENT

Tachograph equipment in use in vehicles should always be correctly programmed to match the vehicle [T.Calibration_Parameters].

Tachograph equipment should always have a correctly set real-time clock [T.Clock]

Incorrect programming may be the result of tachograph equipment failure or of changes to the vehicle (e.g. change of tyre size). To counter such situations, tachograph installations must to be checked regularly [M.Regular_Inspections] (i.e. every 2 years) or when there has been a significant change to the vehicle which might affect the calibration.

Incorrect programming may be the result of lack of understanding/training/ competence on the part of the fitter within the workshop. To minimise this risk, all tachograph fitters shall have received appropriate approved training and shall have demonstrated their ability to carry out calibration and programming procedures correctly. [M.Faithful_Calibration]. Fitters shall undergo further training from time to time to ensure that their knowledge and competence is up-to-date.

Incorrect programming may be the result of inaccurate calibration equipment. All equipment used in a workshop which might affect the calibration of a vehicle/tachograph installation shall be of a type approved for this application and shall be checked from time to time to ensure that it is still functioning correctly [M.Faithful_Calibration].

Incorrect programming may be the result of the activities of a dishonest workshop or tachograph fitter.

Incorrect programming may be the result of use of a borrowed or stolen workshop card by an unauthorised person [T.Access]. Measures must be taken within workshops to ensure that workshop cards are kept secure at all times and available only to authorised persons [M.Card_Availablity]. Delivery of workshop cards must be traceable [M.Card_Traceability].

Any loss of workshop cards must be reported to the competent authority who must keep records of such losses [M.Card_Traceability].

In the event that a workshop card is lost or stolen, it is still only useful to others if they have knowledge of the related PIN. Measures must be taken to avoid the PIN becoming known to anyone other than the authorised holder of that card. These means must include a secure means of sending the PIN to the authorised card holder and thereafter measures to ensure that the PIN is not disclosed (e.g. by writing it on the card or by pinning up in the workshop).

To allow control authorities to check the activities of fitters and workshops, records of workshop activities (calibration, programming etc.) must be kept and made available for audit [M.Controls].

The recording capacity of individual workshop cards is such that records will quickly get overwritten by more recent data, particularly in busy workshops. Therefore it is essential that calibration etc. records are downloaded frequently and those records are subsequently retained on some other storage medium. To avoid the possibility of records being lost in the event of failure of the data storage equipment, each workshop shall implement a suitable data backup process [M.Controls].

2.6 - USE OF NON-ACTIVATED EQUIPMENT

All VUs are required to be activated immediately after fitting into a vehicle and prior to that vehicle leaving the workshop (or manufacturer's premises) [T.Non_Activated]. Workshops must comply with this requirement.

Any equipment (VUs etc.) which is stolen from a workshop will in general be in a non-activated state. Clearly the equipment will not have been programmed appropriately for any particular vehicle. It is therefore essential that workshops take all possible precautions to ensure that tachograph equipment is not stolen from the workshop [T.Non_Activated].

2.7 - FITTING OF SECOND-HAND EQUIPMENT

As far as the new user of a second-hand VU is concerned, there should be no problems provided that it is checked and confirmed to be working correctly and that it is then installed and calibrated correctly.

There is, however, a potential security issue relating to where the second-hand VU came from. In many cases its provenance will be clear – e.g. 'it came out of that crashed truck over there'. In other cases the provenance will be much less obvious. There is a well-known fraud opportunity whereby a VU is replaced in a vehicle in order to avoid discovery of serious breaches of the drivers hours regulations. To respect the main security objective of the tachograph system [O.Main], any previously-used VU should be downloaded prior to installation in the next vehicle. These downloaded records should then be made available to the appropriate control authority.

2.8 - MAINTENANCE OF DRIVERS HOURS RECORDS

The primary objective of the tachograph system is to maintain records of drivers hours. The primary security objective is to ensure that those records are available and to ensure the completeness, authenticity and integrity of those records [O.Main]. Workshops have a key part to play in this when it comes to maintenance of records from displaced VUs.

Any data downloaded by a workshop must be stored along with the related digital signature in order to verify the completeness, authenticity and integrity of the data [O.VU_Main]. Digital signatures must be checked against the related data to ensure that they correspond.

As data downloaded by workshops forms a significant part of the audit trail relating to recording of drivers hours, and as such forms part of the security of the tachograph system, measures must be taken by workshops to ensure that records are maintained and protected against loss in the event of storage equipment failure [O.Main].

Other than the main security objectives of the tachograph system to maintain data suitable for later audit by control authorities, there are no security issues identified in Appendix 10 related to downloaded data. The authenticity and integrity of downloaded data is confirmed by digital signatures which must be stored along with the data but which are otherwise outside the control of workshops.

2.9. - RECORD-KEEPING

Law enforcement controls are required to be carried out by control authorities [M.Controls]. For these controls to be possible it is essential that accurate records are kept of the activities of fitters and the vehicles and equipment installed/calibrated/programmed.

2.10. - DATA PROTECTION

Data downloaded from VUs contains 'personal data' according to the definition in the Data Protection regulations/directives. Therefore that data must be treated according to data protection rules. This is a data protection issue and explicitly *not* a tachograph system security issue.

Data protection rules require:

- Workshops could have to register under data protection legislation, depending on the national laws applicable in the different EU Member States ;
- Data must be stored such that access to that data is restricted to authorised persons.

In the case of downloaded tachograph data:

- A workshop must be satisfied that the person receiving a copy of any downloaded data is in fact authorised to receive that data ;
- A workshop must ensure that copies of downloaded data are received only by the appropriate person and not lost to or copied by others on the way.