A Review of the Digital Tachograph System

Igor Furgel[1] and Kerstin Lemke[1,2]

[1] T-Systems GEI GmbH
Solution & Service Center Test Factory & Security
Rabinstr. 8
53111 Bonn, Germany
{igor.furgel, kerstin.lemke}@t-systems.com

[2] Horst Görtz Institute for IT Security
Ruhr-Universität Bochum
44780 Bochum, Germany
lemke@crypto.rub.de

Summary. The European Commission stated the requirements for the digital tachograph system in the regulation No 1360/2002 that has to be fitted into new trucks from 5 August 2005. The digital tachograph system consists of three main components: the motion sensor, the digital tachograph and tachograph smartcards. Each component has to undergo type approval, including an ITSEC/Common Criteria security evaluation. This contribution gives an introduction for the digital tachograph system. Both the technical and non-technical security-related requirements are analysed and (potential) weak points are discussed.

Keywords: digital tachograph, vehicle unit, motion sensor, tachograph cards

1 Introduction

The European Commission regulation No 1360/2002 requires that trucks shall be equipped with a digital tachograph from 5 August 2005. The current analogue tachographs will then be replaced by a digital tachograph system. Note that the EU Directive requires that the digital tachograph is fitted into new vehicles, but not exchanged in vehicles which are already in service.

Originally, the fitting of digital tachographs into all new vehicles was fixed to 5 August 2004. In the meantime, it has turned out that this date is no longer realistic. In a letter dated at 21 April 2004 the EU Commission introduced a moratorium of 12 months starting on 5 August 2004 for the fulfillment of the requirements for the digital tachograph system in all Member States. Now, there are some discrepancies between the European Commission and the EU Parliament concerning the introduction of the digital tachograph (see press

report of the EU Parliament of 13 April 2005, doc. A6-0076/2005). Parliament took the view that all vehicles manufactured after 5 August 2006 should be fitted with this recording equipment. After August 2007, all vehicles put into service for the first time should be fitted with these digital instruments. This question should be agreed in the Conciliation Committee.

Tachographs have been developed to control the working and rest hours of truck drivers as well as the vehicle speed. The EU Commission aims to improve road safety by minimizing accidents that are caused by overtired or speeding truck drivers.

The concern of the EU Directive conflicts with the commercial interest of transport companies. Organisational and technical means have been found to bypass the control of working hours and speed using analogue tachographs. One procedural offense is described in [11]: two drivers swap their vehicles half-way through the working day. If controlled, they show only each second tachograph chart to the control person, so it seems that they stayed overnight at the changing location.

The analogue tachographs do not make use of secured communication channels and could be easily by-passed technically. Ross Anderson showed in [11] that so called "Italian Devices" are available for sale that are fitted in between the analogue tachograph and the motion sensor. This "man in the middle" attack allows control of the forwarding of the number of pulses sent by the motion sensor. There are commercial devices available that leave out 10% or 20% of the pulses on behalf of the driver.

The parties involved in operation are the drivers and transport companies, the workshops, and the enforcing police authorities. Security-relevant manipulations at the tachograph system have to be recognised by the control personnel.

This paper aims to provide an introduction to the binding of the technical components involved as well as the non-technical assumptions on the working environment. Further, some constructional weaknesses are analysed.

2 General Architecture

The general architecture of the digital tachograph system is represented in Fig. 1.

The *tachograph system* consists of the *recording equipment* and *tachograph cards* embedded into the technical and organisational infrastructures (among other key management and fitter workshops) being run by the respective Member State operators.

The *recording equipment* comprises two different elements, as there are the *vehicle unit* (digital tachograph) and the *motion sensor*. It is intended for installation in road vehicles to show, record and store automatically or semi-automatically details of the movement of such vehicles and of certain work periods of their drivers.

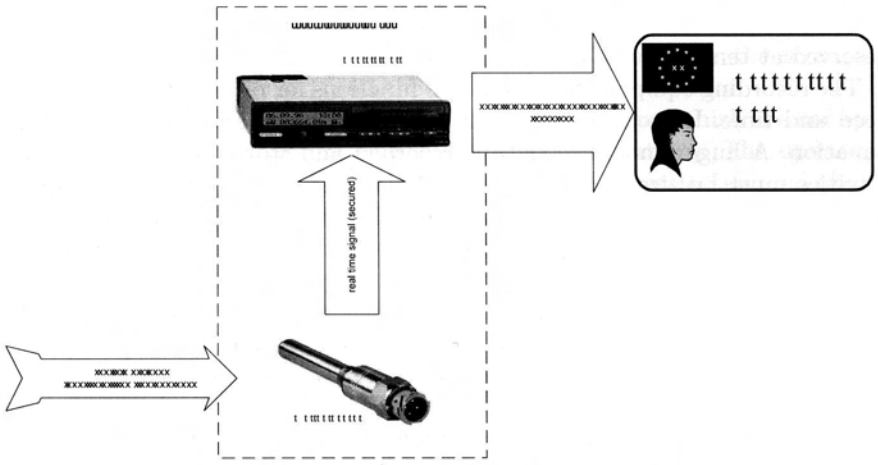

Fig. 1. Architecture of the digital tachograph system

The motion sensor is normally installed in the gearbox of a vehicle and provides a signal representative of vehicle speed and/or distance traveled to the vehicle unit. The latter processes these real-time signals and records the relevant data. The physical information on the vehicle's motion is gained by a mechanical interface.

The tachograph card represents an intelligent storage medium distinguishing different user groups and managing the relevant data. Each user group is equipped with its dedicated tachograph card. The following user groups are defined:

- driver (white card),
- forwarding company (yellow card),
- workshop (red card), and
- control authority (blue card).

After a valid tachograph card has been inserted into one of the two slots for smartcards at the vehicle unit, a mutual authentication between the vehicle unit and the card is performed, so that the vehicle unit "knows" the user operating it. On the other side, the tachograph card is sure that it communicates with a genuine vehicle unit.

3 Functional Specification of the Recording Equipment

The purpose of the recording equipment is to record, store, display, print, and output data related to activities of the system users (i.e. drivers, companies, workshops and controllers). The recording equipment should be fully operational under quite demanding environmental conditions, e.g., the vehicle unit in the temperature range minus 20°C to 70°C and the motion sensor in

the temperature range minus 40°C to 135°C. Data memory content shall be preserved at temperatures down to minus 40°C.

The recording equipment provides the functions for measuring of distances, speed and time. It monitors the activities of the users and creates audit information. A huge amount of data is recorded and stored, e.g., many driver activities must be stored for at least 365 days. Herein, we omit a complete list of data items and refer to the EU Directive [1]. The recording equipment includes different output channels: information can be displayed and printed and there is a secured data download channel. Moreover, functions for the configuration of the recording equipment – the pairing of the vehicle unit with the motion sensor, calibration of the recording equipment and time adjustment – are included. For a complete description of functional requirements we refer the reader to section 3 of [1].

The recording equipment recognizes four modes of operation:

- operational mode,
- company mode,
- calibration mode, and
- control mode.

After a valid tachograph card has been inserted into and recognised (authenticated) by the vehicle unit, the latter switches to a mode of operation according to the rules of [1].

Access conditions on functions provided by and data stored in the vehicle unit depend on its current mode of operation. In order to enforce the prescribed access conditions the vehicle unit implements an integral access control functionality monitoring the current mode of operation and all requests for functions and data. The access control function decides about granting or denying of access to these resources.

4 Functional Specification of the Tachograph Cards

The main purpose of the tachograph cards is to store the relevant data kept by the recording equipment. There are three groups of data to be stored, as shown in Fig. 1.

The electronic part of the tachograph cards is compliant with ISO/IEC 7816 "Identification cards–Integrated circuits with contacts". The tachograph cards should be capable of operating correctly within a five-year period in all the climatic conditions normally encountered in European Community territory and at least in the temperature range minus 25°C to +70°C with occasional peaks of up to +85°C.

The data structures and the access conditions of the files stored on the tachograph cards are specified in section 4 of [1], Appendix 2. This section does not specify the structures used for cryptographic keys and the workshop PIN needed: these structures can be individually defined by each manufacturer.

The minimum storage capacity needed for tachograph data is more than 11 kbytes. On the driver card, this amount is mainly used for the storage of activities, the vehicles used, and the events and faults.

Note that all data files (except for cryptographic keys, which are not specified) can always be read out (without any authentication). The update requires a successful execution of the mutual device authentication and the use of secure messaging. Identification data can never be updated.

Table 1. Data to be stored by the tachograph cards

Data to be stored	Card type			
	driver	workshop	control	company
Card identification and security data (initialisation data)				
application identification	x	x	x	x
chip identification	x	x	x	x
IC card identification	x	x	x	x
standard security elements	x	x	x	x
specific security elements	-	x	-	-
Card personalisation data				
card identification	x	x	x	x
card holder identification	x	x	x	x
driving licence information	x	-	-	-
Activity data				
vehicles used data	x	x	-	-
driver activity data	x	x	-	-
daily work periods start and/or end	x	x	-	-
events and faults data	x	x	-	-
control activity data	x	x	x	-
company activity data	-	-	-	x
card session data	x	-	-	-
specific conditions data	x	x	-	-
calibration and time adjustment	-	x	-	-

All data records are organised as ring data structures, so that the newest record will overwrite the oldest record, when the data container is full.

5 Security Requirements

5.1 Recording Equipment

The security of the recording equipment aims to protect

- the data recorded and stored in such a way as to prevent unauthorised access to and manipulation of the data and detecting any such attempts,
- the integrity and authenticity of data exchanged between the motion sensor and the vehicle unit,
- the integrity and authenticity of data exchanged between the recording equipment and the tachograph cards, and
- the integrity and authenticity of data downloaded.

The security requirements for the components of the recording equipment are comparable to the requirements of cryptographic modules, except for the physical security (see Section 8.13).

The general evaluation assurance level defined is ITSEC E3 high or Common Criteria EAL 4+ [2].

5.2 Tachograph Cards

The tachograph card security aims

- to protect the integrity and authenticity of data exchanged between the cards and the recording equipment,
- to protect the integrity and authenticity of data downloaded from the cards,
- to exclude any possibility of falsification of data stored in the cards,
- to detect any attempt and to prevent tampering of that kind.

The Tachograph Card Generic Security Target in Annex 10 of [1] requires that the integrated circuit (IC) of the smartcard is compliant with the

- Smartcard Integrated Circuit Protection Profile – version 2.0 – issue September 1998, registered at French certification body under the number PP/9806 [7], or
- alternatively (see [2]) the BSIPP02: Smartcard IC Platform Protection Profile, 1.0, issued by the "Bundesamt für Sicherheit in der Informationstechnik" [6]

The compliance with these protection profiles is further refined in Appendix 10 of [1].

The general evaluation assurance level defined is ITSEC E3 high or Common Criteria EAL 4+ [2].

5.3 Key Management

The EU legislative for the Digital Tachograph provides in Appendix 11 of the Annex I (B) two different cryptographic systems:

- the *asymmetric* cryptographic system for securing the communication between the vehicle unit and the tachograph card, and
- the *symmetric* cryptographic system with splitting key technology for securing communication between the vehicle unit and motion sensor within the recording equipment.

Asymmetric Cryptography "Vehicle Unit ↔ Tachograph card"

The asymmetric cryptographic system for the digital tachograph is based on the standard Public Key Infrastructure (PKI). The following three hierarchical levels of this PKI are defined:

- European level,
- Member State level, and
- equipment level.

Figure 2 represents the general context of the PKI through the entire hierarchy.

The Digital Tachograph System European Root Policy (Administrative Agreement 17398-00-12 (DG-TREN)) defines the general conditions for the PKI concerned and contains accordingly more detailed information.

The **European Authority** being responsible for the European Root Certification Authority policy is represented by

European Commission
Directorate General for Transport and Energy
Unit E4 – Satellite Navigation System (Galileo); Intelligent Transport
Rue de Mot, 28
B-1040 Bruxelles.

The **European Root Certification Authority** (ERCA) responsible for implementation of the ERCA policy and for the provision of key certification services to the Member States is represented by

Digital Tachograph Root Certification Authority
Traceability and Vulnerability Assessment Unit
European Commission
Joint Research Centre, Ispra Establishment (TP.360)
Via E. Fermi, 1
I-21020 Ispra (VA)

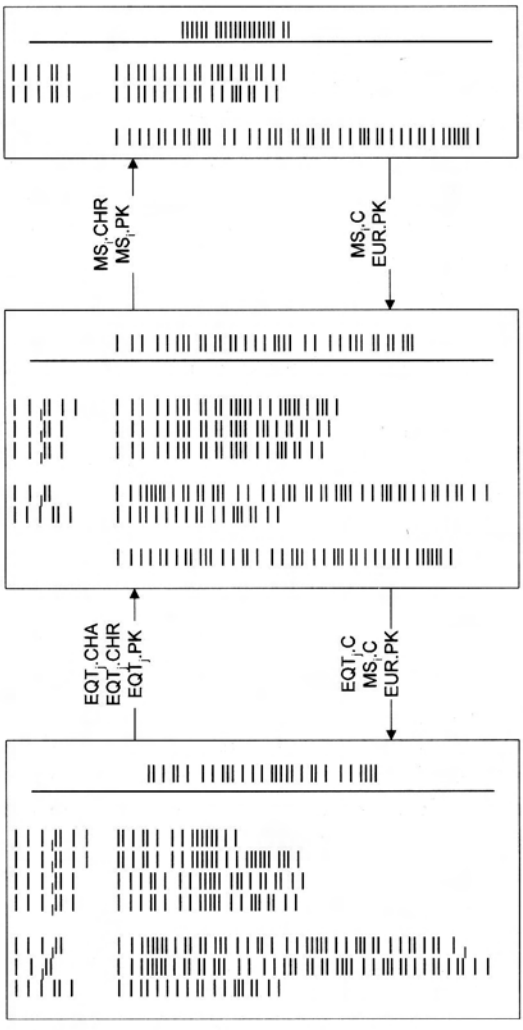

Fig. 2. PKI hierarchy

The ERCA policy [9] is not a part of the Commission Regulation 1360/2002 and represents an important additional contribution. It was approved by the European Authority on 9 July 2004. The ERCA policy is available in electronic form from the web site `dtc.jrc.it`.

At the European level, ERCA generates a single European key pair (EUR.SK and EUR.PK). It uses the European private key to certify the Member States' public keys and keeps the records of all certified keys. A change of the European (root) key pair is not intended.

Each Member State of the European Union establishes its own national **Member State Authority** (MSA) usually represented by a state authority,

e.g. Ministry of Transport. The national MSA runs some services, among others the **Member State Certification Authority** (MSCA). The MSA has to define an appropriate Member State Policy (MSA policy) being compliant with the ERCA policy. At the Member State level, each MSCA generates a Member State key pair (MS_i.SK and MS_i.PK). Member States' public keys are certified by the ERCA (MS_i.C). MSCAs use their Member State private key to certify public keys to be inserted in equipment (vehicle unit or tachograph card) and keep the records of all certified public keys with the identification of the equipment concerned. MSCA is allowed to change its Member State key pair.

At the equipment level, one single key pair (EQT_j.SK and EQT_j.PK) is generated and inserted in each equipment unit (vehicle unit or tachograph card). Equipment public keys are certified by a Member State Certification Authority (EQT_j.C). This key pair is used for

- authentication between vehicle units and tachograph cards,
- enciphering services: transport of session keys between vehicle units and tachograph cards, and
- digital signature of data downloaded from vehicle units or tachograph cards to external media.

The respective MSA (MSA component personalisation service) is responsible for issuing of equipment keys, wherever these keys are generated: by equipment manufacturers, equipment personalisers or MSA itself.

Integrity and authenticity of the entities to be transferred between the different levels of the PKI hierarchy are subject to the ERCA and MSA policies.

The concrete cryptographic algorithm currently being used for the asymmetric cryptographic system is the RSA algorithm. All RSA keys (whatever the hierarchical level) have a length of modulus of 1024 bits.

Symmetric Cryptography "Vehicle Unit ↔ Motion Sensor"

The symmetric cryptographic system for the digital tachograph is based on the splitting key technology. Figure 3 represents the general management of the relevant keys.

The ERCA generates two symmetric partial master keys for the motion sensor: Km_{wc} and Km_{vu}. The first partial key Km_{wc} is intended to be stored in each workshop tachograph card; the second partial key Km_{vu} is inserted into each vehicle unit. The final master key Km results from XOR (exclusive OR) operation between Km_{wc} and Km_{vu}. The additional identification key Kid is calculated as XOR of the master key Km with a constant control vector CV.

The final master key Km and the identification key Kid are used for authentication between the vehicle unit and the motion sensor as well as for an encrypted transfer of the motion sensor individual pairing key Kp from the motion sensor to the vehicle unit. The master key Km and the identification

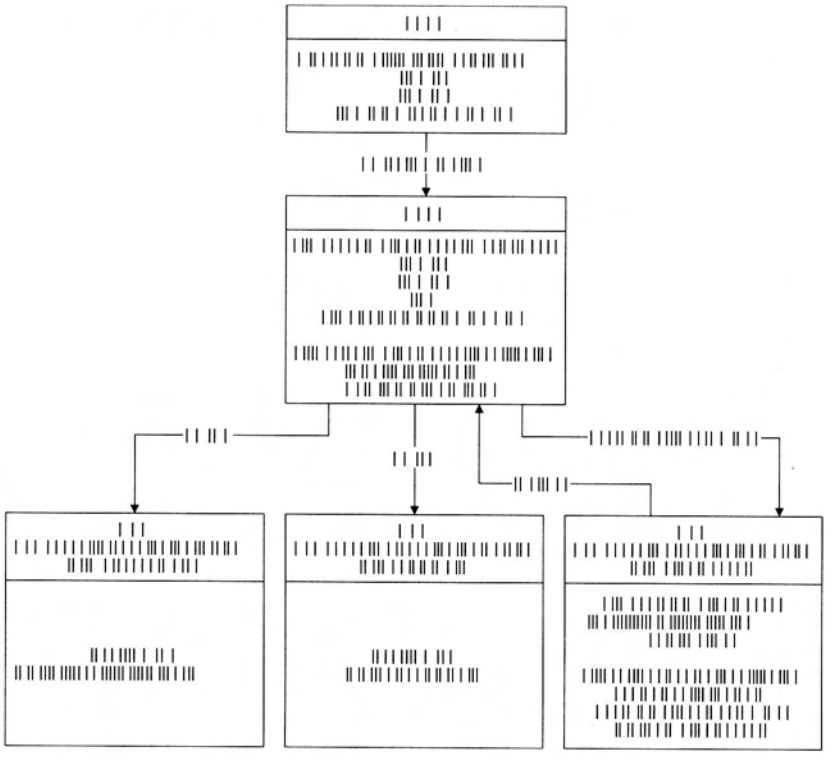

Fig. 3. Key management for the motion sensor

key Kid are used merely during the pairing of a motion sensor with a vehicle unit (see ISO 16844-3 [3] for further details). They are stored neither in the motion sensor nor in the vehicle unit.

Confidentiality, integrity and authenticity of the entities to be transferred between the different levels of the hierarchy within the tachograph system are subject to the ERCA and MSA policies.

The concrete cryptographic algorithm currently being used for the symmetric cryptographic system is the Triple-DES algorithm. Both Triple-DES partial master keys have an effective length of 112 bits (total length of 128 bits).

6 Communication Protocols

6.1 Vehicle Unit and Tachograph Card

Appendix 11 of Annex I (B) of the EU legislative provides two communication phases at the logical level:

- identification and authentication phase and
- operational phase.

During the first phase both communicating parties authenticate each other. As the result of this authentication a common symmetric session key will be established. This session key remains valid till the card is withdrawn from or reset by the vehicle unit. This session key is used for communication between the entities within the operational phase.

Authentication

A mutual authentication between the VU and the tachograph card is required by the EU legislative. Each communicating party should demonstrate to the other that it owns a valid tachograph key pair, the public key of which has been certified by a Member State certification authority, itself being certified by the European certification authority as described above in Section 5.3. The mechanism is triggered at card insertion by the VU. It starts with the exchange of certificates and unwrapping of public keys, and ends with the setting of a session key. Demonstration is made by signing with the equipment private key a random number sent by the other party, which must recover the random number received when verifying this signature and compare the values of the random number sent with the random number received. The relevant protocol is exactly defined in Appendix 11 of Annex I (B) of the EU legislative.

Operation

The operational communication between the VU and the tachograph card can be performed either

1. in plain or
2. using secure messaging in authenticated mode or
3. using secure messaging in encrypted and authenticated mode.

The communication at the logical level succeeds by using the smartcard command set defined in Appendix 2 of Annex I (B) of the EU legislative (see also Section 4). Whether and which secure messaging mode will be used is also defined there.

6.2 Motion Sensor and Vehicle Unit

The EU legislative requires the communication protocol between the motion sensor and the vehicle unit to be compliant with ISO 16844-3 "Motion Sensor interface". This ISO standard provides two communication phases at the logical level:

- pairing phase and

- operational phase.

During the pairing phase a motion sensor will be "paired" with a vehicle unit. As the result of this pairing a common symmetric session key will be established. This session key remains valid till the next pairing and is used for communication between the entities within the operational phase. Note that this session key is valid for up to 2 years. The pairing can be performed only by an accredited workshop possessing a genuine, valid tachograph workshop card. Generally, the motion sensor implements a set of instructions and plays a passive role, whereas the VU plays an active role in sending these instructions to the motion sensor.

Pairing

Pairing of a motion sensor with a vehicle unit is triggered by a special instruction sent from the VU to the motion sensor. A valid tachograph workshop card must be inserted into and accepted by the VU. After a successful mutual authentication between the workshop card and the vehicle unit, the VU reads out the workshop card part of the master key Km_{wc}. The vehicle unit recomputes the final master key from $\mathrm{Km} = \mathrm{Km}_{vu} \oplus \mathrm{Km}_{wc}$ and the identification key $\mathrm{Kid} = \mathrm{Km} \oplus \mathrm{CV}$. The vehicle unit authenticates itself by the motion sensor using Kid. A random Triple-DES session key Ks for the operational communication between the VU and the motion sensor is then established. In the last step, the motion sensor authenticates itself by the vehicle unit using the pairing data, the pairing key Kp and Ks. If the mutual authentication was successful, the operational communication continues with the session key Ks. For the concrete details, we refer the reader to [3].

Operation

After having been paired, the motion sensor and the vehicle unit can communicate for operational purposes. Three different kinds of data can be transmitted from the motion sensor to the VU in response to an appropriate instruction:

1. real-time movement pulses,
2. secured value of the pulse counter and
3. secured content of the motion sensor's files being read by the VU.

The real-time movement pulses are continuously transmitted in plain to the VU (when the vehicle is moving) without any security attribute. The frequency of these pulses depends on the instantaneous velocity of the vehicle and the concrete construction of the gearbox, where the motion sensor is mounted (the correct conversion coefficients are determined and stored in the VU during its calibration by an approved workshop).

The motion sensor as well as the connected vehicle unit each runs a pulse counter. Their values are synchronised immediately after the pairing procedure. The VU periodically sends an authentication token to the motion sensor

(at most once per hour), which answers with the random part of the authentication token and the current value of the pulse counter encrypted by the session key Ks. The VU compares

1. the received parts of the authentication token with the respective value having been sent and
2. the current value of its own pulse counter with the value received from the motion sensor.

If these comparisons are successful, the VU "knows" that the motion sensor connected is a correct one and no real-time pulse has been lost or inserted.

In this way the recording equipment assures the correctness of the mean value of the movement data between two subsequent requests for the secured value of the pulse counter. In other words, the trusted input from the motion sensor is supplied as the secured counter value.

Some data (like error messages, serial number, pairing data, etc.) permanently stored in the motion sensor are organised into files, which can be read by the vehicle unit connected. After a special request (including among others an authentication token and the file number) the motion sensor sends the content of the requested file encrypted with the session key Ks.

7 Type Approval of the Components

The prescribed European type approval procedure (see [1], Appendix 9) concerns only three components of the tachograph system – the motion sensor, the vehicle unit and the tachograph card – and comprises four steps:

- Security Certification,
- Functional Certification,
- Interoperability Certification, and
- Type Approval Certification.

7.1 Security Certification

Each of the three components should be certified after ITSEC on the assurance level E3 with the claimed strength of security mechanisms "high". It is also possible to perform the security certification according to the Common Criteria (CC), using a special assurance package E3hAP defined in the "Joint Interpretation Library: Security Evaluation and Certification of Digital Tachographs" [2]. This special assurance package is generally commensurate with the CC Evaluation Assurance Level 4 augmented in the first line by vulnerability analysis for a high attack potential.

[1] also defines a mandatory Generic Security Target for each of three components under consideration, where the required security policies are described. The security policies are defined for the operational life phase of the

tachograph components. The security certificate indicates that the certified product meets the security policy defined in the related security target.

The evaluation and certification processes are usually initiated by the product manufacturer. A prerequisite for issuing a security certificate by an accredited certification body is a successful evaluation having been performed by a licensed evaluation facility.

7.2 Functional Certification

The functional certificate is issued by the national type approval authority. This certificate indicates that at least all functional tests specified by the EU legislative for the tachograph system (Appendix 9 of [1]) have been successfully performed. The functional tests are performed by an accredited laboratory and their results delivered to the national type approval authority issuing the functional certificate. The product manufacturer initiates the functional testing. The functional certificate can normally be gained after issuing the security certificate.

7.3 Interoperability Certification

The interoperability testing aims to ensure that the equipment of different manufacturers works together properly. The product manufacturer requests the interoperability certificate. The application should contain among other things the security and functional certificates. The interoperability certificate is issued by a single central laboratory under the authority and responsibility of the European Commission (JRC Laboratory, Ispra, Italy). This laboratory also carries out the interoperability tests. The interoperability certificate indicates that all interoperability tests specified by the EU legislative for the tachograph system (Appendix 9 of [1]) have been successfully carried out.

7.4 Type Approval Certification

Only a product possessing such a certificate is allowed to be installed into a vehicle. Having received all three certificates – security, functional and interoperability – the national type approval authority issues the type approval certificate for the product in question. The product manufacturer gets a copy of this certificate. The second copy is delivered directly to the central laboratory for interoperability testing (JRC), which updates and publishes on its web site (`dtc.jrc.it`) the current list of products which have achieved the type approval certificate.

8 Conceptual Vulnerabilities

8.1 Long Roll-Out Period

[1] requires that the digital tachograph is fitted into new vehicles, but it does not require exchange of the analogue tachograph built into vehicles already in service. Assuming a truck life-time of more than 20 years, there will be a long period of running both types of tachograph systems in parallel.

As already described in [11] procedural bypasses are possible that allow a company to operate both new and old trucks and to establish a regular change of drivers. If a driver is controlled in a truck, old tachograph charts can be removed in case of a control without notice.

It is recommended to outline a definitive end of the analogue tachographs.

8.2 Delivery and Configuration/Personalisation of Recording Equipment and Tachograph Cards

[1] does not regulate delivery and configuration procedures of the tachograph system components. On the other side, there are special requirements of the criteria for security evaluation (ITSEC and CC) on the properties of delivery and configuration procedures, whereby these could be different for each equipment manufacturer and each Member State. In order to gain harmonised delivery procedures within the whole of Europe, it is necessary to have a common understanding for the delivery methods and responsibilities of the parties participated. Delivery procedures and responsibilities can more easily be understood in the context of the concrete life cycles of the technical components of the tachograph system.

Recording Equipment

Figure 4 visualises the aspects of the delivery and configuration of a VU (the life cycle of the motion sensor is almost the same) in the context of its typical life cycle described in Appendix 10 of [1].

Generation of the VU takes place in the following life cycle phases:

- first initialisation (by the VU manufacturer) and
- initialisation and configuration (by an approved workshop).

During the "first initialisation" phase the cryptographic keys will be loaded into the VU (among other items). The "Component Personaliser Service" of the MSA is responsible for the generation and embedding of cryptographic material into the tachograph equipment (see [9]), wherever such a service is placed. The "Component Personaliser Service" acts upon the National Security Policy of the respective Member State issued by the MSA. So, an appropriate generation as well as a secure delivery of these keys to the VU manufacturer will be assured by the MSA Security Policy.

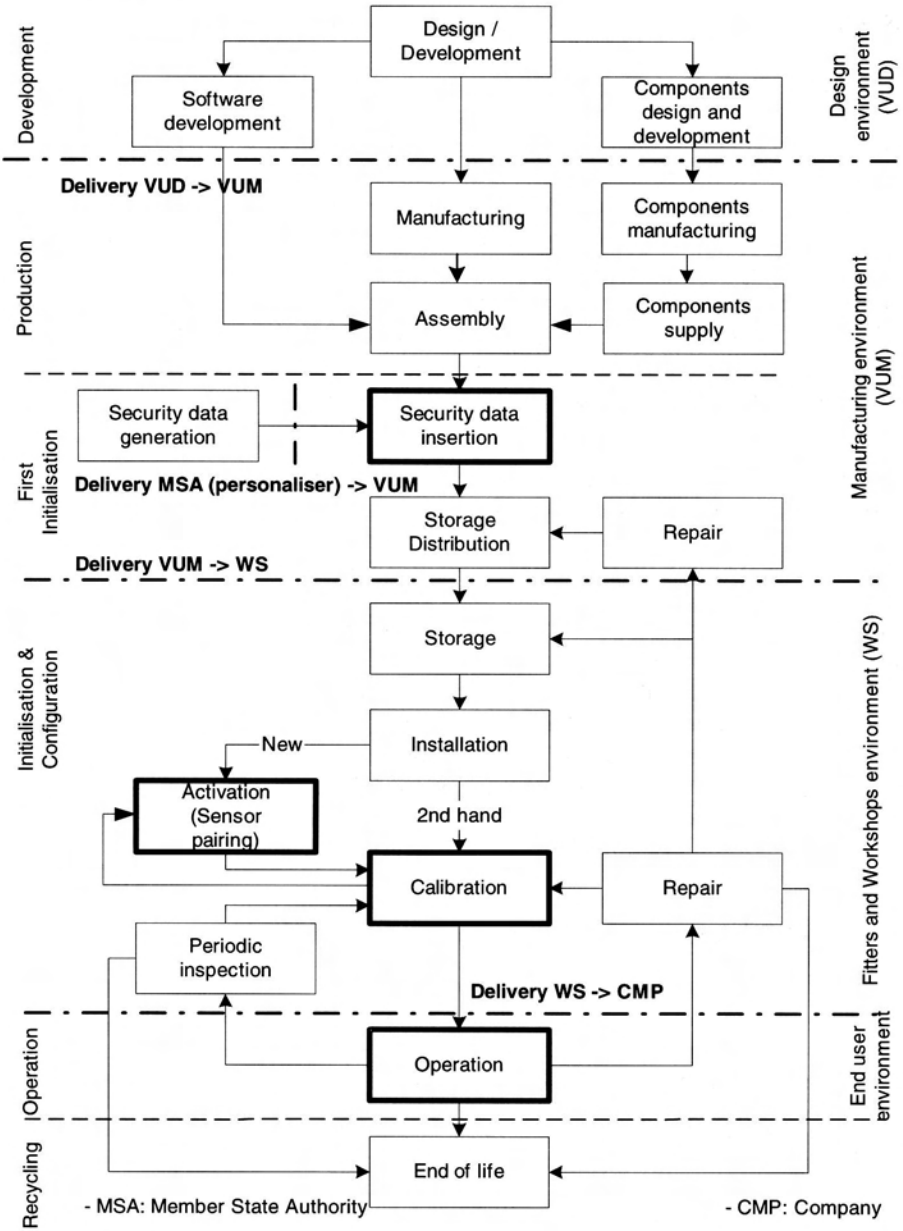

Fig. 4. Vehicle unit life cycle

Configuration of the VU takes place in the phase "initialisation and configuration" by an approved (MSA) workshop. The VU manufacturer should describe the initialisation and configuration procedures supported by the VU

in the User's Manual for the workshop. The technical and organisational environment of the approved workshops should support and provide these procedures. The approved workshops act under surveillance of the MSA.

There are four delivery interfaces (see Fig. 4):

- VU developer → VU manufacturer,
- MSA → VU manufacturer,
- VU manufacturer → approved workshop, and
- approved workshop → company.

Each delivery interface has to be considered in relation to the following questions:

- whether the VU provides any functionality that helps to secure such a delivery interface (this functionality and its usage should then be described in the guidance documents), and
- whether security of the VU depends on the organisational environment during its delivery and what exactly has to be protected by these means. The assumptions about the organisational measures should be described in the guidance documents; compliance with the National Security Policy of the MSA could be helpful.

Tachograph Cards

Figure 5 visualises the aspects of the delivery and configuration of a tachograph card. The phases 1 to 7 correspond to the generic life cycle in [8].

Generation of the tachograph card (TC) takes place in phase 4 "First Initialisation" by and under responsibility of the card manufacturer (CM). At this stage of the card life cycle there is no difference between driver, workshop, company and control cards: the smartcards leave the card manufacturer in the same state.

Configuration of the TC takes place in phases 5 and 6 – Initialisation and Personalisation – by the "Component Personaliser Service" of the MSA, wherever it is placed. The "Component Personaliser Service" acts upon the National Security Policy of the respective Member State issued by the MSA. So, an appropriate generation and loading of card identification, security (among others the key material of high quality) and personalisation data will be assured by the MSA Security Policy. The TC manufacturer should describe the initialisation and personalisation procedures being by the TC in the User's Manual for the MSA Component Personaliser, whose technical and organisational environment will support and provide these procedures. The Component Personaliser acts under surveillance of the MSA.

As one can see in Fig. 5 the smartcards delivered from the card manufacturer to the MSA Component Personaliser do not distinguish between different types of tachograph card. First in the life phase 5 "Initialisation" the card type specific data as Application Identification and Card Certificate will

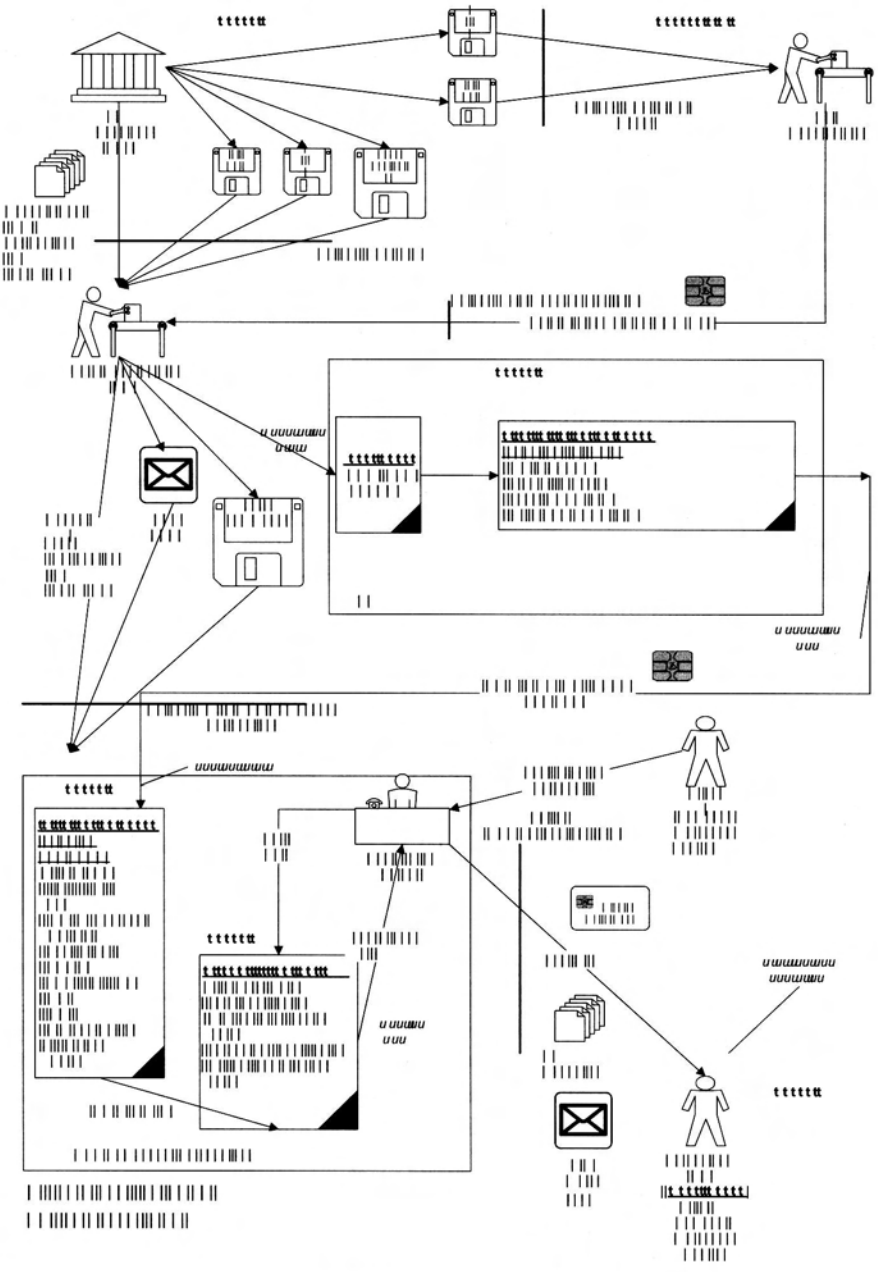

Fig. 5. Tachograph card life cycle

be loaded into the smartcards. After this step the type of tachograph card is unambiguously and irreversible defined: it is either a driver or a company or

a workshop or a control card. Hence, this stage is very appropriate for embedding the ICC into its respective plastic body (so called packaging): white for the driver card, blue for the control, red for the workshop and yellow for the company card.

Generally, the following considerations are helpful: (i) card manufacturer delivers the tachograph cards without any type differences to the MSA, (ii) the MSA first puts the card type specific data into the cards and then (iii) personalisation data concerning the concrete end user of the card (life phase 6 "Personalisation").

There are five delivery interfaces (see Fig. 5):

- developer → chip manufacturer,
- chip manufacturer → card manufacturer,
- developer → card manufacturer,
- card manufacturer → MSA Component Personaliser, and
- MSA Component Personaliser → card holder.

The delivery interfaces have to be considered in the same manner as for the VU (see above).

8.3 Restriction on RSA Key Length

The Public Key Infrastructure which has to be used by the vehicle units and the tachograph cards has already been represented in Section 5.3. The concrete cryptographic algorithm being currently provided for the asymmetric cryptographic system is the RSA algorithm, whereby all RSA keys (whatever the hierarchical level) have a length of modulus 1024 bits (see Appendix 11 of [1]).

In order to gain type approval for a component of the tachograph system this component must obtain security certificate, whereby the strength of security mechanisms must be confirmed to be "high" (see Section 7 and Appendix 10 of [1]). Consequently, also the security mechanisms implementing RSA must be of a high strength, which depends concretely also on the length of modulus.

According to the criteria that may be used for security assessment of the tachograph components (ITSEC and CC), the final decision on the assessment of cryptographic algorithms is made by the security certification body and, eventually, the national competent authority.

It is an established practice to reconsider the cryptographic strength from time to time as new attack techniques are constantly being invented. In order to deal with this fact the responsible national authorities define time restrictions for using cryptographic algorithms as "high-secure" algorithms beforehand. In summary, each Member State has its own guideline for it, which is not made generally public.

In Germany such a guideline is public, and has to be used in the first line in the context of the German Digital Signature Law. Nevertheless, it also

represents a helpful and valid reference for other purposes. The competent national authority is the "Bundesnetzagentur" (Federal Network Agency, `www.bundesnetzagentur.de`), which issues an annual bulletin for the appropriate cryptographic algorithms (the last publication is dated by 2 January 2005).

Concretely, this bulletin of the German authority allows the use of the 1024-bit sized RSA as "high-secure" in the context of the German Digital Signature Law merely until end of 2007 (see Fig. 2).

Table 2. RSA, Length of modulus

		period		
		till end of 2007	till end of 2008	till end of 2009
length of modulus	at least	1024	1280	1536
	recommended	2048	2048	2048

As far as we know the assessments of other authorities lie in a similar range or are even more stringent.

Due to this circumstance the evaluator has to bind his evaluation verdict on the restriction that the assessment of the strength of mechanisms is reconsidered at the latest by end of the period of validity for the current implementation. The product is then reconsidered and eventually recertified.

If at a future time the RSA algorithm with 1024-bit key length cannot be considered as "high-secure", the operators of the tachograph system (the respective MSAs) will face the problem of running the system on equipment (VU and TC) no longer compliant with the requirements of Annex I (B) of [1]. The question of liability in this case is an important one.

8.4 Maintenance of the PKI for the Tachograph System

Proceeding from the issue of length of the RSA modulus touched upon in Section 8.3, the question of maintenance of the PKI arises for the tachograph system.

[1] prescribes a fixed length for the RSA modulus at 1024 bits. Moreover, it does not provide any option for changing the European key pair (EUR.SK, EUR.PK) controlled by the ERCA. The latter plans the life time of this root key pair for a period of 30 years (see [9], section 4.2.6). Of course, ERCA assumes that technological progress over the next 30 years will render its IT systems obsolete. Nevertheless no change procedure for the European key pair has been defined.

According to [1] MSCAs are allowed to perform a regular change of their key pairs (MS_i.SK, MS_i.PK). The European Root Security Policy restricts the use of the MSCA key pair to a period of at most two years starting from

certification by the ERCA (see [9], section 5.3.4). The ERCA will issue a new certificate MS_i.C for each new MSCA key pair. This means that there will be some generations of equipment certificates EQT_j.C having been issued using different MSCA private keys. This does not represent a problem as long as the trustworthiness of the certificate chain can be determined by using the common European public key.

It is the core of the conflict between the prospective necessity to exchange the European key pair against a longer one and the current specification of the tachograph system not providing and not allowing any exchange procedure: neither of a technical nor of a procedural nature.

Also from the logistical point of view, the distribution of a new EUR.PK and of the respective Member State certificates MS_i.C among the single equipment units (already in operation) may be a big challenge for the entire tachograph community. Hence, in order to be prepared for such problems, the tachograph community should already have a modification procedure for the European key pair in place.

8.5 Master Key for the Motion Sensor

A universal master key for the motion sensor is used for the pairing between the digital tachograph and the motion sensor. The key is split (XOR) into two parts. One half is stored in the workshop cards, while the other half is stored in the vehicle unit (see Fig. 3). If this master key is compromised, the security of the overall tachograph system is jeopardised. In detail, the consequences are as follows:

- The observation of the pairing protocol discloses the session key. An additional simulating device can be used in operation that is placed between the vehicle unit and the motion sensor.
- The initiation of the pairing protocol can be invoked without use of a workshop card.
- Cloning of motion sensors is feasible.

There are no precautions taken to replace this master key in the actual key management design.

8.6 PIN Management

The PIN is transferred in clear by the digital tachograph to the workshop card as part of the mutual authentication sequence. Internally, the workshop card verifies the PIN value and returns an "OK" or "KO" message. A "KO" return value results in a failed authentication. After five unsuccessful PIN authentication events, the workshop card is blocked, and cannot be reset to an operational mode.

There are two technical issues. First, the PIN is sent in clear by the tachograph; an interception of the PIN value at the communication line is possible.

Second, the protocol does not include a message authentication for the return value. The return code "OK" can stem from an additional device in between that blocks the "Verify PIN" request.

In Appendix 10 of [1] (functional requirement UIA_302) it is stated that the PIN mechanism is intended "for the vehicle unit to ensure the identity of the card holder, it is not intended to protect workshop card content". This is unusual for smartcard specifications that protect the use of certain functions on human or device authentication.

Typically, workshop cards are used by all employees of a workshop, which results in organisational questions concerning PIN handling. It is probable that the PIN is noted at the workshop card or stored in additional software tools. Further, it might be that the PIN is not entered manually at the keyboard of the digital tachograph, but sent by a standard automotive interface device (e.g. by using the CAN-bus).

Note that the digital tachograph is not a physically secure PIN-entry device. There are no physical requirements to secure the path between the keyboard and the processing unit. Nevertheless, this is a minor issue, formally mended by the organisational measure M.Approved_Workshops (see Section 8.8).

8.7 (Non-)Trustworthy Physical Motion Information

The physical information used to derive the motion data is generated outside the motion sensor. If the physical environment of the motion sensor can be manipulated, the motion information gained can depend on this manipulation. This weak point has been outlined by Ross Anderson [12].

The non-technical requirement M.Mechanical_Interface, which is part of the security target of the motion sensor in Appendix 10 of [1], says "*Means of detecting physical tampering with the mechanical interface must be provided (e.g. seals)*". The environmental conditions within a gearbox include heat and dust. It remains doubtful whether typical measures for tamper evidence such as security seals can be used in this hostile environment reliably.

8.8 (Non-)Trustworthy Workshops

Ross Anderson outlined [12] that about 70% of the employees of workshops have been in conflict with the law in the United Kingdom. The non-technical requirement M.Approved_Workshops, which is part of the security targets for both the motion sensor and the digital tachograph in Appendix 10 of [1] says "*Installation, calibration and repair of recording equipment must be carried by trusted and approved fitters or workshops*". There are serious doubts whether this personal assumption holds in reality.

The non-technical requirement M.Faithful_Calibration ("*Approved fitters and workshops must enter proper vehicle parameters in recording equipment*

during calibration."), which is part of the security target of the digital tachograph, causes similar doubts.

The operator of the tachograph system (the MSA, e.g. the Ministry of Transport) will audit and license the approved workshops. In this way the operator can control the workshops.

8.9 (Non-)Trustworthy Drivers

The security target for the digital tachograph requires that "*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, ...)*" (M.Faithful_Drivers).

Drivers are controlled by the tachograph system. Naturally, supervised persons try to find ways to circumvent an external control.

Currently the actual working hours needed can exceed the limits of the EU Directive; conflicts with the company are probable when acting in accordance with the rules of the digital tachograph system.

Another issue might be the financial interest for the driver to enter a false activity (e.g. working time instead of rest time). The monitoring of speeding events is once more an issue that incite manipulation by the driver.

Easier problems may arise because of the handling of the extensive functions of digital tachographs.

8.10 Frequency of Controls

The procedural requirement M.Controls says "*Law enforcement controls must be performed regularly and randomly, and must include security audits*". Due to today's heavy truck traffic (especially in transit) an adequate frequency of controls can probably not be guaranteed.

The future will show how many obviously "out of function" digital tachograph systems will be notified at controls. Note that the company has 15 days before the tachograph has to be exchanged/repaired.

8.11 Training of Control Personnel

The control authority is the only instance that is actually assumed to play by the rules of the tachograph system. It is up to the control personnel to prove any indication of manipulation of the digital tachograph system which would allow the truck to be taken for detailed analysis. Note that the physical security requirement "tamper evidence" requires that trained controllers examine the digital tachograph and the motion sensor in detail (especially, from all sides).

By checking the tachograph's data memory it is assumed that irregularities of other drivers can be detected. It has to be clarified how this is going to be handled.

Miscalibration of the vehicle unit leads to deviations between the motion data measured and the real motion data. The basic parameters for the vehicle characteristics are named "*w, k, l, tyre size, speed limiting device setting, current UTC time, current odometer value*". w and k are constants that give the number of impulses per kilometre, l is the effective circumference of the wheel tyres in millimetre. These parameters are also noted on an installation plaque that is placed in or near the tachograph. Nevertheless, if the workshop does not act by the rules, it may become probably difficult for the control personnel to check the correctness of these vehicle characteristics.

8.12 Controlled Data: Download Data and Paper Printouts

The easiest way for the control personnel is to download the data of the digital tachograph and of the tachograph card of the driver to a laptop. In this way, the authenticity of the downloaded data is guaranteed. Provided that appropriate software is used, an automatic check of irregularities can be carried out, which simplifies the control efforts.

An alternative method is that the control personnel checks the paper printouts.

As printouts can be faked, if the original paper is used there is no assurance that existing printouts were originally generated by a digital tachograph. If the paper printouts were not generated by the digital tachograph of the controlled vehicle, serious doubts remain if the data files of the tachograph card are not checked. Note that the control personnel can produce printouts from the vehicle unit also during a control.

Another disadvantage of paper printouts is the fact that the check for irregularities has to be performed manually, which is a difficult and time-consuming task.

8.13 Physical Security of the Recording Equipment

The Generic Security Targets in Annex 10 of [1] require that the motion sensor and the vehicle unit should fulfil the following requirements being reprinted below:

"*If the motion sensor is designed so that it can be opened, the motion sensor shall detect any case opening, even without external power supply for a minimum of six months. In such a case, the SEF shall generate an audit record of the event (It is acceptable that the audit record is generated and stored after power supply reconnection).*
If the motion sensor is designed so that it cannot be opened, it shall be designed such that physical tampering attempts can be easily detected (e.g. through visual inspection)." (RLB_106)

"*If the VU is designed so that it can be opened, the VU shall detect any case opening, except in calibration mode, even without external power supply for a minimum of six months. In such a case, the SEF shall generate an audit record (It is acceptable that the audit record is generated and stored after power supply reconnection).*
If the VU is designed so that it cannot be opened, it shall be designed such that physical tampering attempts can be easily detected (e.g. through visual inspection)." (RLB_206)

The second implementation choice ("case cannot be opened") calls for tamper-evident measures. The first choice ("case can be opened") is unusual for requirements on the physical security of cryptographic modules. Especially, after the first case opening, it has to be assumed that the motion sensor or VU is no longer trustworthy, as its internals may be modified. Moreover, it is important to add that the workshops are allowed to open the case in calibration mode for maintenance.

Note that tamper evidence calls for a frequent and random control of the vehicle (see Section 8.10) as well as for a careful inspection (see Section 8.11).

9 Conclusion

In this contribution we reviewed the digital tachograph system and addressed some conceptual vulnerabilities. Further directions for development are suggested.

References

1. Commission Regulation (EC) No 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress. Council Regulation (EEC) No 3821/85 on recording equipment in road transport, Annex 1 B, Requirements for Construction, Testing, Installation and Inspection
2. Joint Interpretation Library (JIL): Security Evaluation and Certification of Digital Tachographs, JIL Interpretation of the Security Certification according to Commission Regulation (EC) 1360/2002, Annex 1B, Version 1.12, June 2003
3. ISO 16844-3, Road Vehicles – Tachograph Systems – Part 3: Motion Sensor Interface, 2004-11-01
4. Information Technology Security Evaluation Criteria (ITSEC), June 1991
5. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Part 2: Security functional requirements, Part 3: Security assurance requirements, January 2004, Version 2.2
6. BSI-PP-0002: Smartcard IC Platform Protection Profile, 1.0, available at `www.bsi.bund.de/cc/pplist/ssvgpp01.pdf`
7. PP/9806: Smartcard Integrated Circuit Protection Profile v2.0, available at `www.ssi.gouv.fr/site_documents/PP/PP9806.pdf`

8. PP9911: Common Criteria for IT Security Evaluation, Protection Profile: Smart card integrated circuit with embedded software, Version 2.0, EUROSMART, June 1999 – Registered by the French Certification Body under the reference PP/9911
9. Digital Tachograph System, European Root Policy, Version 2.0, Adminstrative Agreement 17398-00-12 (DG-TREN), European Commission
10. Ross J. Anderson, *On the Security of Digital Tachographs.* In: Lecture Notes in Computer Science, Vol. 1485, pp. 111
11. Ross J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley & Sons, Inc., 2001
12. Ross J. Anderson, Invited Talk at ESCAR 2003