TRANSPORT
2008
23(1): 82–87

EXCHANGE OF EXPERIENCE

SOME PROBLEMS OF DATA SECURITY OF DIGITAL TACHOGRAPH SYSTEM

Gabriel Nowacki, Izabella Mitraszewska, Andrzej Wojcechowski, Tomasz Kamiński

Motor Transport Institute, Jagiellońska 80, 03–301 Warsaw, Poland
E-mail: gabriel.nowacki@its.waw.pl

Received 15 April 2007; accepted 20 November 2007

Abstract. The paper refers to some introduction problems of Digital Tachograph System (DTS) in EEA. It affects 25 states of the European Union and EFTA (Island, Liechtenstein, Norway) and Switzerland. The legislation principles and structure of DTS in the EU are characterized, especially Polish elements. The current state of DTS introduction in the EU Member States was also noted. Some problems of data security concern TACHONET system that ensures reliable and secure exchange of data between Member States issuing tachograph cards. The digital tachograph security principles (ITSEC) of the motion sensor, the vehicle unit and the smart cards were taken into consideration.

Keywords: digital tachograph, security system, transport.

1. Introduction

Analogue tachograph is an instrument which records on paper record sheets (paper discs) driving time, period of work, other periods of availability, breaks of work and daily rest periods, as well as vehicle speed and distance of the journey. Used on a daily basis it creates a continuous permanent record of both the driver's activity and vehicle's use.

Analogue tachograph was used in the United States in 1939, but it was implemented in German legislation in 1952 for heavy goods vehicles and in 1953 for buses.

Over this time the tachograph has evolved. In the early days we had mechanical tachographs, which progressed to the early electronic units, but these were subject to interfering by unscrupulous users.

After 30 years in use, it has been found that the analogue recording equipment is technologically outdated, not economically effective and makes it possible to falsify and manipulate the data recorded. The analogue tachographs no longer satisfy the purpose they were introduced for, which means efficient control of the driver's compliance with the so-called social regulations, and consequently - do not serve for the improvement of the road traffic safety.

Supported by the road transport industry and social partners, the European Commission (EC) decided to implement the most technologically advanced device that effectively controls drivers and enterprises performing the road transport activity, namely Digital tachograph (DT). All parties are of the opinion that introduction of the DT will bring a major advantage to the road safety by ensuring that professional drivers keep to their driving and rest times.

A digital tachograph includes processing unit, data memory, real time clock, two smart card interface devices (driver and co-driver), printer, display, visual warning, calibration/downloading connector, and facilities for entering user's inputs.

The biggest difference between the current, analogue tachograph and the digital tachograph will be the use of a smart card instead of the record sheets (often called charts, discs, and tachos) used in analogue tachographs. There are 4 cards (collectively known as Tachograph Cards) that are used by the digital tachograph system:

- driver card – used by drivers to allow the recording of drivers' hours;
- company card - for use by the operator to protect and download the data;
- workshop card - available only to approved calibration centres;
- control card - available only to the Police, Road Transport Inspection personnel for carrying out the law enforcement activities.

ISSN 1648-4142 print / ISSN 1648-3480 online
www.transport.vgtu.lt

Before allowing to use, a digital tachograph, as well as electronic cards must have a type approval which is based on:

- a security certification, performed by an ITSEC authority;
- a functional certification performed by a Member State authority;
- an interoperability certification performed by the competent body certifying that the digital tachograph is fully interoperable with the necessary tachograph card.

At present, in Europe, three companies producing digital tachographs received type homologation certifications, consistent with the standards of the European Union:

- Actia Smartach digital tachograph;
- Siemens – DTCO 1381 digital tachograph;
- Stoneridge – SE 5000 digital tachograph.

2. Structure of digital tachograph system in EEA

The conception of using digital technology in road transport arose in Council Regulation EEC No. 3820 (1985) and Council Regulation EEC No. 3821 (1985). Next, on the community level, the regulations containing technical details and propositions of organizational-legal solutions have been evaluated.

Council Regulation EEC No. 2135/98 (1998) is a framework laying down the general legal provisions for introducing the new digital tachograph, the Council authorized a Committee to prepare the detailed technical specifications. This work was finalized on 13 June 2002 and the Annex IB was published in the Official Journal of the European Union on 5 August (2002).

Council Regulation EC No. 561/2006 (2006) applies to the carriage by road: of goods where the maximum permissible weight of the vehicle, including any trailer, or semi-trailer, exceeds 3,5 tones, or of passengers by vehicles which are constructed or permanently adapted for carrying more than nine persons including the driver, and are intended for that purpose. Also see Directive 2006/22/EC (2006).

From 2010 (16 June) the implementation of DTS shall concern the signatories of AETR Agreement (1976), countries which belong to the European Economic Area.

On the basis of regulation of the Council of Europe 2135/98 a concept of all-European Digital Tachograph System has developed as a modern way to increase effectiveness of control of driving time and rest of lorry and bus drivers in order to improve road traffic safety and working conditions. The means to accomplish this task is a replacement of the previous system based on recording charts by digital recording devices. These devices require from drivers and amongst the other control organs, authentication by means of electronic cards (driver's card, workshop's card, company's card and control card).

The elements responsible for introduction of DTS amongst the others are:

- the European Commission (DG JRC – for interoperability test, DG TREN for telematics system – TACHONET and General European Certifying Authority);
- government administration of particular Member States (ministries equivalent of transport, authorized entities);
- subjects, institutions involved in DTS, producers of tachographs and cards.

The Republic of Poland joined the European Union on the 1st May 2004 and that made it obligatory to implement Digital Tachograph System; more so, it is bound by the whole previous legal output of the European Union („acquis communataire"). On 29 July 2005 the Parliament of the Republic of Poland passed the Act on Digital Tachograph System (2004 and 2005). The institution responsible for the implementation of DTS in Poland is the Ministry of Transport. The Polish Security Printing Works (Polska Wytwórnia Papierów Wartościowych), according to the Act of the Digital Tachograph System, has been appointed the Card Issuing Authority, the Certification and Personalization Centre. The Central Office of Measures (Główny Urząd Miar) is responsible for issuing type approval certifications, permits for running workshops, authorising workshop's technicians to perform activities connected with installation, activation, calibration and repairing of DT.

The Policy of the Republic of Poland concerning Digital Tachograph System was approved on 8 February 2006 by the European Root Certification Authority. The document concerning the national security policy within the scope of DTS was registered by the Joint Research Center (JRC) under the number D3275.

Currently, three Member States of EU implemented Digital Tachograph System (Germany, France, Sweden), 13 states are in the final phase, 5 – in the an advanced phase (Czech Republic, Denmark, Finland), 5 states – in the medium advanced phase (Island, Liechtenstein, Switzerland), 3 states are in the initial phase (Cyprus, Greece, Malta). The 3 member states have not connected to TACHONET, issued digital tachograph cards, and approved workshops.

3. Data security in TACHONET

TACHONET is Telematics Network for the Exchange of Information Concerning the Issuing of Tachograph Cards. The cohesion of data interchanging ensures XML metalanguage, which the European Union considers as a standard for the European public administration. A key element of the new Regulation is to ensure that a driver does only hold one tachograph card. To overcome this major issue between MS, it has been decided to create a network interconnecting all the MS national administrations (in charge of issuing tachograph cards to their respective truck drivers) aiming at:

- facilitating the data exchange between those latter ones;
- guaranteeing the uniqueness of the driver card;
- ensuring that the card is valid, for instance, during a road check.

Thanks to TACHONET system, the national authority and administration will be able to control driver's

work, interchange information concerning electronic cards, at the same time lowering the number of road accidents. The system operation is based on the central information interchange centre between the governmental administrations of the European Union states, which are responsible for supervision in the scope of installation and service of tachographs, cards' issuing and obeying driver's stops and rest during driving (Fig. 1).

TACHONET is managed by the Department of Transport and Energy of the European Union. The users of Digital Tachograph System can be divided into two types: active- workers of the body issuing cards and officers of control service who can read and modify data from cards, and passive- drivers, traders and workers of the workshops operating tachographs, who have special rights to read the data from cards.

The TACHONET system has been developed with the main purpose to combat the fraud attempts on the part of the drivers. TACHONET Network:

- Ensures a reliable and secure exchange of data between MS issuing the tachograph cards. For restricting access to this sensitive information and providing the confidentiality and data integrity, the following horizontal services were chosen, supplied by IDABC (DG ENTR):
  - the use of TESTA II network (private network of the EC, not open to the Internet);
  - PKI service required for data encryption and integrity.
- Imposes a set of limited constraints on the legal systems processing and handling the driver cards in the MS.
- Uses standard network infrastructure and tools available on the market.
- TACHONET is a centralized architecture but not a centralized database. It is a single point of contact for the MS national administrations and acts as a relay in the exchanges of information.

Four business processes have been developed in TACHONET, namely:

1. First Issue Process: Required for checking whether an applicant driver does not already hold a tachograph card in another MS via TACHONET.
2. Declare Card Status Modification: Any modification of the card such as: stolen, lost, defective, exchanged or suspended must be transmitted to the MS having issued the card via TACHONET.
3. Check Card Status: The process of getting information about the status of the driver's card via TACHONET applicable, for instance, during a road check by the enforcers.
4. Issued Card Information for Driving License: After issuing a card to a given driver, MS CIA must inform another country having issued the driving license via TACHONET that a card has been issued using the corresponding driving license number.

Thanks to TACHONET system, the national authority and administration will be able to control drivers' work, interchange information concerning electronic cards, at the same time lowering the number of road accidents. The system operation is based on the central information interchange centre between the governmental administrations of the European Union states, which are responsible for supervision of installation and service of tachographs, cards' issuing and obeying driver's stops and rest during driving.

4. Data security of tachograph unit, cards and motion sensor

The digital tachograph (VU) is intended to be installed in road transport vehicles. Its purpose is to record, store,

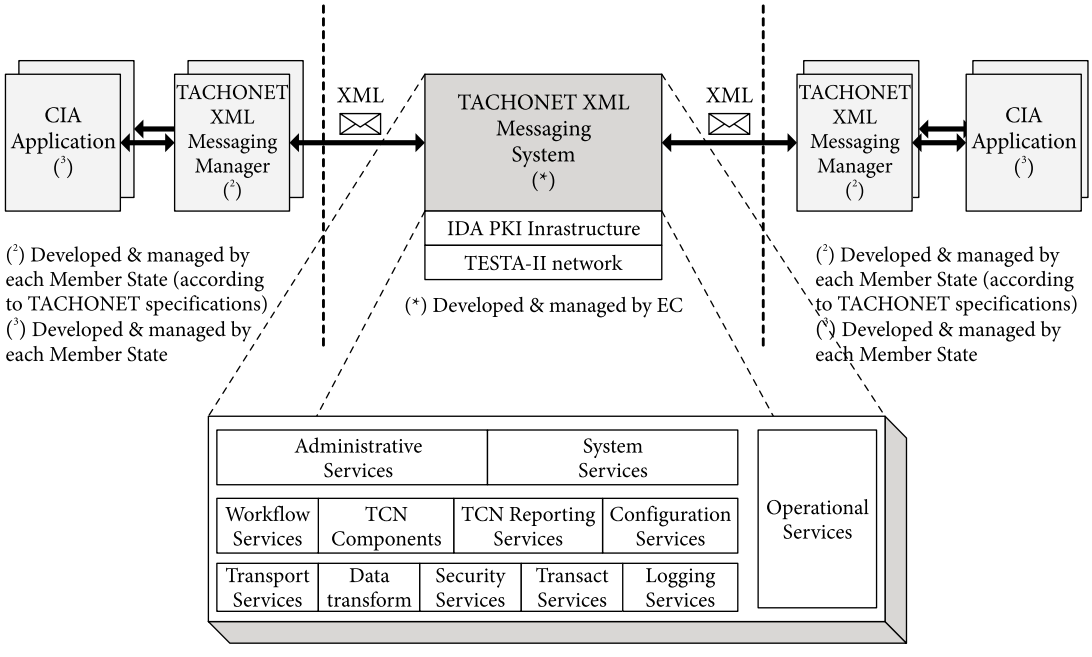

Fig. 1. TACHONET structure

display, print and output data related to driver activities. It is connected to a motion sensor; it exchanges vehicle's motion data with. Users identify themselves to the VU using tachograph cards. The VU records and stores user activities data in its data memory, it also records user activities data in tachograph cards. The VU outputs data to a display, printer and external devices. The vehicle unit's operational environment while installed in a vehicle is shown in Fig. 2.

The digital tachograph system security principles have been named as ITSEC (Information Technology Security Evaluation Criteria). Research in the scope of information technology security (ITSEC – Information Technology Security Evaluation Criteria) in the European Union can be conducted by: The Federal Bureau for Information Technology Systems Security (BSI – Bundesamt für Sicherheit in der Informationstechnik) in Germany, The Central Management of Systems and Information Technology Network Security (DCSSI – Direction Centrale de la Sécurité des Systemes d'Information) in France, CESG – Computer Electronics Security Group in Great Britain, Netherlands National Comsec Agency in Netherlands.

The DTS security aims at protecting the data memory in such a way as to prevent unauthorized access to and manipulation of the data and detecting any such attempts, protecting the integrity and authenticity of data exchanged between the motion sensor and the vehicle unit, protecting the integrity and authenticity of data exchanged between the recording equipment and the tachograph cards, and verifying the integrity and authenticity of data downloaded.

The security targets of digital tachograph components (motion sensor, vehicle unit - VU and tachograph smart cards), approved by laboratory in order to provide an independent view on their suitability, completeness and appropriateness for the ITSEC E3 evaluation. The VU general characteristics, functions and mode of operations are shown in Fig. 3.

The component manufacturers will define most of the security mechanisms needed to fulfil these requirements. Some security mechanisms, though, need 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.

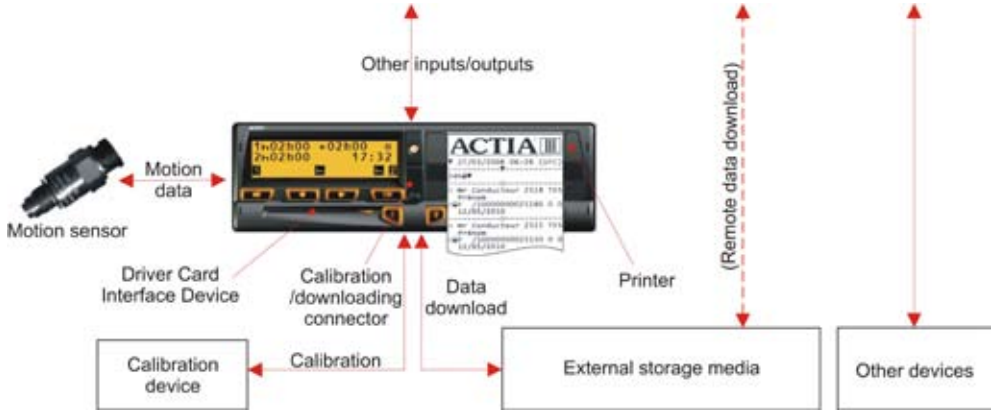

Fig. 2. VU operational environment

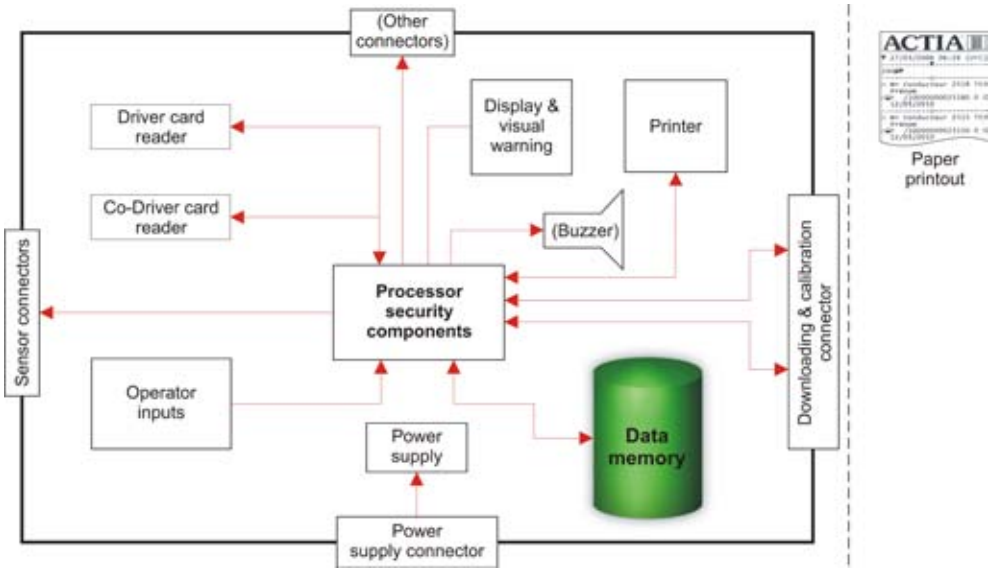

Fig. 3. Typical VU options

Security mechanisms are closely related to security elements (e.g. cryptographic keys), distribution methods and both need to be defined together. Therefore, this document describes the recommended 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.

Cryptographic information technology provides security mechanisms able to fulfil authentication and data integrity requirements. The authentication requirement implies that any element of the system (VU, card) must be able to prove its belonging to the system and 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 organization) has been able to distribute. Any symmetrical cryptographic system makes an 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).

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

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

- European level;
- Member State level;
- Equipment level.

At equipment level, one pair of keys (EQT.SK and EQT.PK) shall be generated and inserted in each equipment. Equipment public-keys shall be certified by a Member State certification authority. These tasks may be handled by equipment manufacturers, equipment personalizers or Member State authorities. This pair of keys is used for authentication, digital signature and encipherement services.

Private keys confidentiality shall be maintained during generation, transport (if any) and storage. For the purpose of equipment testing (including interoperability tests) the European certification authority shall generate a different single European test pair of keys and at least two Member State test pairs of keys – the public keys which shall be certified with the European private test key. Manufacturers shall insert test keys certified by one of these Member State test keys in equipment undergoing type approval tests.

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.

5. Conclusions

The Implementation of Digital Tachograph System for the Republic of Poland, as well as for many other Member Sates of the EU, constitutes an undertaking which is complex and difficult for realization. It requires many different actions coordinated not only on the state but also on the international level. This will prolong and make the process of the system implementation more difficult, but due to its global range it will bring measurable benefits.

The Implementation of DTS will enhance low enforcement in relation to drivers and road transport traders, which will largely contribute to improvement of traffic safety, but at the same time, can rationalize functioning of transport firms. One of the main roles in mentioned scope is played by TACHONET that minimizes the possibility of manipulating the data concerning the driver's work in the whole European Union and effectively maximizes his work (among the others, it ensures the equal rights of drivers, carriers and transportation firms, increases the road traffic safety by obeying stops and rest, avoiding control, stops due to speeding).

The digital tachograph security principles (ITSEC) refer generally to motion sensor, the vehicle unit and the smart cards. The VU shall authenticate the motion sensor it is connected to: at motion sensor connection, at each calibration of the recording equipment, at power supply recovery. Vehicle units and tachograph cards shall use a classical RSA public-key cryptographic system to provide the following security mechanisms:

- authentication between vehicle units and cards;
- transport of Triple-DES session keys between vehicle units and tachograph cards;
- digital signature of data downloaded from vehicle units or tachograph cards to external media.

References

AETR – European agreement concerning the work of crews of vehicles engaged in the international road transport, Geneva, 1 July 1970 (approved on 5 January 1976).

Council Regulation (EEC) No. 3820/85 as of 20 December 1985 on the harmonization of certain social legislation relating to road transport (also called "Drivers' Hours' Rules"), *The Official Journal of the European Union*, L 370, 31 December 1985.

Council Regulation (EEC) No. 3821/85 as of 20 December 1985 on recording equipment in road transport (also called "Analogue Tachograph"), *The Official Journal of the European Union*, L 370, 31 December 1985.

Council Regulation (EC) No. 2135/98 as of 24 September 1998 amending Regulation (EEC) No. 3821/85 on recording equipment in road transport and Directive 88/599/EEC concerning the application of Regulations (EEC) No. 3820/84 and (EEC) No. 3821/85 (also called 'Digital Tachograph'), *The Official Journal of the European Union*, L 274, 9 October 1998.

Council Regulation (EC) No. 1360/2002 as of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No. 3821/85 on recording equipment in road transport (Text with EEA relevance) (also called "Technical Specifications of Digital Tachograph"), *The Official Journal of the European Union*, L 207, 5 August 2002.

Council Regulation (EC) No. 561/2006 as of 15 March 2006 on the harmonization of certain social legislation relating to road transport and amending Council Regulations (EEC) No. 3821/85 and (EC) No. 2135/98 and repealing Council Regulation (EEC) No. 3820/85, *The Official Journal of the European Union*, 11 April 2006.

Directive 2006/22/EC of the European Parliament and of the Council of 15 March 2006 on minimum conditions for the implementation of Council Regulations (EEC) No. 3820/85 and (EEC) No. 3821/85 concerning social legislation relating to road transport activities and repealing Council Directive 88/599/EEC.

The Act of 29 July 2005 on digital tachograph system. 2005. *The Official Journal of Poland*, 180, pos. 1494.

The Act of 16 April 2004 on driver work time. 2004. *The Official Journal of Poland*, 92, pos. 879.