European Commission

JRC SCIENTIFIC AND POLICY REPORTS

Cryptographic security mechanisms of the next generation digital tachograph system and future considerations

Mehmet Colak, James Bishop, Jean Pierre Nordvik, Vincent Mahieu, Jan Loeschner

2012

Report EUR 25663 EN

Joint Research Centre

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Address: Joint Research Centre, Via Enrico Fermi 2749, TP361, 21027 Ispra (VA), Italy
E-mail: Vincent.mahieu@jrc.ec.europa.eu
Tel.: +39 0332 78 9305
Fax: +39 0332 78 5145

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC77933

EUR 25663 EN

ISBN 978-92-79-27990-4 (pdf)
ISBN 978-92-79-27991-1 (print)

ISSN 1831-9424 (online)
ISSN 1018-5593 (print)

doi:10.2788/74093

Luxembourg: Publications Office of the European Union, 2012

Printed in Italy

Table of contents

List of Figures

List of Tables

List of Acronyms

AETR	European Agreement Concerning the Work of Crews of Vehicles Engaged in International Road Transport
DT	Digital Tachograph
DTS	Digital Tachograph System
ERCA	European Root Certification Authority
ETSI	European Telecommunications Standards Institute
ISO	International Standards Organization
MS	Motion Sensor
MSA	Member State Authority
MSCA	Member State Certification Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructures
VU	Vehicle Unit
CP	Component Personaliser
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSP	Certification Services Provider
EA	European Authority
KCR	Key Certification Request
KDR	Key Distribution Request (for motion sensor master keys)
KDM	Key Distribution Message (encrypted motion sensor master key)
Km	Motion sensor master key
KmV_U	Motion sensor master key inserted in vehicle unit
KmW_C	Motion sensor master key inserted in workshop card
PK	RSA public key
RSA	Rivest, Shamir, Adleman (asymmetric encryption scheme)
SK	RSA secret key
ITS	Intelligent Transport Sytems
ITS-S	ITS Station

1 Introduction

This technical report is going to cover digital tachograph (DT) security assessment and definition of an adequate level of security of the digital tachograph for the years to come. DT security assessment and definition of an adequate level of security of the digital tachograph for the years to come is investigated. The possible convergence of driving licenses with DT cards is introduced. Eventual expansion of digital tachograph to ITS and possibility of ERCA to be a trust anchor for ITS is analysed.

In this document, firstly the current system components of the digital tachograph system and their functionality along with provided security mechanisms are summarised, secondly the vulnerabilities of the current cryptographic mechanisms and possible solutions are discussed, thirdly the possible convergence of driving licenses with DT cards is introduced, finally possible expansion of digital tachograph to ITS along with the idea of using Mobile Signature in DTS is introduced.

This report partially answers the Deliverable of Objective 2.2 of the CIDIPRINT 2011 Action Plan 2011 and adds a chapter for the investigation of ITS for the possible merge of DT to ITS in the future.

The deliverable reads as follows:
Risk assessment of the digital tachograph system: threads, occurrence and intensity evaluation and remedies. Focus on user identity, possible convergence of driving licences with DT cards, frauds, privacy, sensitive data access (competition, dangerous or valuable goods, location), DT security assessment and definition of an adequate level of security of the digital tachograph for the years to come.

2 Brief description of the digital tachograph system

This section describes the basic structure of the recording equipment and its behaviour in normal operation. This section contains elements from the Vulnerability report [DT VULNERABILITIES]

2.1 The recording equipment

The recording equipment consists of two main elements (see **Figure 1**):

- a Motion Sensor (MS) and
- a Vehicle Unit (VU)

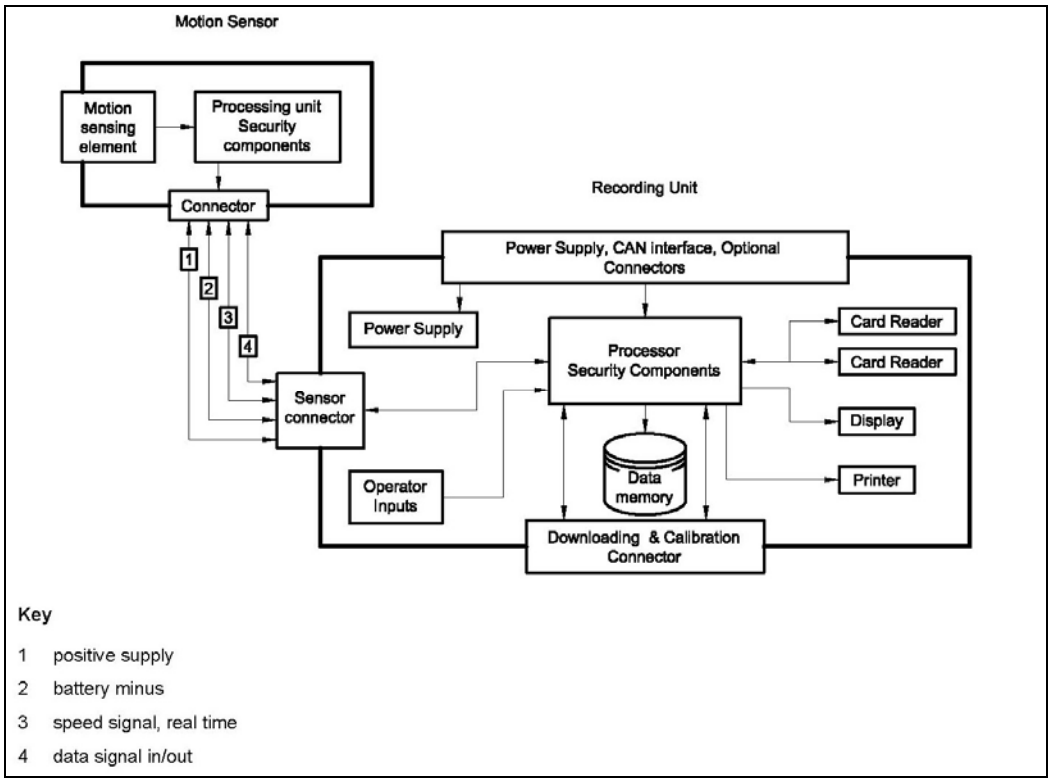


Figure 1 - Schemata of typical recording equipment (extracted from ISO-16844-3)

2.1.1 The Motion Sensor

As stated in the legislation [DT REGULATION], the purpose of a MS is to provide the VU with secured motion data representative of vehicle's speed and distance travelled. A MS is mechanically interfaced to a moving part of the vehicle, which movement can be representative of vehicle's speed or distance travelled.

In practice a MS is usually screwed into the vehicle's gear box. Movement detection is provided in most cases by a Hall-effect position sensor located in the MS. The Hall-effect position sensor is a non-contact device that detects the small electromagnetic variations created by the movement of a toothed ring inside the gear box or inside the sensor itself. The Hall-effect position sensor converts these variations into electrical signals. These signals are processed by a small electronic board inside the MS. Real time speed pulses are sent via the cable to the VU. In addition, a secured serial data communication signal on the same cable allows for mutual authentication and identification between MS and VU, and secured transmission of data. Encryption is carried out by a dedicated crypto-chip soldered on the electronic board.

Figure 2 - Motion Sensor [SECURITY ATTACKS TO DT]

Every MS is identified by a unique MS identification data which is stored once and for all in the MS by the MS manufacturer.

A MS must be marked with all or if not possible part of its MS identification data.

If a MS is designed so that it cannot be opened, it shall be designed such that physical tampering can be easily detected (e.g. by visual inspection). This is accomplished by sealing the MS in the Workshop after pairing with the VU.

Power to a MS is always supplied by the VU via the Cable.

There are currently two approved manufacturers of the so-called encrypted MS: Actia and Siemens VDO.

2.1.2 The Vehicle Unit

The role of a VU is to record, store, display, print and output data related to driver activities. It is connected to MS with which it exchanges vehicle's motion data.

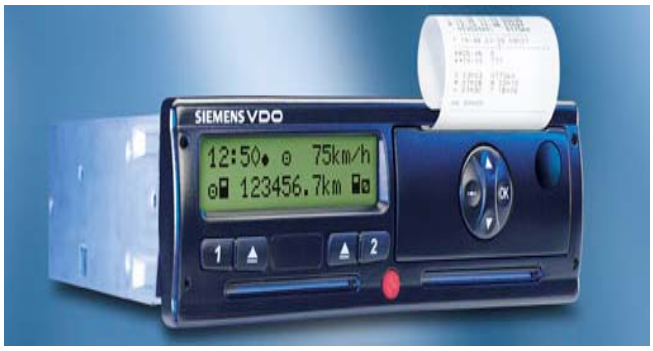


Figure 3 - Vehicle Unit [SECURITY ATTACKS TO DT]

A 4-wire cable connects physically without interruption the MS with the VU. It provides wires for the transmission of encrypted data between VU and MS, the supply of energy to the MS, and the transmission of real time speed pulses to the VU.

The cable, the connector of the MS, the electrical characteristics of the data exchanged between the MS and the VU and the communication protocol between MS and VU are specified in the standard ISO 16844-3.

There are four approved manufacturers of VU's:

Actia, Continental, Stoneridge and Efkon.

A Vehicle Unit (VU) records the following data [DT REGULATION]:

2.1.2.1 Equipment Identification Data

Vehicle Unit Identification Data (name and address of the manufacturer, serial part and approval numbers, etc.)
Motion Sensor Identification Number (name and address of the manufacturer, serial part and approval numbers, etc.)
Security Elements (European and Equipment Public Keys, Member State and Equipment Certificates)

2.1.2.2 Driver Card Insertion and Withdrawal Data

At each insertion and withdrawal cycle of a driver, or workshop card, in the equipment, the cardholder's first and last names, his/her card number, insertion and withdrawal date & time, vehicle odometer at card insertion and withdrawal, etc.

2.1.2.3 Driver Activity Data

All driving activities (even without the card inserted), availability, work, rest/break, the driving status (single or crew), etc.

2.1.2.4 Location

Where Daily Work Periods start and/or end
Driver Card Number
Date & Time of Entry
Type of Entry (beginning or end)
Country & Region (when applicable)
Vehicle Odometer Value

2.1.2.5 Odometer Data

Odometer data are recorded every calendar day at midnight

2.1.2.6 Detailed Speed Data

Detailed Speed Data over the last 24 hours (second per second)

2.1.2.7 Events and Faults Data

Card Conflicts,
Speed Abuse,
Power Supply Interruption,
Card & Recording Equipment Faults, etc.

2.1.2.8 Calibration Data

Vehicle Parameters (type, size, setting of speed limit)
Date & Time of Five Most Recent Calibrations with workshops' details

2.1.2.9 Time Adjustment Data

Time adjustment data are the largest five time adjustments with Workshops' Details

2.1.2.10 Control Activity Data

Date & Time of Control,
Type of Control,
Control Card Number and Card Issuing Member State.

2.1.2.11 Company Locks Data

Lock-in & Lock-out dates & times,
Company Card Number and Card Issuing Member State,
Company Name & Address.

2.1.2.12 Download Activity Data

Date & Time of Downloading,
Company or Workshop Card Number,
Card Issuing Member State,
Company or Workshop Name.

2.2 Tachograph Cards

Central to the introduction of digital tachograph technology is the provision of smart cards for use by drivers, companies, calibration workshops and enforcement officers.

National authorities are responsible for card issuing:

- general management (issuing, renewal, replacement)
- security: data protection, driver identification, workshop passwords

Figure 4 - Tachograph Cards

2.2.1 Driver Card

The personal driver card:

- is a plastic card similar in size to a credit card, with a microchip in it.
- the card can store all relevant driver data required for EU Drivers Hours regulations including break and rest times (see Figure 5).
- is personalised to the individual driver and valid for 5 years
- can store information for at least 28 days (with few exceptions)

- one card is issued per driver during period of validity (except in the case of a damaged, lost, stolen or faulty card).
- a driver is only authorised to use his/her own personalised card
- if the card is lost a driver is required to report it and to make an application for a replacement card within 7 days of its loss
- a card may be suspended or withdrawn by an enforcement officer if the card has been falsified, if the person using the card is not the legal holder of the card or if the card has been obtained by false declaration or forged documents.

File	File ID	Access conditions		
		Read	Update	Encrypted
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	ALW	NEV	No
├─EF Card_Download	050E	ALW	ALW	No
├─EF Driving_Licence_Info	0521	ALW	NEV	No
├─EF Events_Data	0502	ALW	PRO SM / AUT	No
├─EF Faults_Data	0503	ALW	PRO SM / AUT	No
├─EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
├─EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
├─EF Places	0506	ALW	PRO SM / AUT	No
├─EF Current_Usage	0507	ALW	PRO SM / AUT	No
├─EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
└─EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

Figure 5 - Driver card file structure [DT REGULATION]

The driver card must be made available to law Enforcement Officers on request.

The legislation requires the driver to either download the data and retain it themselves or allow the company to download the data from their driver card and retain for inspection.

2.2.2 Company Card

A company card is valid for 5 years and serves to protect company-related data in the VU. The card allows a company to download the information from the VU in order to carry out checks on drivers' hours (roster, etc.), as required by the legislation and to maintain the required records for examination by Transport Officers. The company card allows a company to lock data recorded in the VU to prevent other operators downloading the data. This is necessary to ensure the protection of personal information of a company and its driver(s), and details of work patterns and times from competitors. This would be important when vehicles are sold or returned to a hire/lease company.

File	File ID	Access conditions		
		Read	Update	Encrypted
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	AUT	NEV	No
└─EF Company_Activity_Data	050D	ALW	PRO SM / AUT	No

Figure 6 - Company card file structure [DT REGULATION]

2.2.3 Workshop Card

A Workshop Card is valid for 1 year.

The workshop card is available only to approved calibration workshops.

Such workshops must be approved by the National Authorities and the workshop fitter must provide proof that he/she has received the necessary qualifications.

If a workshop fitter is employed by more than one workshop, he/she must hold a workshop card for each workshop that he/she is working for.

General Rules:

- The Workshop manager is responsible for the workshop cards at all times.
- The Workshop manager is responsible for the return of cards if/when fitters leave their employment.
- If a card cannot be returned such as lost/stolen/malfunctioning the Workshop foreman is obliged to notify the Road Authority.
- The PIN is personal to a fitter and is posted to him/her personally. This should not be disclosed to any other person.
- The Workshop card can only be used by the person to whom it is issued.

		Access conditions		
File	File ID	Read	Update	Encrypted
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	ALW	NEV	No
├─EF Card_Download	0509	ALW	ALW	No
├─EF Calibration	050A	ALW	PRO SM / AUT	No
├─EF Sensor_Installation_Data	050B	ALW	NEV	Yes
├─EF Events_Data	0502	ALW	PRO SM / AUT	No
├─EF Faults_Data	0503	ALW	PRO SM / AUT	No
├─EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
├─EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
├─EF Places	0506	ALW	PRO SM / AUT	No
├─EF Current_Usage	0507	ALW	PRO SM / AUT	No
├─EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
└─EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

Figure 7 – Workshop card file structure [DT REGULATION]

2.2.4 Control Card

The control card is available only to law Enforcement Authority Officers for carrying out enforcement of digital tachograph legislation.

- A control card enables the mass memory of digital tachographs and driver card data to be accessed.
- Allows printouts of all relevant information to be made at any time.
- A control card has a maximum validity of 5 years, although some users adopted a shorter one (e.g. 2 years).

File	File ID	Access conditions		
		Read	Update	Encrypted
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	AUT	NEV	No
└─EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	No

Figure 8 - Control card file structure [DT REGULATION]

3 AETR

The geographic coverage of the digital tachograph system is extended beyond the EU borders (see Figure 9) as it has become mandatory for the contracting parties to AETR since 2010. The AETR agreement concerns the work of crews of vehicles engaged in international road transport. The agreement covers 49 contracting parties (will soon be 50 countries) including all EU Member States. Its provisions are aligned with the current EU legislation on driving times, breaks and rest periods. In 2006 the AETR agreement was amended in order to introduce the use of the digital tachograph.

European Commission provides root level PKI services to non EU AETR countries according to the Memorandum of Understanding, between The European Commission Services and the United Nations Economic Commission for Europe (UNECE) which was signed on 23/01/2009.

Figure 9 – AETR countries [UNECE]

4 Cryptographic Systems in DTS

This section describes the major characteristics of the cryptographic systems and communication protocols in use in the DTS [ERCA POLICY].

The key and certificate management in the DTS is depicted in Figure 10. Four entities are depicted: the ERCA certification service provider (CSP); an MSCA CSP; and the two types of component personaliser (CP): tachograph card or vehicle unit manufacturing; and motion sensor manufacturing.

The ERCA and MSCA CSPs in Figure 10 create and maintain appropriate secret encryption keys and use them to validate digital tachograph security data, only after verifying that the data to encrypt are complete, correct, and duly authorised.

The card, vehicle unit or motion sensor CPs in Figure 10 insert validated security data into digital tachograph equipment by appropriately secured means.

Abbreviations in Figure 10 are as defined in Annex I(B) Appendix 11 [DT REGULATION], ISO / IEC 16844-3 Motion sensor interface [ISO-16844-3].

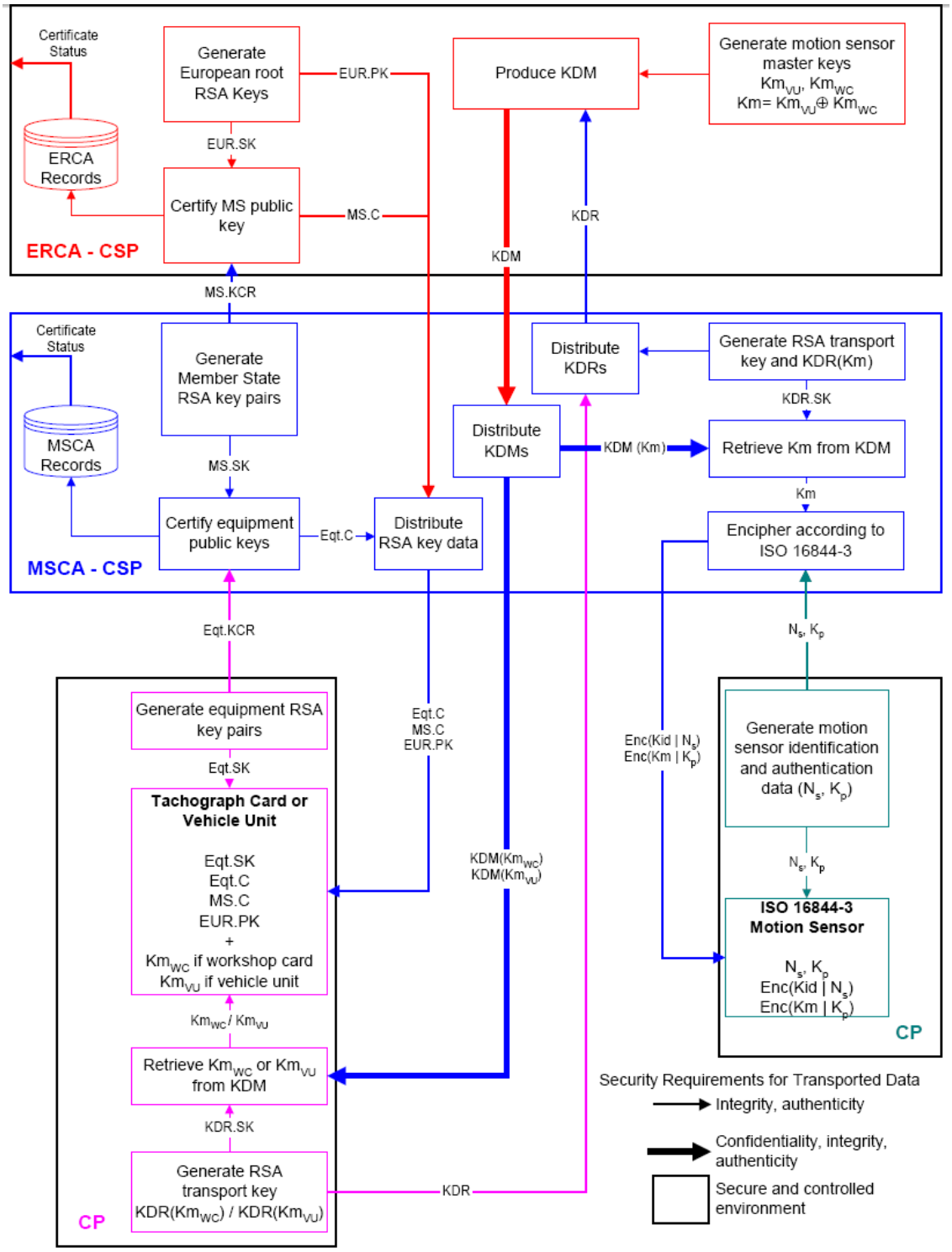


Figure 10 – Description of DT Regulation Annex I(B) key management [ERCA POLICY]

Two different cryptographic systems are used in the DTS:

- Asymmetric cryptographic system for securing the communication between the VU and the Cards, and

- Symmetric cryptographic system with splitting key technology for securing communication between the VU and MS as well as the communication between VU and the cards.

4.1 The Public Key cryptographic system in DTS

The asymmetric cryptographic system based on the standard Public Key Infrastructure (PKI) is used for securing the communication between the VU and the tachograph card. The Digital Tachograph System European Root Policy [ERCA POLICY] defines the general conditions for the PKI concerned and contains accordingly more detailed information. The key management of the PKI system in DTS is depicted in Figure 11. Three hierarchical levels are defined:

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

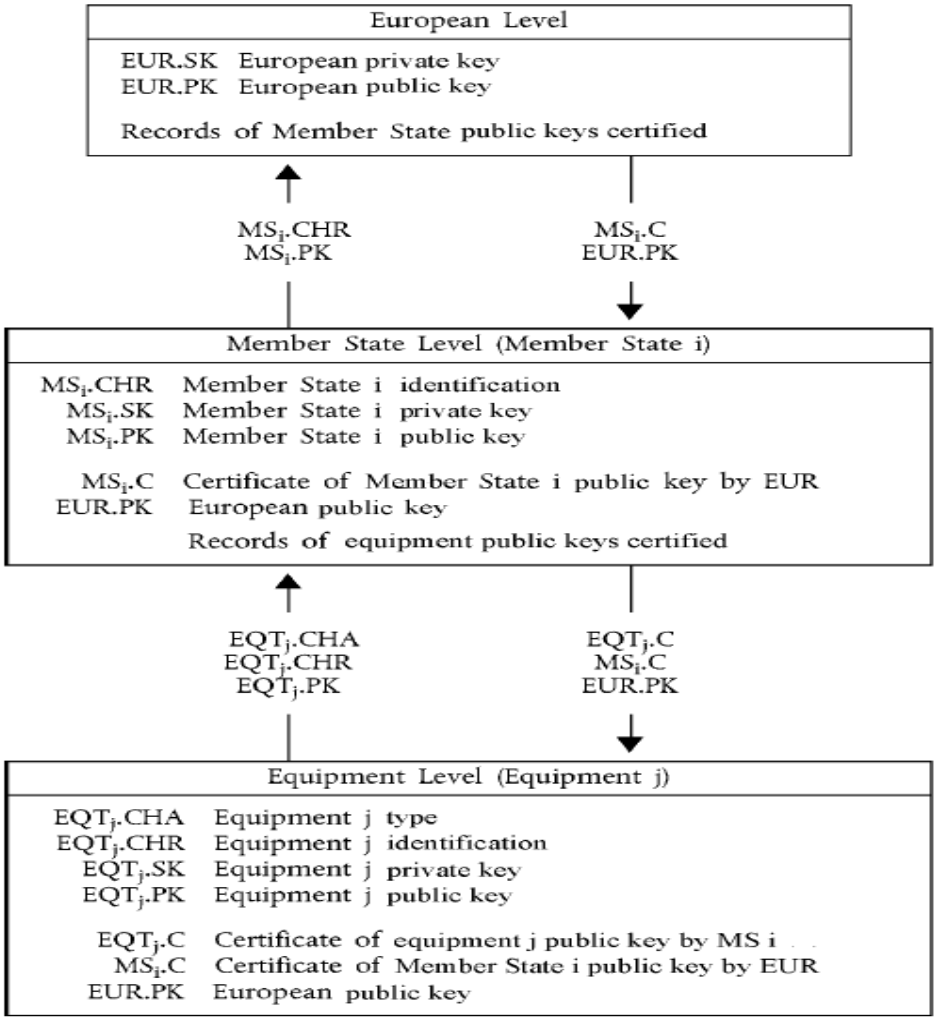


Figure 11 – DT public key management [DT REGULATION]

At the European level, European Root Certification Authority (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 foreseen in the current system.

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 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 [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 (vehicle unit or tachograph card). Equipment public keys are certified by a Member State Certification Authority (EQT_j.PK). This key pair is used for

- authentication between vehicle units and tachograph cards,
- 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.

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 have length of modulus of 1024 bits.

4.2 The symmetric cryptographic system in DTS

The symmetric cryptographic system for the digital tachograph is based on the splitting key technology. Figure 12 represents the general management of the relevant keys. This section builds on the materials found in [Automotive IT].

The ERCA generates two symmetric partial master keys for the MS: 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 VU. 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 VU and the MS as well as for an encrypted transfer of the MS individual pairing key Kp from the MS to the VU. The master key Km and the identification key Kid are used merely during the pairing of a MS with a VU. They are stored neither in the MS nor in the VU.

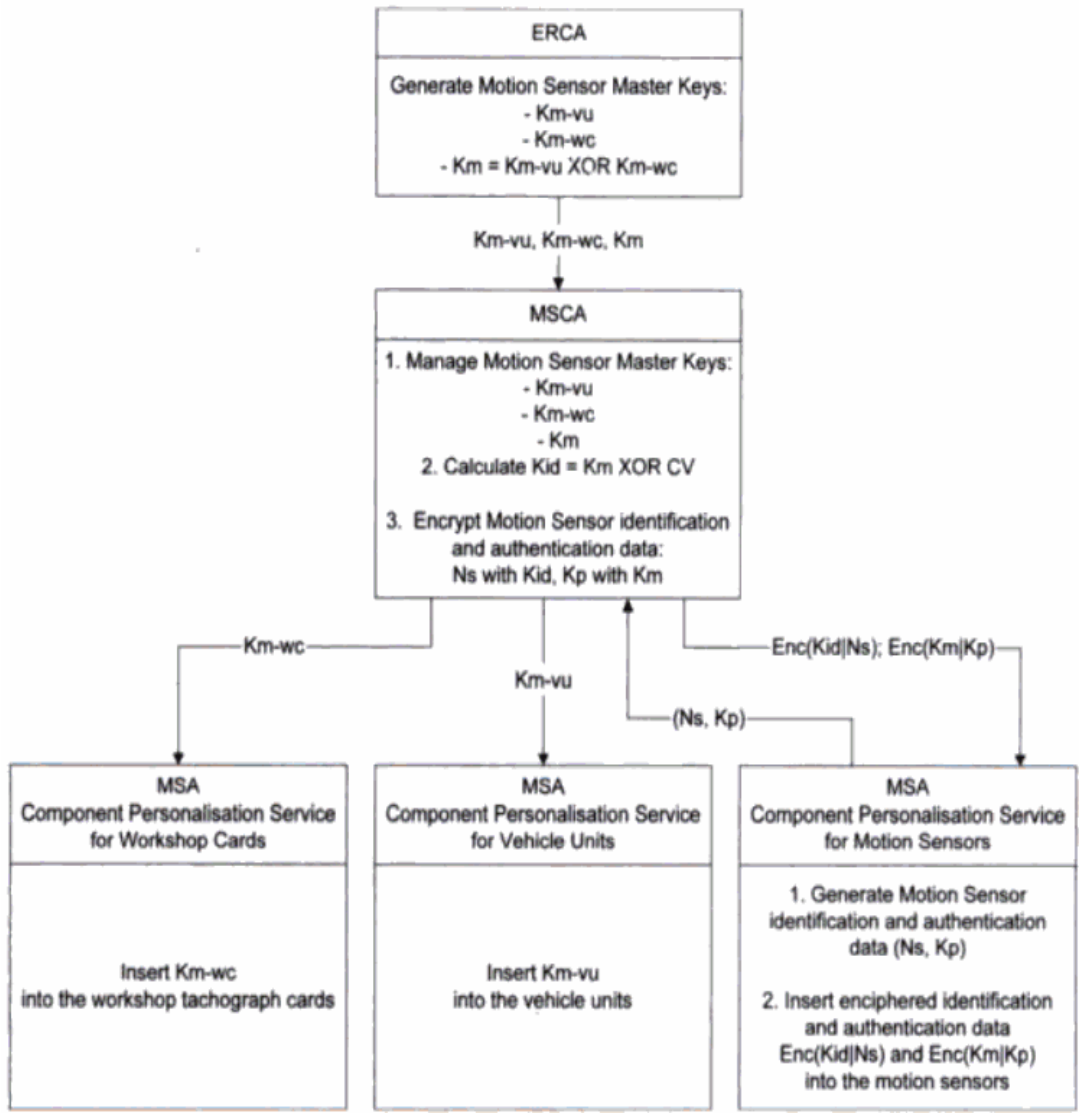


Figure 12 – DT key management for the motion sensor [Automotive IT]

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)

4.3 Communication between Vehicle Unit and Tachograph Card

Appendix 11 of Annex I (B) of the EU regulation [DT REGULATION] 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 a result of this authentication a common symmetric session key is established. This session key remains valid until the card is withdrawn from or reset by the VU. This session key is used for communication between the entities during the operational phase.

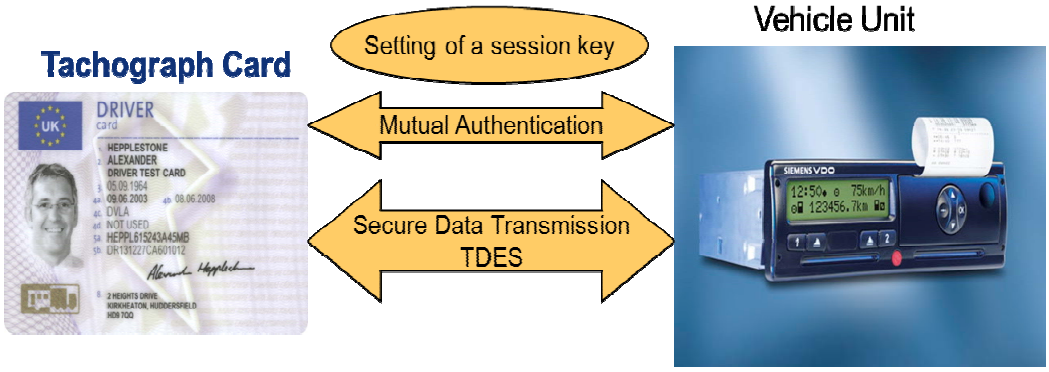
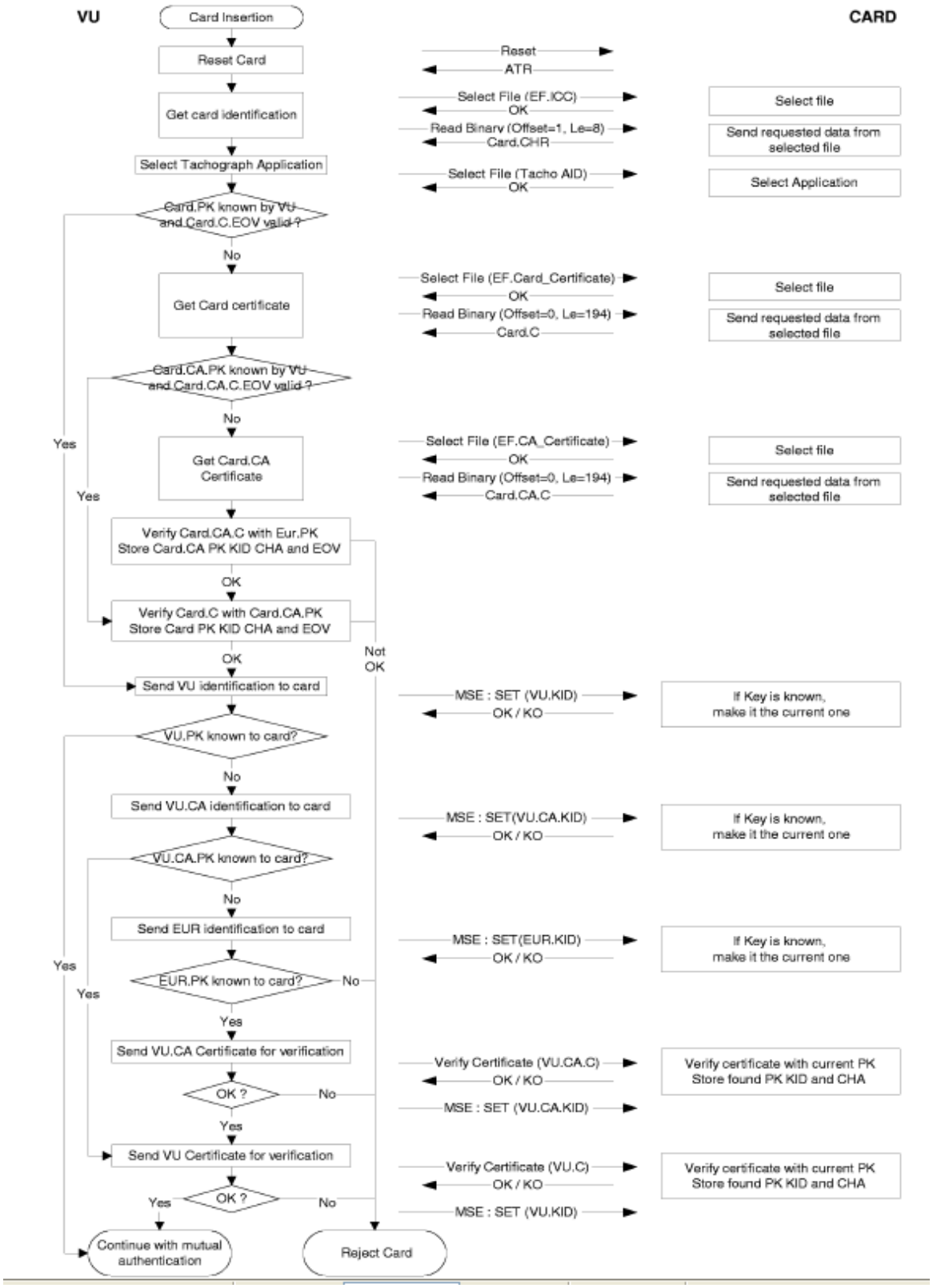


Figure 13 - Communication between VU and Tachograph card

4.3.1 Mutual Authentication

A mutual authentication between the VU and the Tachograph card is required by the EU regulation [DT REGULATION]. 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. 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 (see Figure 14) is defined in Appendix 11 of Annex I (B) of the EU legislation.


VU
CARD
Card Insertion
Reset Card
Reset
ATR
Get card identification
Select File (EF.ICC)
OK
Select file
Read Binary (Offset=1, Le=8)
Card.CHR
Send requested data from selected file
Select Tachograph Application
Select File (Tacho AID)
OK
Select Application
Card.PK known by VU and Card.C.EOV valid ?
No
Get Card certificate
Select File (EF.Card_Certificate)
OK
Select file
Read Binary (Offset=0, Le=194)
Card.C
Send requested data from selected file
Card.CA.PK known by VU and Card.CA.C.EOV valid ?
No
Yes
Get Card.CA Certificate
Select File (EF.CA_Certificate)
OK
Select file
Read Binary (Offset=0, Le=194)
Card.CA.C
Send requested data from selected file
Yes
Verify Card.CA.C with Eur.PK
Store Card.CA PK KID CHA and EOV
OK
Verify Card.C with Card.CA.PK
Store Card PK KID CHA and EOV
OK
Not OK
Send VU identification to card
MSE : SET (VU.KID)
OK / KO
If Key is known, make it the current one
VU.PK known to card?
No
Send VU.CA identification to card
MSE : SET(VU.CA.KID)
OK / KO
If Key is known, make it the current one
VU.CA.PK known to card?
No
Send EUR identification to card
MSE : SET(EUR.KID)
OK / KO
If Key is known, make it the current one
Yes
Yes
EUR.PK known to card?
No
Yes
Send VU.CA Certificate for verification
Verify Certificate (VU.CA.C)
OK / KO
Verify certificate with current PK Store found PK KID and CHA
OK ?
No
MSE : SET (VU.CA.KID)
Yes
Send VU Certificate for verification
Verify Certificate (VU.C)
OK / KO
Verify certificate with current PK Store found PK KID and CHA
Yes
OK ?
No
MSE : SET (VU.KID)
Continue with mutual authentication
Reject Card

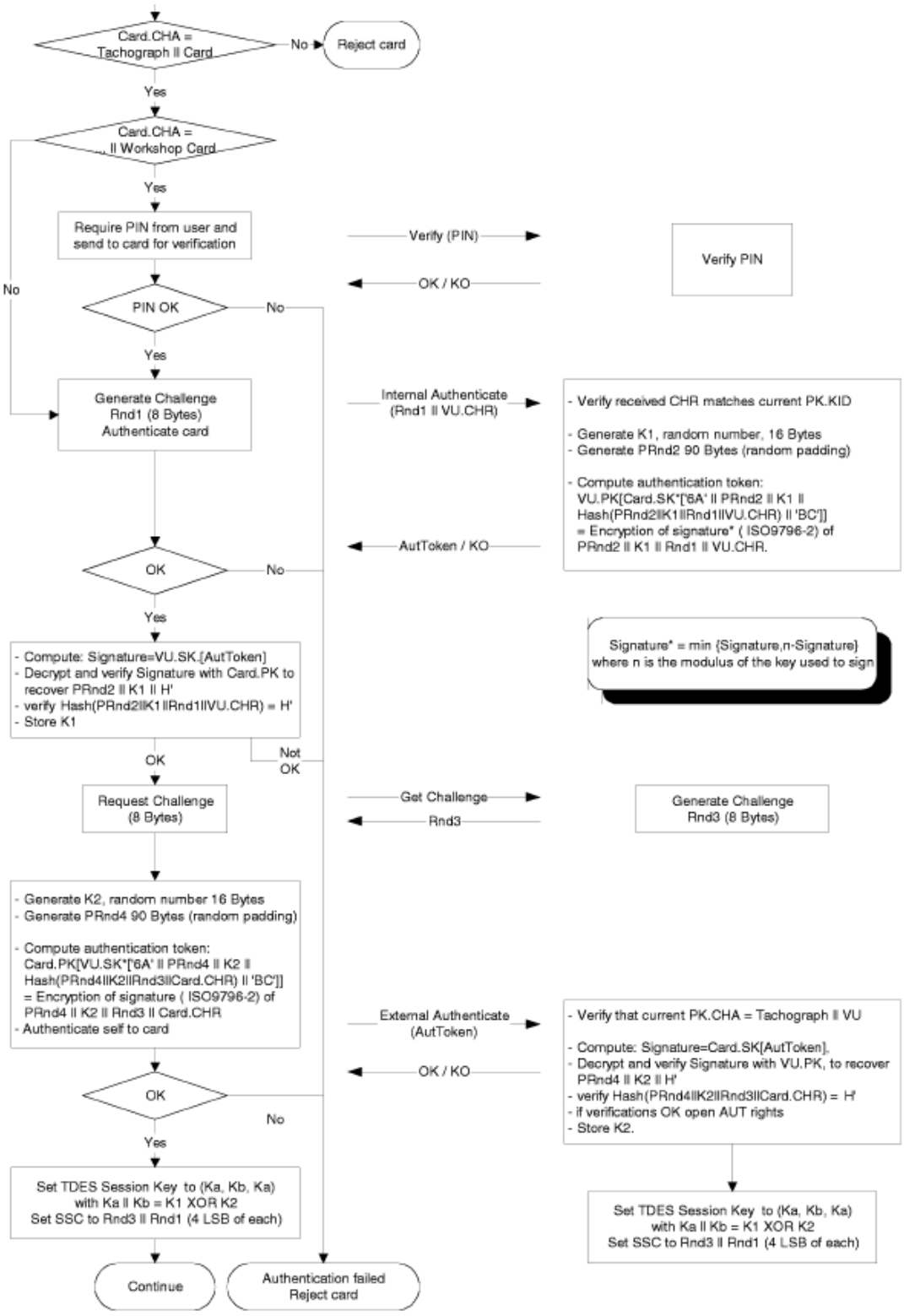


Figure 14 - Mutual authentication according to Appendix 11 of the regulation

4.3.2 Operation

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

- in plain or
- using secure messaging in authenticated mode or
- 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 regulation.

4.4 Communication between Vehicle Unit and Motion Sensor

The EU regulation requires the communication protocol between the MS and the VU to be compliant with ISO/IEC 16844-3 "Motion Sensor interface" [ISO-16844-3]. This section also use some materials found in [Automotive IT].

This ISO standard provides two communication phases at the logical level:

- Pairing phase
- Operational phase

During the pairing phase a MS will be "paired" with a VU. As a result of this pairing a common symmetric session key is established. This session key remains valid until 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 MS implements a set of instructions and plays a passive role, whereas the VU plays an active role in sending these instructions to the MS.

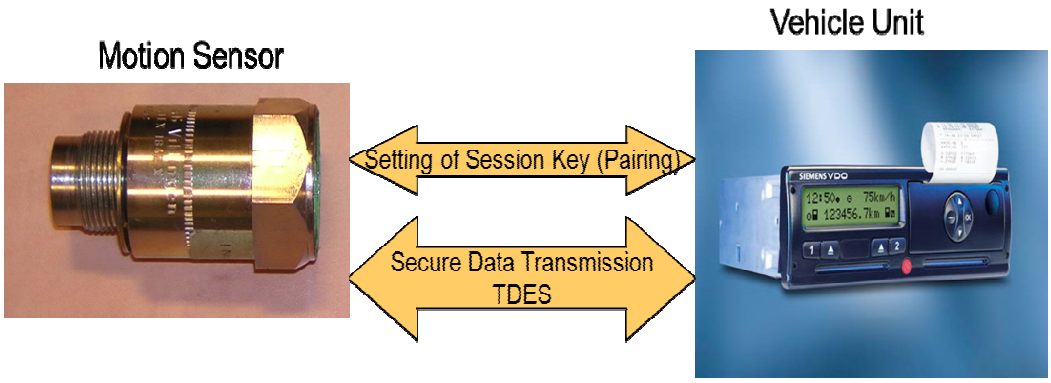


Figure 15 – Communication between VU and MS

4.4.1 Motion sensor state at the end of production

The European certification authority shall generate two independent and unique Triple DES keys Km_{vu} and Km_{wc}, and calculate Km as: $Km = Km_{vu}$ XOR Km_{wc}

The European root certification authority shall forward these keys, under appropriately secured procedures, to Member State certification authorities at their request.

Member State certification authorities shall:

- use Km to encrypt motion sensor data requested by MS manufacturers,
- forward Kmvu to VU manufacturers, under appropriately secured procedures, for insertion in

VUs,
- ensure that Kmwc will be inserted in all workshop cards during card personalisation.

The MS shall be prepared for pairing when it leaves the factory, i.e. the following values shall be stored in its non-volatile memory:
- the extended serial-number of the MS in plain text, NS;
- the extended serial-number of the MS encrypted with the identification key, eKID (NS);
- the pairing key of the MS in plain text, Kp;
- the pairing key of the MS encrypted with master key, eKm (Kp).

The master key and identification key shall not be stored in the non-volatile memory of the MS. The pairing key shall be unique to each MS. The pairing key is only used to pair the MS and the VU. The two 64 bit halves of the pairing key are distinct. A unique session key is generated during the pairing.

The master key shall not be stored completely within the VU memory. The identification key shall not be stored within the VU memory and shall be derived by adding a constant control vector on the master key (K_{ID}=Km XOR CV).

4.4.2 Necessary sequence of instruction for pairing

Pairing of a MS with a VU is triggered by a special instruction sent from the VU to the MS. 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 VU, the VU reads out the workshop card part of the master key Km_{wc}. The VU recomputes the final master key from Km = Km_{vu} XOR Km_{wc} and the identification key K_{ID} = Km XOR CV. The VU authenticates itself by the MS using K_{ID}. A random Triple-DES session key Ks for the operational communication between the VU and the MS is then established. In the last step, the MS authenticates itself by the VU 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.

The pairing process according to ISO 16844-3 is as follows:

- VU Initializes pairing
- The MS sends its serial number Ns.
- The VU sends the extended serial number of the MS encrypted with identification key.
- If the extended serial number of the MS encrypted with identification key, which was stored in its non-volatile memory before pairing, is the same as the one received from VU, the MS returns the pairing key encrypted with master key.
- The VU sends the session key, encrypted with pairing key.
- The session key is decrypted with the pairing key and stored permanently in the non-volatile memory of the MS. It shall be changed by every initialization.
- The VU encrypts the pairing information with the pairing key and shall transmit it to the MS.

- The MS decrypts the pairing information with the pairing key and stores it permanently in the non-volatile memory of the MS. The pairing information shall be found at two locations in the non-volatile memory: at the location for the first pairing and the location for the last pairing. While the pairing information of the first pairing shall never be overwritten, the pairing information of the last pairing changes with every pairing.

4.4.3 VU authentication to MS

- VU Request for authentication
- The MS sends the pairing information encrypted with session key.
- The VU shall decrypt the data bytes with the session key and compare the decrypted data with the pairing information of the current pairing. If they are equal, it is assumed that the authentication of the MS to the VU is correct and that the MS is using the correct session key.

4.4.4 Communication of MS and VU in normal use

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

- real-time movement pulses,
- secured value of the pulse counter and
- secured content of the MS files being read by the VU.

The real-time movement pulses are continuously transmitted in plain to the VU 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 MS is mounted (the correct conversion coefficients are determined and stored in the VU during its calibration by an approved workshop).

The MS as well as the connected VU each runs a pulse counter. Their values are synchronized immediately after the pairing procedure. The VU periodically sends an authentication token to the MS. which answers with the random part of the authentication token and the current value of the pulse counter encrypted by the session key. The VU compares

- the received parts of the authentication token with the respective value having been sent and
- the current value of its own pulse counter with the value received from the MS.

If these comparisons are successful, the VU “knows” that the MS 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 MS is supplied as the secured counter value.

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

The communication of MS and VU in normal use is summarized in ISO 16844-3 as follows:

- The VU sends authentication data to the MS.
- The VU sends request for response to the MS.
- If the VU is authorised, the MS sends authentication and sensor data to the VU.

ISO 16844-3 summarizes the sequence of instruction for VU to read data from MS as follows:

- The VU sends authentication data and the number of the requested file to the MS.

- The VU sends request for response to the MS.
- If the VU is authorised, the MS sends authentication and requested data to the VU.

5 Vulnerabilities and limitations of security mechanisms

Appendix 10 of Annex IB of the regulation [DT REGULATION] on Generic Security Targets requires the minimum strength of the security mechanisms of the MS, the VU and the tachograph cards to be high, with a target level of confidence ITSEC[1] level E3. Appendix 11 of Annex 1B, Common Security Mechanisms, specifies the security mechanisms ensuring that such requirements are fulfilled. This section builds on the materials found in [DT VULNERABILITIES].

Appendix 11 covers the specifications for:

- the mutual authentication between VUs and tachograph cards, including session key agreement,
- the confidentiality, integrity and authentication of data transferred between VUs and tachograph cards,
- the integrity and authentication of data downloaded from VUs and tachograph cards to external storage media.

The confidentiality, integrity and authentication of data transferred between VU and MS is specified in the standard ISO 16844-3. In the following sections, a number of vulnerabilities associated with the security mechanisms are discussed.

The ITSEC E3 HIGH Common Criteria EAL level 4 (with exceptions) should read/follow the better description of Common Criteria from the German BSI.

5.1 DT general security considerations for the future

This section is revised based on the presentation by Prof.Dr. Ernst G. Giessmann at “Future of the Digital Tachograph System Security” meeting in JRC-ISPRA, 05-06/03/2012 [GIESSMANN]. Thanks also to Dr.Giessmann’s comments during the brainstorming session of the above mentioned meeting which I used to revise this section of the document.

DT security model should recognize that we are dealing with the ERCA/DT as a closed system which hence may face a different scale of risk threats than an open system. Consequently for the update of the system security, e.g., the impact of increasing the key length, must be evaluated according to the closed system.

A generic protection profile which defines abstract functionality including the migration concept for DT, as the flexibility to update the security in DT is crucial, is needed. Most important question is how to migrate from one algorithm to the next rather than to decide which algorithm to use next. The eventually defined DT system Protection Profile would need abstract intent and need to identify the functional and conceptual requirements. The Protection Profile shouldn't contain implementation details.

An Algo paper “The crypto in demand “ for the DT closed system which is revised in certain intervals of time, e.g., every 5 years, is also needed. The Algo paper shall contain detailed information regarding the use of a certain cryptographic algorithm with certain parameters, e.g., key length, for a certain interval of time. The Algo paper could be an appendix to the abstract Protection Profile.

[1] The Information Technology Security Evaluation Criteria (ITSEC) is a structured set of criteria for evaluating computer security within products and systems. The ITSEC has been largely replaced by Common Criteria, which provides similarly-defined evaluation levels and implements the target of evaluation concept and the Security Target document. ITSEC level E3 corresponds to common criteria EAL4 security level.

5.2 Obsolescence of Security Mechanisms

The legislation does not accommodate a way to deal with the continuous progress made in cryptography and in cracking ciphers, and consequently, with the obsolescence of the prescribed security mechanisms.

The strength of a number of security mechanisms of Appendix 11 is below the level currently requested for ITSEC High. This threatens the continued delivery of security certification for new DT equipment by security certification authorities.

Although, exceptionally, security certification has continued until now to be granted on condition that the actual security mechanisms have not been defeated in practice and the risk of the defeat of the security mechanisms is low because of the fact that the DTS is a closed system.

The design of Digital Tachograph System should be reviewed to allow adaptation of its security mechanisms so as to maintain over time an adequate level of strength.

In the following parts, elements of security mechanisms subject to obsolescence are described.

5.2.1 Digest Algorithm SHA-1

The Digest algorithm is used to compute the digest value of the message to be signed in the process of preparing the message for digital signature. In modern digital signature applications the message digest is prepared on the computer and sent to the smart card where the RSA[2] algorithm or a relevant algorithm together with the private key is used to generate the signature from the digest value. Afterwards the signature generated is sent back to the computer from the smart card.

The Digest algorithm is a one way function which takes a message as an input and gives a fixed length digest value as the output. Since it is a one way function it is not possible to produce the original message from the digest value. Also there is no way to have the same message digest value from two different messages. The strength of the message digest algorithm depends on these two properties of digest functions.

SHA-1, which is 160-bit message digest algorithm proposed by US government standards agency NIST[3], is used in digital tachograph system. Both digital signature on the downloaded data and the digital signature on the public key certificates utilize SHA-1 digest algorithm.

SHA1 hash algorithm is vulnerable in collusion attack but not broken yet. This attack is not applicable in DT closed system.

According to NIST Recommendation for Key Management SHA-1 provides a level of security that is below the recommended minimum level for the security applications after 2010. Consequently, It is recommended to replace SHA1 with stronger “SHA-2” family of hash functions.

5.2.2 RSA Key Length

RSA is the cryptographic algorithm being currently provided for the asymmetric cryptographic system in the DTS. RSA keys currently used in DTS have a length of modulus of 1024 bits. In the literature, it is forecasted that a RSA 1024 key length could be broken in an academic set-up around 2016 using

[2] RSA (from the names Rivest, Shamir and Adleman who first publicly described the algorithm) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

[3] National Institute of Standards and Technology

substantial computer power. A similar attack would still need to be carried out afterwards by malicious attackers on the digital tachograph keys, before the keys are broken.

RSA key length of 1024 is not considered a measure providing sufficient strength to the security mechanisms of the DTS [Automotive IT]. 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”. Consequently, also the security mechanisms implementing RSA must be of a high strength, which depends concretely also on the length of modulus.

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 practice, each Member State has its own guideline for it, which is not made generally public. In Germany such a guideline is public and allows the use of the 1024-bit sized RSA as “high-secure” merely until end of 2007, in the context of the German Digital Signature Law.

In order to maintain the security level of the system as high it is recommended to move to RSA Key length of 2048 bits or longer after 2010 according to NIST Recommendation for Key Management.

5.2.3 Moving to longer keys of RSA

In order to maintain the security level one solution would be to use longer keys (e.g. 2048 bits). This will solve the problem for a while (e.g., 5 years) and after the longer keys will not be able to maintain the security level. Then it will be necessary to increase the key length again. At this point it is important to have flexibility in the system to enable increasing the key length and even change the cryptographic algorithm.
However increasing the key length has an impact on the certificate verification time and RSA operations on the card delaying the response time of the card. It is necessary to use faster algorithm providing high security with shorter key length.

We have no security problem (today) for smart cards but it is necessary to listen to the alarm signals.

Tachograph PKI can consider consider different security at different hierarchy levels e.g. RSA1024 on smartcards and RSA 2048 or better for ERCA and MSCAs. Since MSCA certificate is verified on the card less frequently than VU certificate, increasing the key length of ERCA/MSCA will not have a significant effect on the card performance.

5.2.4 Elliptic Curve algorithm

As increasing the key length of the RSA algorithm will have a significant impact on the performance of the system as the RSA encryption and decryption will take much longer time with longer keys, as a result the mutual authentication will take longer time. Therefore a better solution would be to switch to elliptic curve algorith (e.g., ecdsa-sha256) as it provides higher level of security with shorter keys. Eliptic Curve Cryptography (ECC) algorithm may be considered to replace RSA although they need a very strong Random Number Generator (RNG). Some systems have been found in internet SSL that use the same RNG due to hardware limitations. ECC devices will need extra protection against side channel power attacks. Although the side channel protection on the cards for ECC is not as mature as for RSA, still high quality vendors, e.g., NXP, Infineon, Gemalto have implemented side channel protection.

5.2.5 Triple DES Encryption Mechanism

The Triple DES (Data Encryption Standard) encryption mechanism is used in secure messaging between cards and VUs as well as between VUs and MS. It is a symmetric key encryption mechanism which provides authenticity and confidentiality for the data transferred between two entities.

Triple DES, which is also called as TDEA, is defined by [NIST-SP800-67]. The algorithm encrypts and decrypts data in 64-bit blocks, using three 56-bit keys. According to NIST Recommendation for Key Management 2TDEA provides 80 bits of security which is below the required level after 2010 although TDES in DTS has not been attacked yet. It is still recommended to switch to AES (Advanced Encryption Standard) with 128 or longer keys after 2010.

5.3 Master Key for the Motion Sensor

A universal master key for the MS is used for the pairing between the VU and the MS. The key is split (XOR) into two parts. One half is stored in the workshop cards, while the other half is stored in the VUs. 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 VU and the MS.
- The initiation of the pairing protocol can be invoked without use of a workshop card.
- Cloning of MSs will be feasible.

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

Moreover, the pairing master key is stored at different places and if it goes lost then it will not be possible to identify where it was lost. Introducing new workshop cards the renewal of the pairing key should be considered. This is at most not a matter of cryptography but of organizational protection [GIESSMANN]

Symmetric authentication scheme should be investigated to replace the current splitting key implementation for the future [CWA14890-1].

5.4 PIN Management of the Workshop Card

There exists vulnerability in the procedure that takes place between a VU and a workshop card at the moment of the authentication of the workshop card using its PIN. The authentication is not protected nor verified by encryption. It is therefore relatively easy to use a workshop card even without knowing its PIN. The security provided by the PIN of a workshop card is therefore very low.

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.

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.

5.5 Communication Protocol of ISO 16844-3

The standard ISO 16844 supports and facilitates the communication between electronic units and a digital tachograph. Part 3 [ISO-16844-] of the standard specifies the physical and data link layers of the electrical interface connecting a MS to a VU. In particular it specifies the communication protocol that encrypts all information exchange between the MS and the VU during mutual authentication and speed data transmission.

This communication protocol is the result of a standardization effort carried out by industrials. It was adapted incrementally a number of times to fix a vulnerability that would allow the injection of false data in the communication between the MS and the VU.

As a result the protocol is complex and not fully aligned with the standard used currently for security certification. It is likely that, currently, a thorough security evaluation of the standard would most likely not successfully pass the required security certification.

Additionally, it is felt that the complexity of the security countermeasures introduced to reinforce the protocol is such that interoperability between cards and VUs is difficult to assure by industrials.

5.6 Data downloaded from Vehicle Unit

Data blocks downloaded from VUs are signed, but most are not time stamped individually. As a consequence, downloaded data can be manipulated by software: blocks extracted from files downloaded at a different moment in time can be pasted together and presented as a plausible downloaded file. Different scenarios can exploit this vulnerability. It is possible to tamper data downloaded at the premises of the undertaking so as to withdraw, for instance, undesired list of events and faults, an entire day of activity, or the last activities of a day. Also, it is possible to paste blocks downloaded using different company cards, in effect selectively hiding activities protected by company locks.

While this threat is real and technically easy to implement, there is no evidence that it is currently exploited, likely because roadside checks are not affected at all (roadside enforcers download unadulterated data). There exist a simple solution, which is also backward compatible with the current DTS, which would solve the scenario of using the activities until the middle as the activity for the whole day.

5.7 Replacement of the ERCA private keys

Currently, it is not foreseen the possibility to use private keys different than those initially generated by the competent bodies at the start-up of the implementation of the digital tachograph system.

Consequently there is no predefined procedure to follow in the case that a private key is lost or disclosed.

In the case of a loss of a private key at national or European level, the direct consequence is that no new certificates at national or European level, respectively, can be generated.

In the case a private key is disclosed, integrity and authentication of the data which is certified by the key cannot be trusted any more.

In both cases, there is the need to generate new keys and introduce them quickly in the system.

5.8 Public Key certificate structure

A public key certificate is an electronic document which uses a digital signature of a Certification Authority to bind together a public key with an identity (information such as the name of a person or

an organization, their address, and so forth). The certificate is used to verify that the public key belongs to the identity.

In the DTS, the certificates are issued to the equipments rather than the persons. As a result the digital signature is not legally binding. X.509 certificates could be issued to the persons rather than the equipments but then because of the larger size of the certificate there would be a significant impact on the card response time as the certificate verification on the card would take longer time.

5.8.1 Current Tachograph Certificate

The current certificate structure in Digital Tachograph System for 1024-bit RSA public keys is described in Annex I(B) Appendix11 CSM_017 and CSM_018. The contents of the certificate consist of the data as depicted in the Table 1, while the structure of the certificate is depicted in Table 2

Data	Format	Bytes	Observations
CPI	INTEGER	1	Certificate profile identifier (‘01’ for the current version)
CAR	OCTET STRING	8	Certification authority reference
CHA	OCTET STRING	7	Certificate holder authorization
EOV	TimeReal	4	Certificate end of Validity. Optional, ‘FF’ padded if not used
CHR	OCTET STRING	8	Certificate holder reference
n	OCTET STRING	128	Public key(modulus)
e	OCTET STRING	8	Public key(public exponent)

Table 1 - DTS certificate contents with 1024-bit RSA key length

RSA Public key certificates used in DTS are non-self-descriptive Card Verifiable Certificates [ISO-7816-8]. Unlike X.509 certificates, Card Verifiable Certificates (CVS) are signed using a signature scheme with message recovery. This saves space and time because essentially only the signature value has to be stored and to be transmitted rather than the signature value together with the plaintext contents. Furthermore, CVC’s do not contain data elements that are hard to be verified on a card, like the validity period [HENNIGER]. The temporal validity is not verified during the certificate verification on the card.

In DTS the certificate holder’s unique identity is not present in the public key certificate structure. As a result, the digital signature generated has no legal value according to [E-SIGN-DIRECTIVE].

CVC is chosen for DTS mainly because of small size, which enables faster verification on the card, and role based authorisation capability as it contains Certificate Holder Authorisation filed which enables role based authorisation in the system.

The current public key certificate content in Table 1 is digitally signed as shown below according to the digital signature mechanism with partial recovery in accordance with ISO/IEC 9796-2, with the Certification Authority Reference appended.

- X.C = X.CA.SK[‘6A’||Cr||Hash(Cc)||’BC’]||Cn||X.CAR

Here X.C represents the public key certificate generated; X.CA.SK represents the secret key of the CA which is used in the RSA operation to generate the encrypted part of the digital signature structure explained in Table 2.

Data	Format	Bytes	Observations
6Ah	INTEGER	1	ISO 9796-2 signature recoverable message start byte
Cr	OCTET STRING	106	ISO 9796-2 signature recoverable message
Hash(Cc)	OCTET STRING	20	ISO 9796-2 SHA-1 hash of message (certificate contents)
BCh	INTEGER	1	ISO 9796-2 signature trailer byte
Cn	OCTET STRING	58	ISO 9796-2 non-recoverable message
CAR	OCTET STRING	8	Certification authority reference

Table 2 - DTS certificate structure with ISO 9796-2:1997 signature

The Certification Authority Reference (CAR) field which is added to the signature is not checked with the one in the signed data, it should be checked that the outside X.CAR is the same as inside the X.CAR during the verification of the certificate.

5.8.2 X509 Certificate

The public key contained in the certificate is used to verify digital signatures that have been created using the corresponding private key. The digital signatures to be verified could, for instance, be created for the purpose of authenticating the certificate owner against the card in a challenge-response protocol using public-key cryptography. For the purpose of device authentication, card-verifiable certificates are used. As explained in [HENNIGER], the attribute "card-verifiable" may suggest that other certificate formats, like X.509 [X509] certificates, could not be verified on smart cards, but this is not entirely true. The authentication against the card can be carried out using the widely used X.509 certificates, without a card-specific certificate format. An essential part of the verification of X.509 certificates on smart cards is possible, although it will have a significant impact on the card response time, yet it is still not possible checking the temporal validity of the certificate and checking whether the certificate has been revoked.

The reason to choose CVS in the DTS was the need to verify the certificate on the smart card during the mutual authentication process thanks to the small size of CVS which enables faster verification on resource constrained environment of cards.

The certificate structure in Table 3 could be used if, despite the issues mentioned above, X.509 will be decided to be used in the future.

Certificate fields		**Type**	**Typical values**
TBSCertificate	version	Integer	**3**
	serialNumber	Integer	**45566**
	signature	AlgorithmIdentifier	**{1 2 840 113549 1 1 5}**
	issuer	RDNSequence	**CN= Member State Certification Authority, L=ISPRA, C=IT**
	validity	UTCTime	**Jan 28, xx10** **Jan 28, xx12**

	subject	RDNSequence	**CN= NAME SURNAME, SERIALNUMBER= 15869063592,C=TR**
	subjectPublicKey Info	BIT STRING	**30 81 89 02 81 81 00 c5 5f 4c 57 a1 df b9 ad 55 b1 dc 65 5d e6 73 e6 5b 92 0d 6e 75 20 46 7a d9 …..**
	certificateHolder Authorisation	Extension	**1 : Digital Tachograph Driver Certificate**
Signature Algorithm		AlgorithmIdentifier	**{1 2 840 113549 1 1 5}**
signature		BIT STRING	**4281a84b3a2e8fc3d254f719ae01b872d4407e4476bd321d3d5ebbd71c9a…..**

Table 3 - X09 certificate content for possible proposal for future DTS

Certificate holder authorization data element (CHA) which exists in the current DTS certificate identifies the role that the certificate holder is allowed to take. Equipment type field in the CHA must be added to X.509 as depicted in Table 3. Extension type can be used for this purpose.

5.9 Driver card authentication

An authentication mechanism between the driver and his driver card is not present in the current DTS. It is, however, important to ensure that the user of a driver card is indeed the genuine owner of the card.

One approach is that the driver card requires a PIN in order for the driver to prove that he is the owner of the card that is being used. The authentication of the driver to the system cannot be considered to be fully established without the use of a PIN or of some other authentication methods (e.g., biometric authentication).

5.10 Signature verification and certificate revocation

Digital signature verification is the process of checking the integrity and authenticity of the signed data in the online systems where the signature verification process involves the revocation checking of the signing certificate which requires reference to signing certificate and revocation information provided to the verification software.

In the public key infrastructures based on X.509 the revocation information is provided over OCSP (Online Certificate Status Protocol) servers or CRL (Certificate Revocation List), which require online connection. Certificate serial number is used to uniquely identify a certificate while revocation reference is used to check if the certificate is valid during the revocation checking when verifying a certificate.

The ERCA maintains a CRL for Member State certificates but there is no CRL for the certificates in the tachograph cards or vehicle units. As the equipment certificates are verified on the cards, adding revocation checking on the card would have a significant impact on the performance which would result in longer card response time.

Consequently, since DTS is an offline system and certificate is verified on the card, it is not feasible to introduce revocation service for the verifications on the card. Although revocation service can be considered for the digital signature verification of the downloaded data.

5.11 Standardization of security mechanisms

5.11.1 Digital Signature standardization

In the DTS, ISO/IEC 9796-2:1997 [ISO-9796-2] standard scheme is used for digital signatures on the public key certificates and PKCS#1 v1.5 is used for the digital signatures on the downloaded data. These schemes have become obsolete and are now superseded by modern and robust standards.

Following attacks around the year 2000, the ISO 9796-2:1997 standard has been revised into ISO 9796-2:2002. ISO 9796-2:2002 defines mechanisms that have some strong, undefeated, security arguments. The attacks against ISO 9796-2:1997 appear, however, impracticable in the context of the DTS, because an attacker has no way to obtain the many signatures of fixed data necessary to carry out the attacks. These attacks do not work on the ISO 9796-2:2002 [ISO-9796-2002] standard.

Similarly, PKCS#1 v1.5 [PKCS 1.5] has been superseded by a newer version, v2.1, of which digital signatures have some strong, undefeated, security arguments.

Ad-hoc signature PKCS #1 V.1.5 is prone to side channel attacks as to be signed data is not randomized before the signature generation takes place. PKCS #1 V.2.1 [PKCS 2.1] uses salt on the data to be signed which makes it stronger against side channel attacks.

5.11.2 Mutual Authentication Mechanism

Although there is no known attack against it, the mutual authentication mechanism used between tachograph cards and VUs is “non standard”.

The protocol discussed in section 5.3.1 has also disadvantage that the card is revealing its identity and certificate before it has verified the credentials of the VU. This could be viewed as a violation of the privacy of the card holder [CWA14890-1].

The fact that the mutual authentication mechanism in DTS is “non standard” is not vulnerability itself, still it can be formalized in the system, e.g., "internal standard of the mutual authentication between tachograph cards and VU's"

Device authentication with privacy protection is recommended for the future DTS [CWA14890-1] for the mutual authentication mechanism in DTS.

5.12 Vulnerability of data stored on Driver Card

Driver cards do not have a security mechanism to check and trace the origin of a modification of their stored data. Modification of driver card data is done via any VU and is allowed thanks to a private key allowing such editing function. If the security of the private key of a single VU is compromised, then it is possible with this key, without time limitation, to tamper data stored on any driver card. In a future system, this risk could be mitigated by changing the method and the information that is stored on the driver cards.

5.13 Key certification requests

Annex A of the Digital Tachograph System European Root Policy document [ERCA POLICY] explains the public key certificate request format arriving from the member states to ERCA. The request carries the digital signature generated by the private key of the member state, the corresponding public key of which is enclosed in the certification request. The protocol demonstrates that the entity submitting the certification request possesses the private RSA key associated with the public RSA key whose certification by the ERCA is requested.

The requests are brought to ERCA by a trusted courier on a CD. The hash of the public key to be certified by ERCA is verified by a telephone call to the identified contact point of the national authority. In that way it is asserted that the public key is coming from the identified national authority.

The public key certification requests can be sent to ERCA by e-mail encrypted by PGP public key of ERCA. The motion sensor master key distribution needs to be continued via the courier as the symmetric master keys needs to be kept confidential.

6 Merge of Driver Card with E-Driving License

With the presentation “PKI considerations for the next generation digital tachograph” at the Smart Event 2011 in Sophia Antipolis in France [DT PKI] the merge of the tachograph driver card with the e-Driving license was suggested offering also the use of the ERCA experience for the top level PKI services for e-Driving license and Intelligent Transport Systems. According to the suggestion the tachograph card application could be added to the same card with e-Driving license as a second application as it is seen in Figure 16. The current card technology (e.g., java cards) supports the hosting of more than one application in the same card.

Having a separate security evaluation for each application in the same card is possible according to different level of security.

The security evaluation includes chip security, card operating system security and application security. In the merged card the chip and the card operating system must satisfy the higher security requirement between the security level of Tachograph card and driving license.

Even though it is possible to have separate security evaluation for each application in the same card, it is still recommended to select the higher level security target and evaluate the card including both applications on the card according to the selected level of security.

UICC protocol can be used to use two crypto set on the card at the same time. Merging the tachograph card with e-Driving license is technically straightforward but the management of the merged card needs to be investigated. Ownership of the card is a question when hosting more than one application on the card. The merge of the two cards needs to be evaluated in terms of the two regulations and the synchronization of the two separate processes. Two cards have different lifetimes and issued by different bodies and involve different procedures.

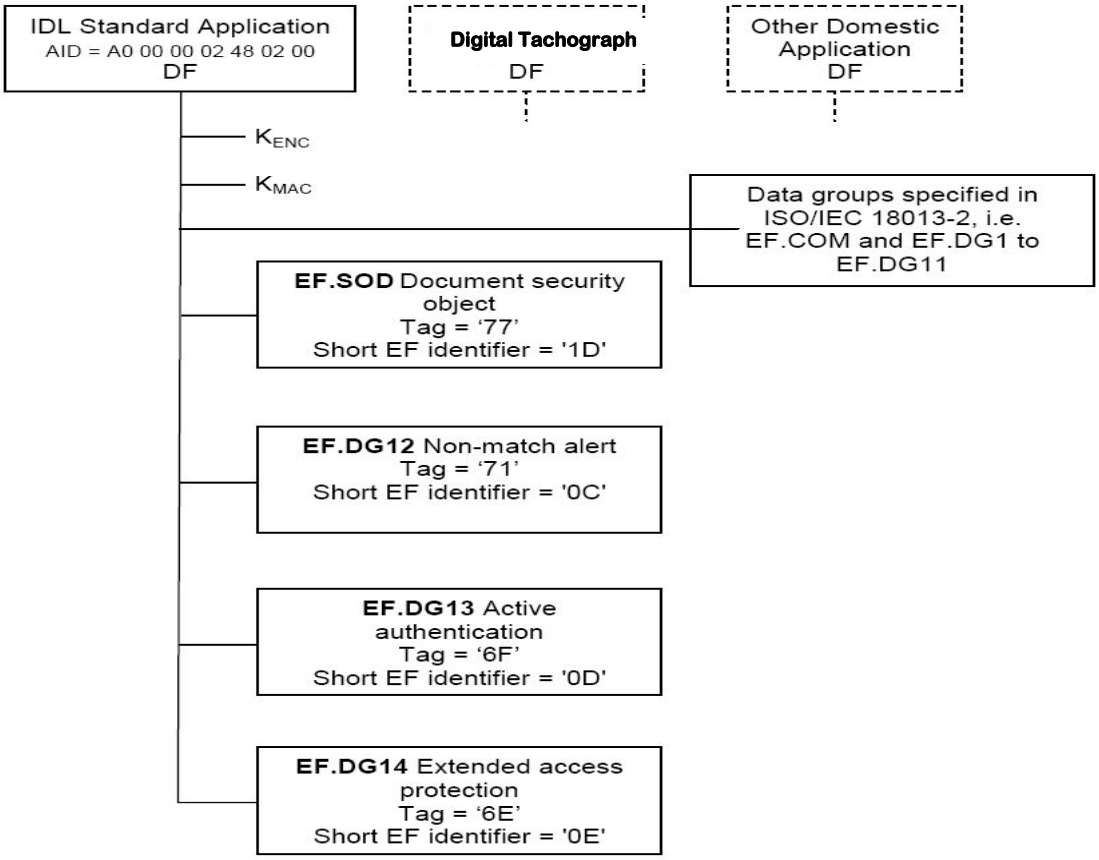


Figure 16 - ISO/IEC 18013-3:2009 DL Data Groups with Digital Tachograph as a second application

6.1 Benefits of the merge

- Drivers only carry one card instead of two
- No need for cross identity link
- Potential fraud reduction
- Merged cards could reduce running costs for card issuing authorities
- It will be easier for enforcers to determine whether tachograph card holder has correct driving entitlement. [CORTE]

7 Considerations for the future DTS

7.1 DT evolution to ITS-S

This section builds on several ETSI ITS standards and the presentation by Scott Cadzow at "Future of the Digital Tachograph System Security" meeting in JRC-ISPRA, 05-06/03/2012 [CADZOW]. Thanks also to Mr CADZOW's comments during the brainstorming session of the above mentioned meeting which I used along this section of the document.

Intelligent Transport Systems (ITS) can be the address of the research on the future Digital Tachograph system. The idea of expansion of Digital Tachograph to ITS needs to be investigated.

During the revision process towards the next generation Digital Tachograph, it must kept in mind that ITS could replace DT in a decade. Working on a generic protection profile for DT which allows eventual expansion to ITS could facilitate the future developments in DT to converge to ITS.

Evolution of ERCA towards a Root CA as central trust anchor for ITS needs also to be considered in the research for the future DTS.

In the following subsections ITS architecture is introduced.

7.1.1 intelligent transportation systems

The term intelligent transportation systems (ITS) refers to information and communication technology applied to transport infrastructure and vehicles that improve transport outcomes such as transport safety, transport productivity, travel reliability, informed travel choices, social equity, environmental performance and network operation resilience.[WIKIPEDIA]

Interest in ITS comes from the problems caused by traffic congestion and a synergy of new information technology for simulation, real-time control, and communications networks. Traffic congestion has been increasing worldwide as a result of increased motorization, urbanization, population growth, and changes in population density. Congestion reduces efficiency of transportation infrastructure and increases travel time, air pollution, and fuel consumption.

Intelligent transport systems vary in technologies applied, from basic management systems such as car navigation; traffic signal control systems; container management systems; variable message signs; automatic number plate recognition or speed cameras to monitor applications, such as security CCTV systems; and to more advanced applications that integrate live data and feedback from a number of other sources, such as parking guidance and information systems; weather information; bridge deicing systems; and the like. Additionally, predictive techniques are being developed to allow advanced modelling and comparison with historical baseline data.

Technological advances in telecommunications and information technology, coupled with state-of-the-art microchip, RFID (Radio Frequency Identification), and inexpensive intelligent beacon sensing technologies, have enhanced the technical capabilities that will facilitate motorist safety benefits for intelligent transportation systems globally. Sensing systems for ITS are vehicle- and infrastructure-based networked systems, i.e., Intelligent vehicle technologies. Infrastructure sensors are indestructible (such as in-road reflectors) devices that are installed or embedded in the road or surrounding the road (e.g., on buildings, posts, and signs), as required, and may be manually disseminated during preventive road construction maintenance or by sensor injection machinery for rapid deployment. Vehicle-sensing systems include deployment of infrastructure-to-vehicle and vehicle-to-infrastructure electronic beacons for identification communications and may also employ video automatic number plate recognition or vehicle magnetic signature detection technologies at desired intervals to increase sustained monitoring of vehicles operating in critical zones.

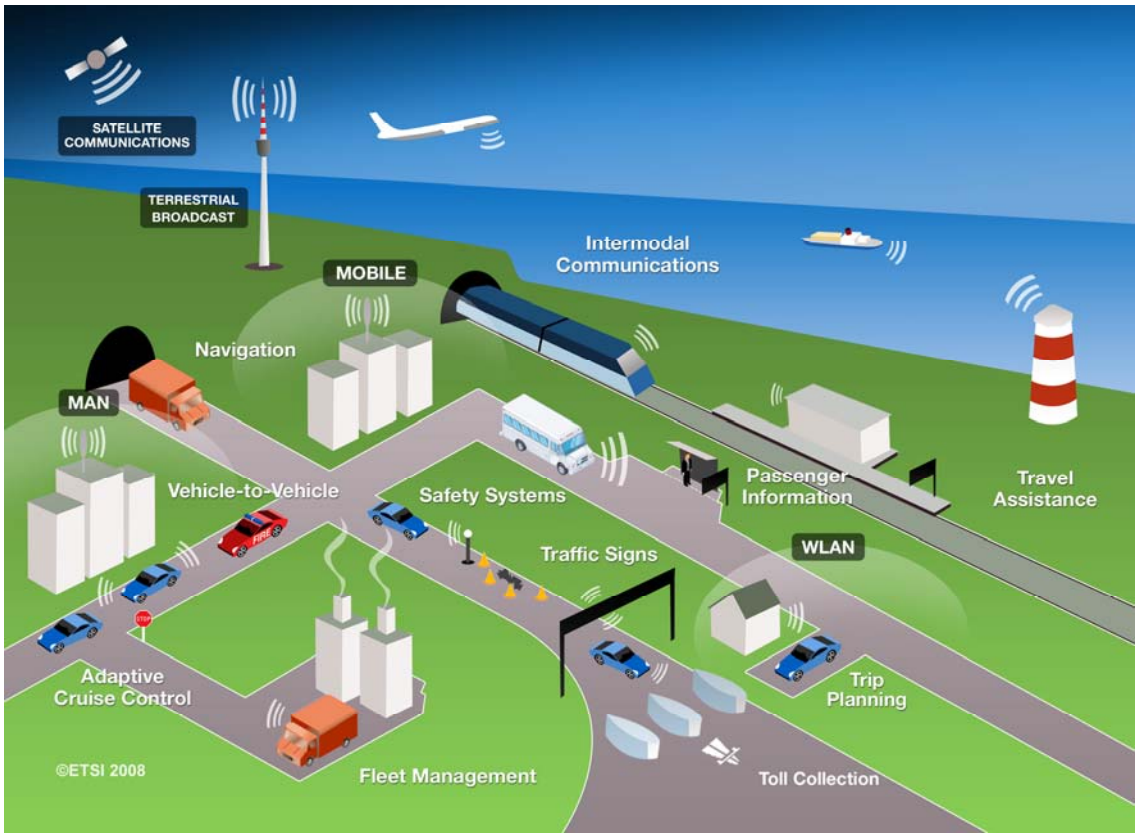


Figure 17 ITS technologies [ETSI ITS]

7.1.2 Cooperative systems on the road

The concept of Intelligent Transport Systems and Services (ITS) includes cooperative systems for vehicles communicating via radio interface with each other and with the roadside infrastructure. Cooperative systems will enhance the support available to drivers and other road users, providing for greater transport efficiency and increased safety.

Communication cooperation on the road includes car-to-car, car-to-infrastructure, and vice versa. Data available from vehicles are acquired and transmitted to a server for central fusion and processing. These data can be used to detect events such as rain (wiper activity) and congestion (frequent braking activities). The server processes a driving recommendation dedicated to a single or a specific group of drivers and transmits it wirelessly to vehicles.

The goal of cooperative systems is to use and plan communication and sensor infrastructure to increase road safety.

- ITS are often classified into the following categories [CADZOW]:
  - Advanced Traveller Information Systems (ATIS)
  - Advanced Traffic Management Systems (ATMS)
  - ITS-Enabled Transportation Pricing Systems
  - Vehicle-to-Infrastructure Integration (VII)
  - Vehicle-to-Vehicle Integration (V2V)

- ITS stations send environmental (event) and (vehicle) status data to other ITS stations
  - DNN, CAM
- ITS stations may exist in vehicles
- ITS stations may exist in roadside furniture
- ITS stations may be networked together
- Interpretation of received data may assist in driver safety
  - E.g. Collision avoidance
- Interpretation of received data may assist in regulatory compliance
  - E.g. Speed limit notification and adherence
- Different data has different authority
  - E.g. Speed limit notification from an authority versus speed assertion from an ITS station

7.1.3 Automotive systems

There are currently the following projects related to automotive ITS [ETSI ITS]:

- Dedicated Short-Range Communications (DSRC) provide communications between the vehicle and the roadside in specific locations (for example toll plazas). Applications such as Electronic Fee Collection (EFC) will operate over DSRC.

- Wireless Communications Systems dedicated to Intelligent Transport Systems and Road Transport and Traffic Telematics will provide network connectivity to vehicles and interconnect them. Using radio bands requires adequate Harmonized Standards which are under development for the bands 5 GHz and 63 GHz.

- Continuous Air interface Long and Medium range (CALM) provides continuous communications between a vehicle and the roadside using a variety of communication media, including cellular, 5 GHz, 63 GHz and infra-red links. CALM will provide a range of applications, including vehicle safety and information, as well as entertainment for driver and passengers.

These technological projects form part of wider initiatives on matters such as road safety (for example the European Commission's eSafety initiative) and road tolling.

7.1.4 Railway systems

The railways industries have agreed to use GSM for the signaling on high speed railways, as well as for conventional railways when interoperating across national borders. Within Europe, interoperability of high-speed railways is a regulatory requirement, addressed by the European Commission's Directive 96/48/EC.

7.1.5 Aeronautical and maritime systems

Aeronautical applications extend from professional services, such as air traffic control systems, to services for passengers, such as onboard telephony, and ETSI is responsible for specifying many of them.

Maritime applications support routine maritime operations, including navigation, as well as safety purposes. ETSI is responsible for producing a range of technical standards and reports concerning radio equipment and system for maritime and inland waterways use.

7.1.6 ITS Architecture Standards

In April 2010, ISO published the ITS communications architecture standard ISO 21217, which is part of the published basic set of communication standards for cooperative systems in ITS. In September 2010, the ETSI version of the ITS communications architecture standard EN 302 665 was published [H.J. Fischer].

IEEE 1609 is developing an ITS communications architecture standard (IEEE 1609.0) for short-range 5.9GHz (IEEE 802.11/1609 (WAVE)) communications only (V2V / V2I)

Basic design principles of the ITS communications architecture are:

• Standards are enabling (different to system specifications)

• Major focus is on the management needs, given by the various communication protocols and supported implementations.

• A distinct class of communication devices with various possible access technologies is necessary to meet ITS requirements.

• ITS Stations (ITS-S) should be capable of communicating over present and future communication networks, esp. the Internet (IPv6)

• ITS-Ss should be capable of communicating with legacy nodes on any network to which they can attach.

• Communication between ITS-Ss and between ITS-Ss and legacy nodes in most cases will be peer to peer.

7.1.7 ITS Station Concept

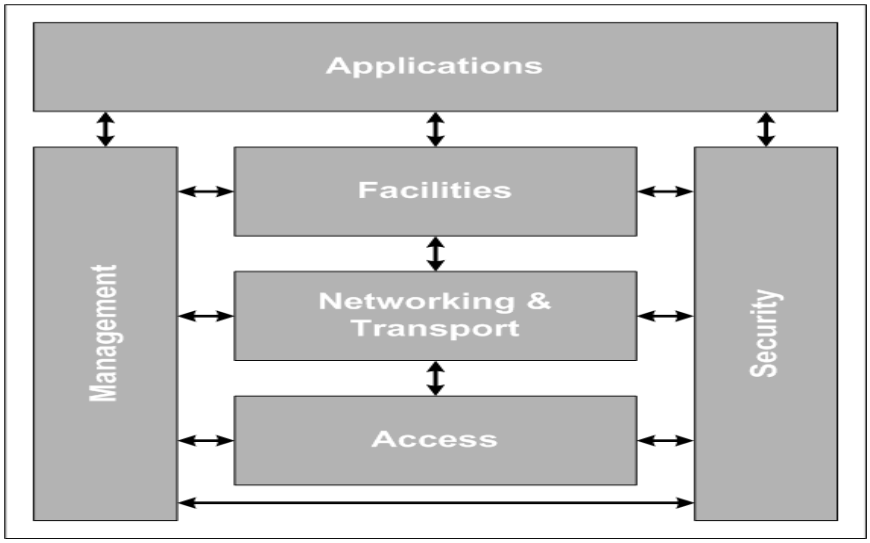


Figure 18 - ITS applications as part of the ITS station reference architecture [EN-302665]

The concept of an ITS station is based on protocols of the OSI model for communications, operating in a bounded secure management domain.

Communications Access for Land Mobiles (CALM) communication standards are built on the basis of the well-known layered OSI model, which was simplified and extended in order to define the ITS station reference architecture [ISO-21217], which consists of six parts Applications, Management, Access, Networking & Transport, Facilities and Security).

The six functional blocks are interconnected via Interfaces (e.g. SAPs, APIs, plug-and-play interfaces).

These interfaces need to be specified in order to allow for components of an ITS station provided by different manufacturers, and in order to support distributed implementations of an ITS station in various physical units.

The Security entity provides means to secure communications and the ITS station [CALM-ITS].

The Managmenet entity provides means to manage the ITS station.

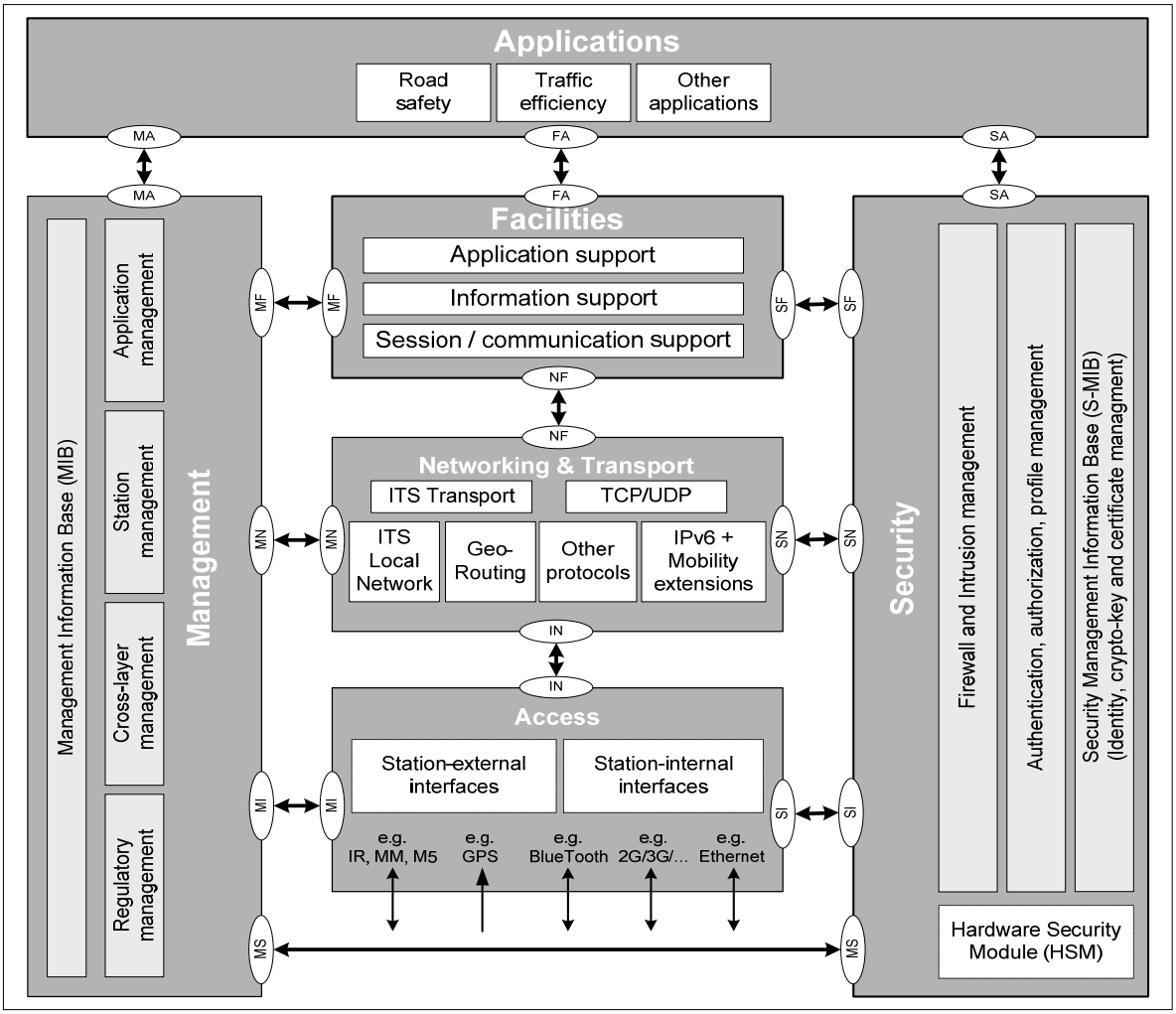
All of these are used by Applications, which contains ITS-S applications.

The six blocks are interconnected via Interfaces [ISO-24102], which may be e.g. service access points (SAPs), application programmer interfaces (APIs) or plug-and-play interfaces.

The term ITS station (ITS-S) identifies the functionality provided by these six blocks. CALM standards do not specify any ITS-S application. Therefore, CALM goes beyond communications - it considers ITS-S applications as part of the Bounded Secured Managed Domain (BSMD)

7.1.8 ITS Station Reference Architecture

Figure 19 :



Examples of possible elements in the ITS station reference architecture [EN-302665]

Figure 19 depicts Examples of possible elements in the ITS station reference architecture. ITS-S Infrastructure is light or no infrastructure is required. Hence,

- ITS-S can be installed in roadside furniture
- ITS-S can be an “app” in a smartphone [CADZOW]

7.1.9 ITS-S Security

ITS-S has a HSM element. For security evaluations ITS-S needs risk analysis per target of evaluation (TOE)

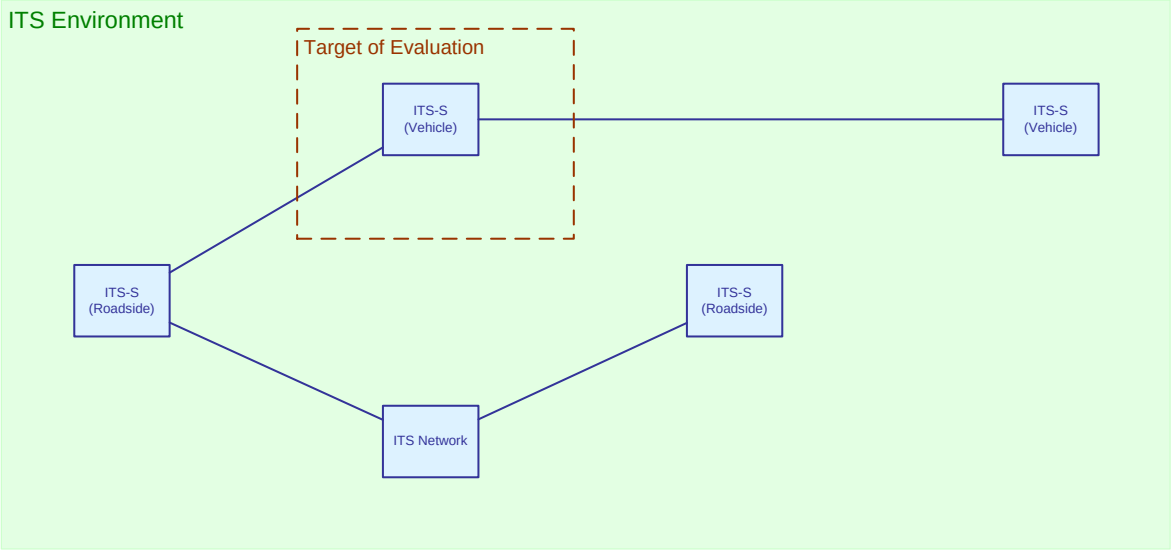


Figure 20 : ITS-S (Vehicle) as the TOE [ETSI TR 102 893]

7.1.10 Privacy in ITS

- The reason for travel is often personal
  - Leisure, work, family travels are not open for all to see and exploit
- A traveller's viewpoint is too low to see the "right path"
  - Needs help from a trusted authority with a better viewpoint
- Asking for directions is naturally a verbal/aural process
  - Often doesn't just concern the shortest/quickest route but the one that fits to the person (e.g. via this type of shop, suitable for a baby buggy, with indoor secure bike parking close to the destination, …)
- ITS-S shall not release identity or identity revealing data to unknown parties
  - Problem: no known parties (ad hoc peer to peer all informed network)
  - Suggested solution [C2CC]:
    - Sign every message but with different signing identity but common (authorisation) authority
    - Double blind identity from authority [CADZOW]

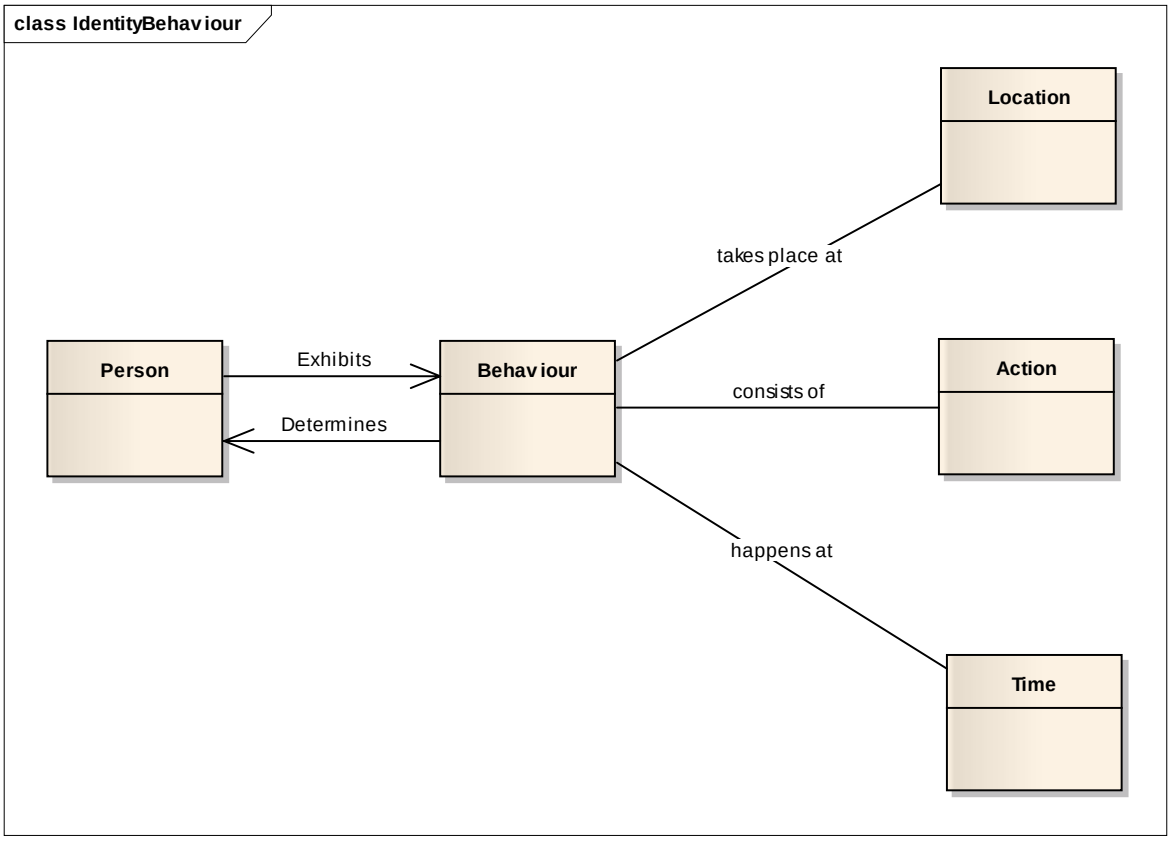


Figure 21- Identity behaviour in ITS [CADZOW]

7.1.11 Trust in ITS

Trust is developed over time from the analysis of actions, reactions, and contributions

- Requires observation and interaction over time
- Requires contextual knowledge
- Trusting party-A in context-X does not mean having to trust party-A in context-Y [CADZOW]

7.1.12 PKI and Certificates

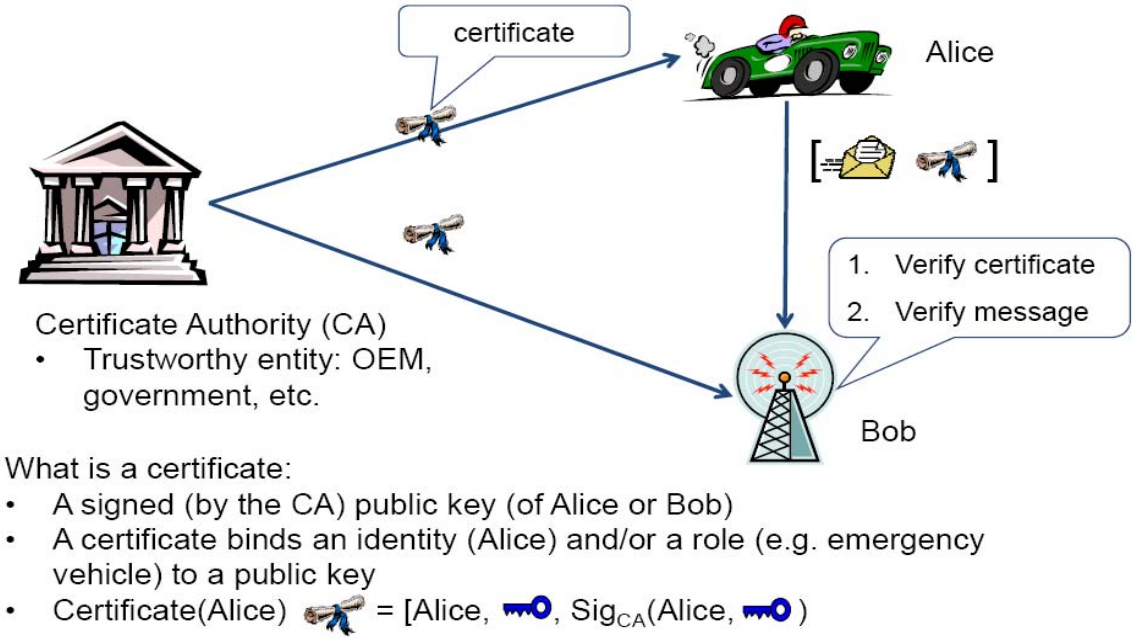


Figure 22: ITS PKI and certificates [CADZOW]

7.1.13 Certificate Authority

- CAs are the basis of PKIs
- There might be several CAs
  - Vehicle enrolment CA
  - Application specific CA (ticket authorization)
- All nodes must trust a CA
- CAs can be public and/or private
  - OEM CA
  - Verisign CA
  - European Union CA
  - National CAs
  - ...
- CAs can be designed hierarchically
  - EU root CA
  - National sub CAs [CADZOW]

7.1.14 Enrolment Authority: Example

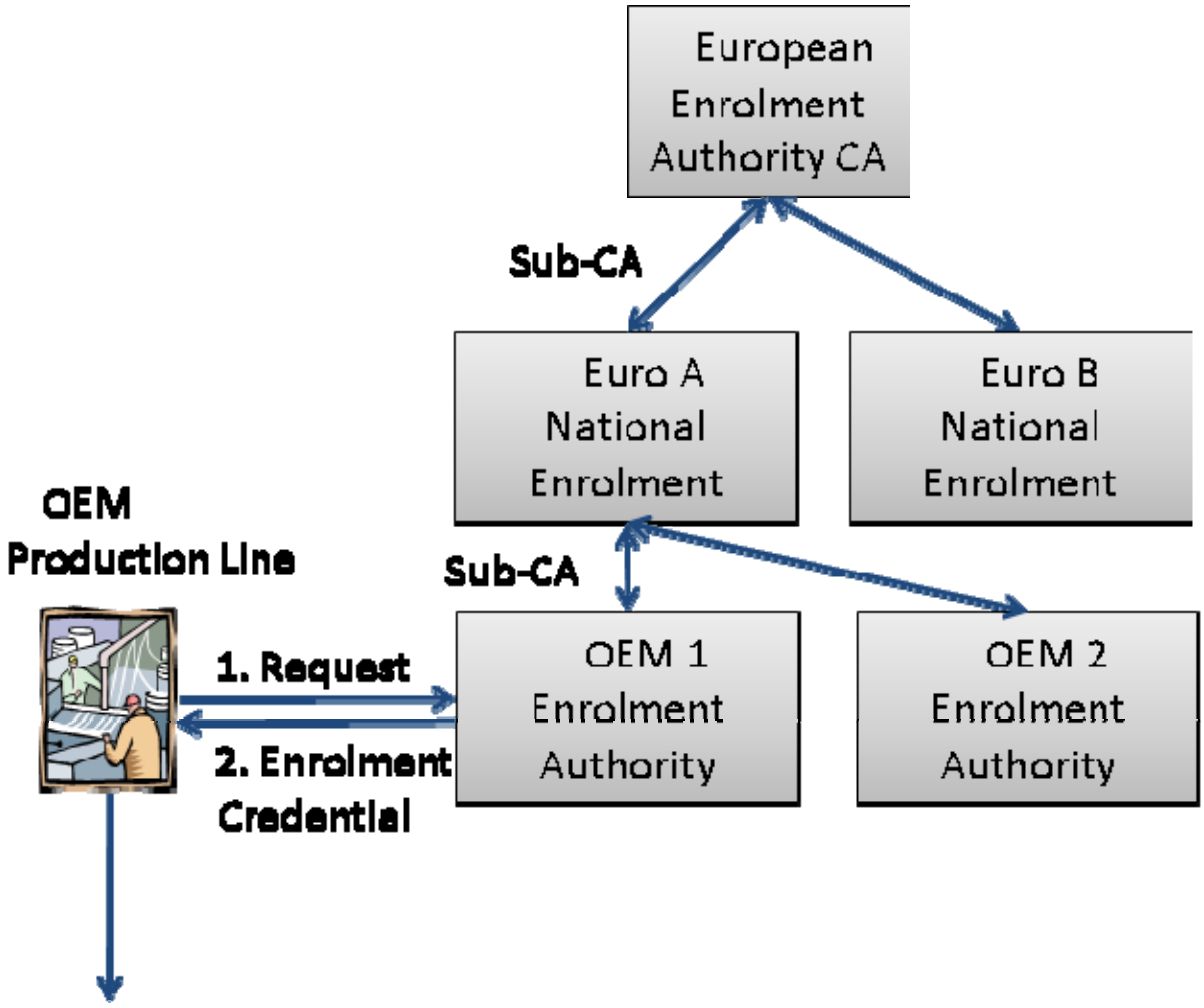


Figure 23 : Enrolment Authority: Example [CADZOW]

A revised ERCA can be a candidate to be the European Enrolment Authority CA in the Figure 23. It would be a good strategy to keep in mind ITS in the future ERCA.

7.1.15 GeoNetworking

The ITS ad hoc network shall provide the transport of [IPv6] packets enhanced by GeoNetworking [ETSI 102 636-3] for communication among ITS stations. The delivery of IPv6 packets shall be achieved by IPv6 in GeoNetworking header tunnelling, i.e. encapsulation of IPv6 packets (header and payload) into GeoNetworking packet headers and routing of the encapsulated packets by the GeoNetworking protocol. From the IPv6 layer perspective, the ITS stations should appear as attached to the same IPv6 'link'. For different communication scenarios, such for ad hoc networking among ITS stations without connectivity to a communication infrastructure or for communication with IPv6 nodes in the Internet, when access to the communication infrastructure is available, specific mechanisms for IPv6 address configuration shall be applied.

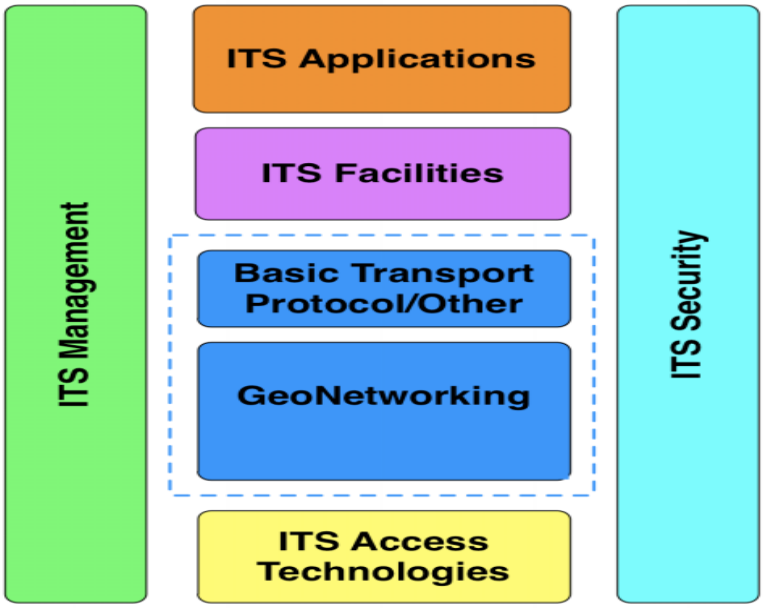


Figure 24 - GeoNetworking protocol stack in an ITS station [ETSI 102 636-3]

Geo-networking address outbound message to specific geographic location. When vehicle ITS stations have access to a communication infrastructure, IPv6 support over geoNetworking should be enhanced with solutions for IP mobility support. Those solutions achieve global reachability of IP nodes and IP session continuity.

7.1.16 ITS Station Implementations

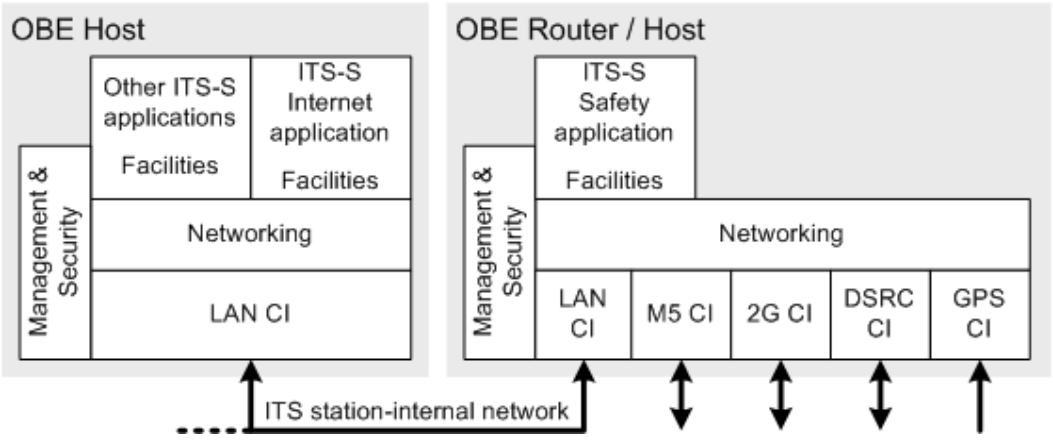


Figure 25 - ITS station implementation [CALM ITS]

In a "simple" implementation of an OBE (On Board Equipment), as e.g. used in the Cooperative Vehicle-Infrastructure Systems [CVIS] project, the whole functionality of the ITS-S is implemented in two physical units, which are interconnected via the IST station-internal network. In this example, distinction is made between an ITS-S Host and an ITS-S Router with some functionality of a host.

An ITS-S Router [ISO-21217] contains the communication interfaces and protocols needed to connect to another ITS-S unit. An ITS-S Host contains ITS-S applications.

There is station-internal management communications between these two units of the OBE as specified in [ISO-24102-3]. As the ITS station-internal network is observable, this management communications needs to be secured in order to protect the ITS-S from unauthorized manipulations, which might have an impact on the whole ITS.

IEEE 802.11p [802.11p] is an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE). It defines enhancements to 802.11 (the basis of products marketed as Wi-Fi) required to support Intelligent Transportation Systems (ITS) applications. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz). IEEE 1609 is a higher layer standard on which IEEE 802.11p is based.[IEEE 1609]

802.11p will be used as the groundwork for Dedicated Short Range Communications (DSRC)

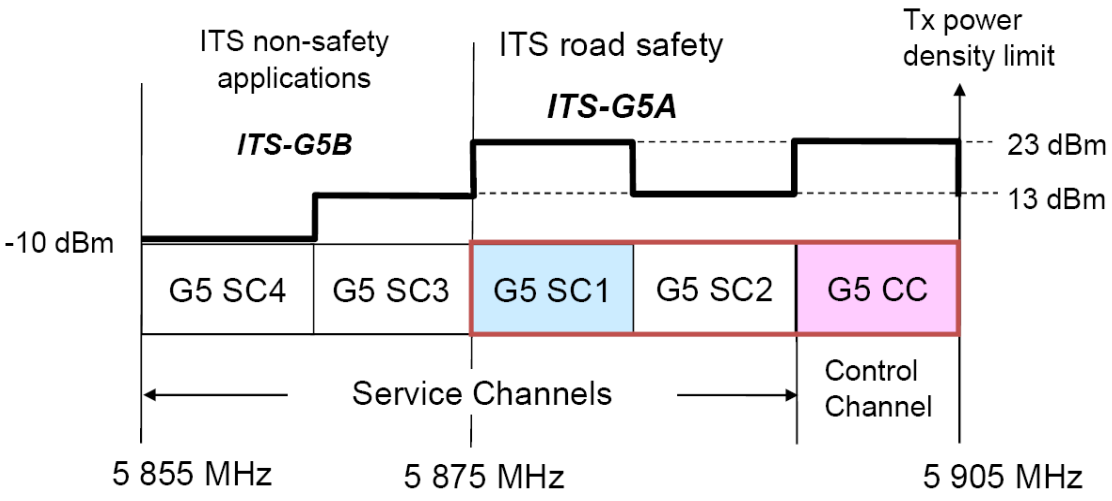


Figure 26 - Frequency allocation in the European Union [ITS WG4]

ETSI ITS-G5 is the current vehicle-to-vehicle communication technology in Europe, which will be standardized by ETSI TC ITS. It is based on IEEE 802.11p and therefore uses a CSMA/CA scheme for Media Access Control (MAC). ITS-G5A (European profile) in 5.875 GHz to 5.905 GHz frequency range.

7.1.17 C2C-CC architecture

This section is extracted from [C2C-CC Architecture]

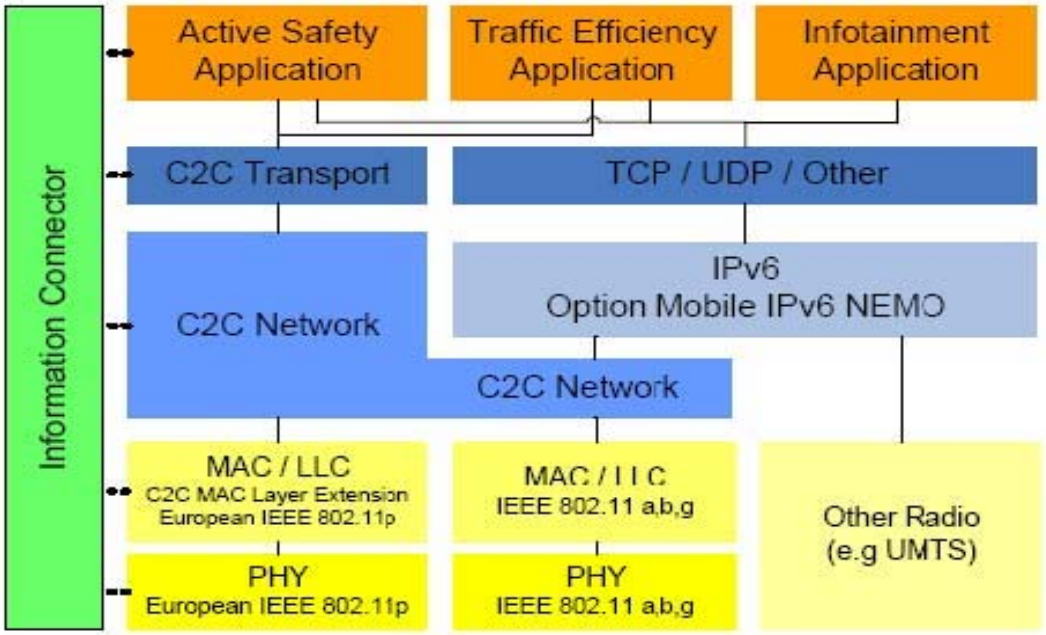


Figure 27 : C2C-CC architecture : outcomes integrated in ETSI ITS [C2C-CC Architecture]

PHY :

- OFDM mod of 802.11a
- 10MHz channels, double GI, MCS 2 for G5CC and G5SC1, MCS 4 for other G5SCs

MAC : CSMA/CA MAC + 802.11e QOS

- No more association, authentication, probe request (scan) in Management frames.
- New Timing Advertisement Management frame: (Synchronization using TSF)
- new EDCA 802.11 parameters (QoS) mapped to logical channels: CCH with optimized CW and AIFSN

Control channel

- Broadcast communication
- Dedicated to short, high-priority, data and management frames:
- Safety-critical communication with low latencies
- Initialization of two-way communication on SCH

Service channel

- Two-way communication between RSU and OBU or between OBUs
- For specific applications, e.g. tolling, internet access
- Different kinds of applications can be executed in parallel on different service channels

C2C Network Layer

- wireless multi hop communications based on geographical addressing and routing protocol
- Location table, beaconing, location service, geographical addressing, forwarding algorithms

Congestion control

- priority handling, load indication from wireless channel, transmit power control, packet discard mechanisms, data and packet rate control

CAM messages in facilities layer

- (Cooperative Awareness Messages (CAMs) distributed within the ITS-G5 (802.11p) network
- information of presence, positions, status of communicating ITS stations to neighboring ITS stations located within a single hop distance
- IPv6 stack implemented in mobile router
- Mobile IPv6 (tunneling)
- NEMO (network mobility management)
- Multi Care of address (simultaneous access networks) multihoming
- QoS for traffic prioritization

7.1.18 C2C-CC PKI Proposal

This section and all the fourth level sub sections are composed of extractions from Public Key Infrastructure Memo [C2CC PKI] of Car 2 Car Communication Consortium.

The proposed solution for a C2C PKI consists of three different, basic types of CAs (relationships depicted in Figure 28):

- Root certificate authority (RCA)
- Long-Term certificate authority (LTCA)
- Pseudonym certificate authority (PCA)

The role of the Root CA is to define common policies among all subordinate certificate issuers. The RCA only issues certificates for Long-Term CAs and Pseudonym CAs, which are valid over long periods. A certification process which needs interaction with the RCA is only required once a new LTCA or PCA is created, and when the lifetime of an LTCA or PCA certificate expires. Such a process should be standardized in order to enable an overall trustworthy usage of RCA issued certificates. It is the task of the RCA to check that the RCAs' certificate issuance policies are adhered to by LTCAs and PCAs.

If there are multiple RCAs, they may cross-certify each other. For mutual trust between Root CAs a cross certification is reasonable because it allows more flexible trust relationships between the Root CAs. However, the overall number of RCAs shall be kept as small as possible.

In the proposed solution as shown in Figure 28, a Root Certificate Authority (depicted in Figure 28 as RCA2) on a European level is proposed to be used as central trust anchor. In order to extend the solution for world-wide interoperability, all existing RCAs may cross certify each other. Every cross certification is done with two new certificates stating the mutual trust status between both Root CAs. Any other cross certification between CAs other than RCAs, i.e. between Long-term CAs and between Pseudonym CAs, is not allowed.

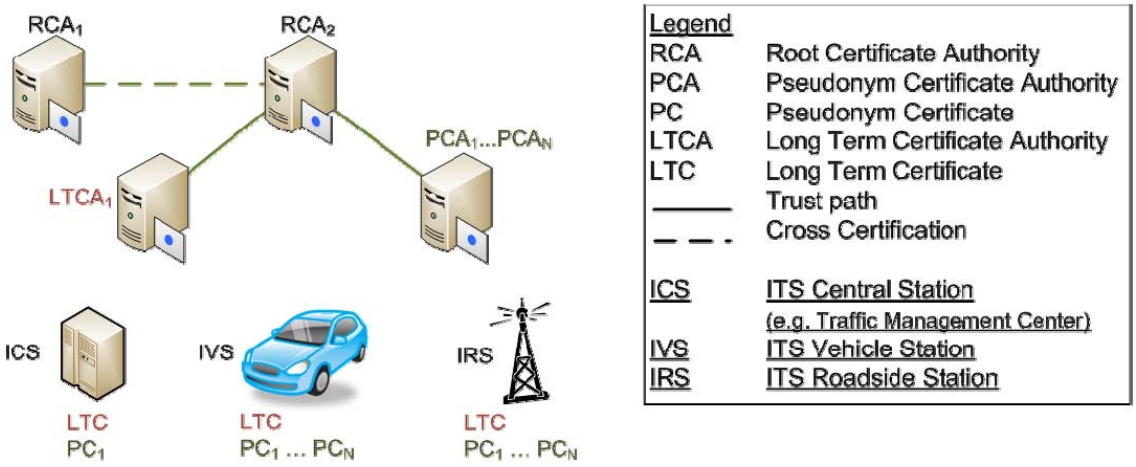


Figure 28 - Proposed PKI Structure

Based on enrolment processes at the Root CA, different institutions may be possible operators of a Long-Term CA (LTCA):

- Organisations such as the Car2Car Communication Consortium (C2C-CC)
- Original Equipment Manufacturers (OEM)
- Suppliers
- Countries
- Trusted Third Parties (e.g. After market supplier)

Every LTCA has a Long-Term CA certificate that is signed with the private key of the Root CA. With a similar process the Root CA issues Pseudonym CAs that provide afterwards valid Pseudonym CA certificates. In the proposed design only the Root CA is able to issue Long-Term and Pseudonym CAs.

Afterwards, the LTCA issues for each responsible ITS station one Long-Term Certificates (LTC), that is valid for a longer period1. Each LTC created by a LTCA is dedicated to identify and authenticate the respective ITS station within the PKI and potentially other services, but they are never exposed to the G5A communication for privacy reasons. In contrast, Pseudonym Certificates (PCs) issued by PCAs are used for the G5A broadcast communication. PCs are dedicated to have a short lifetime and are exchanged frequently.

For the long-term certification, LTCAs must provide suitable processes to associate an LTC to an ITS station, to revoke and to update it. For the provisioning of PCs, an efficient refill process is required, but it is sufficient for an ITS station to prove ownership of the private key of its LTC to acquire new pseudonyms.

7.1.18.1 Cost efficiency of a Root CA

Having a Root CA as central trust anchor the registration of new Long-Term CAs and Pseudonym CAs is more easy and cost efficient than without such a central trust anchor. It was discussed to allow independent LTCAs and PCAs and let the car manufacturer decide, which LTCAs and PCAs to add to the list of trusted CAs. However, this has the disadvantage of less comparable trust of different CAs that use different policies. Moreover, assuming several hundred Long-Term CAs are present

worldwide, a new Pseudonym CA operator has to make contractual relationships with all Long-Term CAs in order to be admitted. In such a scenario the number of contracts (and costs) is raising in a quadratic manor whereas a Root CA leads to simple linear effort. Furthermore, the distribution of updates to the vehicles containing the new list of Pseudonym CAs would be challenging if we assume vehicles may not be reachable for a longer time. For these reasons, Root CAs are proposed as a trust anchor of all other CAs (LTCA, PCA). The update or exchange of Root CAs on ITS stations is only possible if at least one Root CA certificate is still valid and can be used to sign the updates. Updates on the root layer can be assumed to be rarely.

7.1.18.2 Pseudonym Verification

Vehicles on the road receive messages very frequently from other ITS stations (other vehicles, roadside stations, traffic management centers, etc.). Verifying the integrity and authenticity of each incoming message requires to verify not only the message but also the sender's Pseudonym Certificate. Especially verifying the latter can under certain situations require up to five steps:

- If a pseudonym previously has been verified successfully then the sender's certificate can be considered authentic.
- Else if the Pseudonym Certificate signer (i.e. Pseudonym CA certificate) is known and has been verified successfully the sender's certificate can be considered authentic.
- Else if Pseudonym CA certificate is known and has been verified successfully then the sender's certificate can be considered authentic. If the Pseudonym CA certificate is not available then the Pseudonym CA certificate has to be requested from the sender as described in section 6.5.
- Else if the Root CA certificate (signer of the Long-Term CA certificate) is known and has been verified successfully then the sender's certificate can be considered authentic. If the Root CA certificate is not available then the sender's certificate cannot be authenticated.

It has to be remarked that the validity of every certificate has to be checked in every step. For optimization purposes an 8 byte signer ID (Cert-ID) is stored in all certificates. If a verified signer ID can be found in the local certificate store then only the expiry date has to be checked. As described in section 8.2 revocation of CA certificates is proposed. Therefore in every verification step the CRL has to be searched.

In this PKI concept special restrictions of specific countries or companies have been considered. Some countries may not accept Pseudonym Certificates that are distributed by foreign instances. As solution a country can operate an own Pseudonym CA that have to cooperate with the Long-Term CAs of the vehicles in order to provide Pseudonym Certificates. Such a country would be able to control privacy protection mechanisms by resolving the link between distributed PCs and the respective Long-Term Certificate. Furthermore, a regular pseudonym change can be prevented by distributing only one Pseudonym Certificate.

7.1.18.3 Initialization of ITS stations

The provisioning of the ITS Stations with the initial LTC is the task of the manufacturer. It has to be guaranteed that only valid vehicles are able to get a Long-Term Certificate. Access to the LTCA has to be protected so that only authorized entities (e.g. OEM, Supplier) are able to send requests for LTCs.

The process as depicted in Figure 29 refers to the very first Long-Term Certificate assignment after production of the C2X Security Module. It shows a possible implementation of a secure initial LTC provisioning. However, the concrete implementation of LTC provisioning is up to each OEM. The described process should be seen as a reference.

On the one hand it has to be ensured that only authenticated Security Modules are receiving a Long-Term Certificate. On the other hand only authorized Long-Term CAs shall be allowed to assign Long-Term Certificates to that Security Module. Please note that within this process we take into account that the manufacturer and Long-Term CA may be two separate entities, e.g. supplier and OEM. In principle the same process may be applied within a single entity in case the manufacturer of the security module also serves as Long-Term CA.

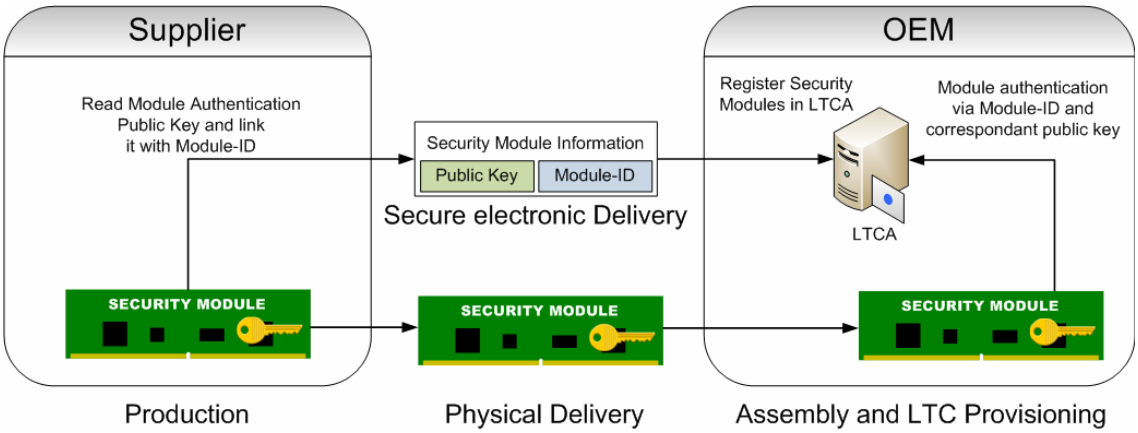


Figure 29 - Authentication Process for initial Long-Term Certificate assignment

According to Figure 29 the supplier triggers the Security Module to generate a public/private key pair. To avoid confusion with previous terminology those keys are named as Module Authentication Keys. The Module Authentication Private Key is permanently stored at the Security Module and later used for authentication towards the Long-Term CA. The corresponding Module Authentication Public Key, together with the Module-ID is delivered to the assigned Long-Term CA via a secure communication link. Once the Security Module has been delivered to the OEM, the key generation is triggered again, to produce a public/private key pair for a Long-Term Certificate. That public key is sent as part of a certificate request to the Long-Term CA, signed via the Module Authentication Private Key. The Long-Term CA is verifying the signature based on the Security Module-ID and the corresponding Module Authentication Public Key. Only if the signature verification succeeds, the Long-Term Certificate is created and stored back on the Security Module. That way only authorized security modules receive a valid Long-Term Certificate.

7.1.18.4 Update of LTCs

The update of the LTC can be similar to a Pseudonym Certificate request. The Long-Term Certificate request may be signed by the valid LTC of the requester. This process is only possible if the Long-Term Certificate is still valid and the lifetime is not expired. In the case that the LTC is expired, the OEM has to define a process that may be similar to the provisioning.

In order to update an expired or corrupted Long-Term Certificate a similar process as the initial provisioning of LTC is proposed. In general we assume that service stations (e.g. garages, car dealer, etc.) will serve as communication interface to Long-Term CAs. To issue a new Long-Term Certificate

the security module generates a new key pair and signs the public key with the Module Authentication Private Key as described before. Based on the Module-ID the service station queries the corresponding Module Authentication Public Key to perform the authentication. Please note that the old Long-Term Certificate may thereby be used to identify the former Long-Term CA for direct association. If the security module is authorized, the Long-Term Certificate is created and stored on the Security Module.

For being able to update the Long-Term Certificate at any time after the vehicle e has left the OEM's factory it is required to store all Security Module Authentication public keys in a secure storage within the Long-Term CA.

7.1.18.5 Obtaining new pseudonyms

Communication Channels for Pseudonym Requests

For retrieving new Pseudonyms a communication channel between the Pseudonym CA to be used and the ITS station has to exist. The following types of communication channels could be regarded for Pseudonym Certificate updates:

- IEEE 802.11p (e.g., via IRS)
- IEEE 802.11a/b/g consumer WLAN (e.g., via IRS or other hotspots and home networks)
- Cellular link
- On Board Diagnosis (OBD) (e.g., at Service garage, TÜV / MOT)
- Removable media (SD-Card, Smart Card, USB Stick, …)
- Wireless link (e.g., Bluetooth, IR, …)
- Wired connection at an electric charging station

General reloading process

The general process for requesting pseudonyms can be described as following.

- An ITS Station generates private and public key pairs and creates a Pseudonym request message containing the created public keys together with the senders Long-Term Certificate. The availability of a link to the Long-Term CA (e.g. IP address, ID, etc) is necessary because the Pseudonym CA may not be able to identify the used Long-Term CA by just the signer ID. Afterwards the sender signs the request with its private key of the Long-Term Certificate and sends it to the Pseudonym CA. Only the Long-Term Certificate can be used to sign the pseudonym request. Furthermore, this concept considers only the solution to generate key pairs in the vehicle. The generation of key pairs in the PCA can be kept as alternative solution, but should be used only as a backup because of slight security and privacy disadvantages.
- The Pseudonym CA sends the request to the responsible Long-Term CA which verifies the Pseudonym request with the senders Long-Term Certificate included in the pseudonym request. Subsequently the Long-Term CA notifies the Pseudonym CA if the pseudonym certificates can be created.
- In case of a positive feedback from the Long-Term CA, the Pseudonym CA creates the new Pseudonym Certificates with an appropriate expiry date and signs the certificate with its private

key. Afterwards, the Pseudonym Certificate is sent to the appropriate ITS Station over a secure communication channel.

In order to protect the driver's privacy besides the Pseudonym Certificate all identification attributes have to be changed regularly. As described in section 4, ITS Stations create key pairs locally and send the public key to the Pseudonym CA in order to get a Pseudonym Certificate. Due to different communication types as mentioned in section 6.3, we do not assume a continuous link to a Pseudonym CA. In the deployment phase of the C2C system, roadside stations will only cover a very small percentage of the road system in Europe and not all vehicles will be equipped with cellular communication technology. Therefore, we assume that a communication between vehicles and a CA may happen extremely seldom.

The Pseudonym CA is responsible for issuing Pseudonym certificates for the requester. The requester generates a number of key pairs which is not further specified. Depending on the vehicle's system performance or the available communication link only a small set of pseudonym can be requested or a large set which would cover several months. The public keys are transmitted to the Pseudonym CA for issuing. Depending on policies the PCA decides how many pseudonyms will be issued with which validity as indicated before.

The final setting of these crucial parameters determines both the security and privacy – and thus the trust – of the entire PKI. In addition, too strict parameters reduce the flexibility, e.g. for refilling the Pseudonym Certificate pool.

7.1.18.6 Refill process

As displayed in Figure 30 the vehicle sends a request to a predefined Pseudonym CA (e.g. Home PCA). This request includes the signer ID of the Long-Term Certificate, the list of public keys, the current position and an ID or address of the Long-Term CA.

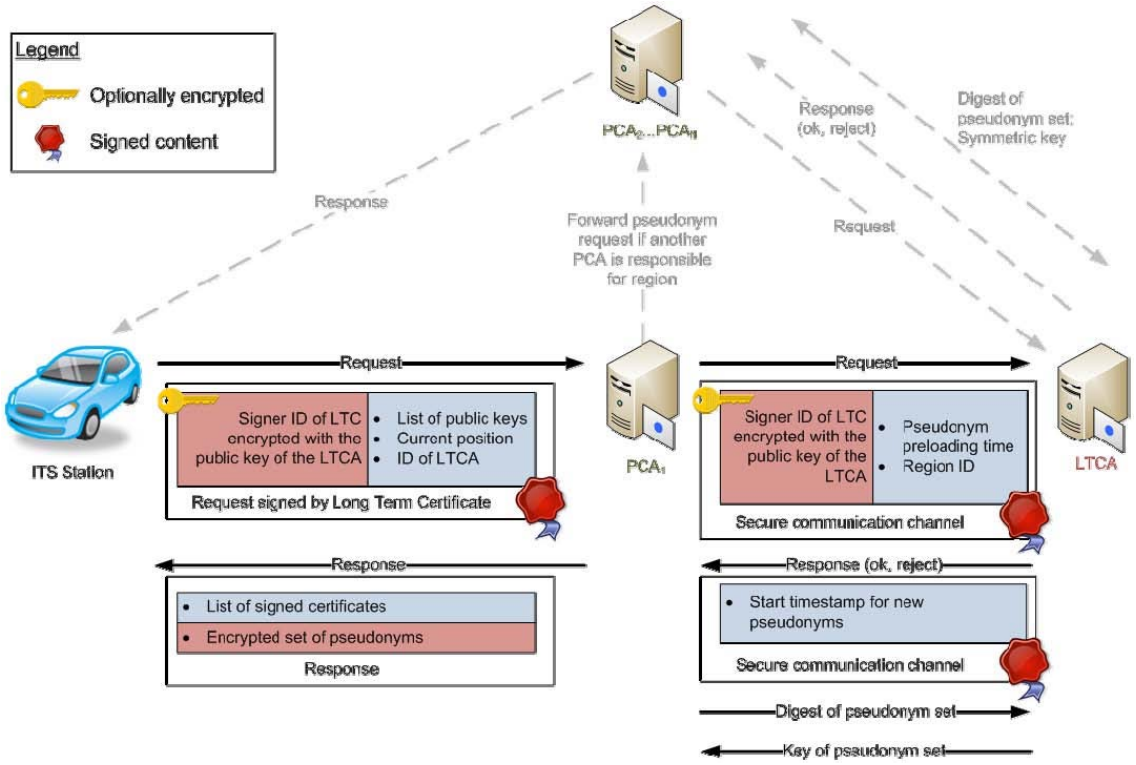


Figure 30 - Pseudonym Request

If a Pseudonym CA receives a request it checks if it is allowed to issue Pseudonyms for the request. For example, if another Pseudonym CA is responsible for the region of the requester, then the request is forwarded to the appropriate Pseudonym CA such as displayed in Figure 30.

For privacy reasons the signer ID of the sender can be encrypted with the public key of the Long-Term CA. In this case, the Pseudonym CA is not able to create a link between the pseudonyms and the Long-Term-ID of the vehicle. Also the Long-Term CA is not able to create such a link because the Pseudonym CA is not forwarding the public keys or pseudonym certificates. Based on legislation, the signer ID can also be transmitted unencrypted so that the Pseudonym CA is able to operate a database with links between the Long-Term CA and the Pseudonym Certificates.

The appropriate Pseudonym CA sends a request with the (encrypted) signer ID of the requester, a calculated preloading time and the region ID to the Long-Term CA for verification. The Long-Term CA maintains a database that stores the timestamp until a vehicle has valid pseudonyms for a distinct region. Only if the following checks are successful the Pseudonym CA gets a positive response from the Long-Term CA.

- Signer ID of LTC can be found at the LTCA and the certificate is not deactivated.
- There are no pseudonyms issued for the given region ID until the given preloading time.

The Long-Term CA sends a positive or negative response with a start timestamp for new pseudonyms back to the Pseudonym CA. With this procedure the PKI can circumvent that vehicles request pseudonyms for the same time interval from different or the same Pseudonym CA. After the creation of Pseudonym Certificates on the PCA, a digest of the pseudonym set is created and sent to the

responsible LTCA. On the LTCA a symmetric key for the pseudonym set is created, stored in the database as well as sent back to the PCA. If the requested pseudonyms are designed for usage in near future time, then the set of Pseudonyms is sent to the ITS station without encryption. Otherwise, if the pseudonyms are designed for a farther future time interval then the set is encrypted with the symmetric key received from the LTCA in order to prevent misuse.

Therefore, short connectivity over G5A for pseudonym requests can be considered because only a key has to be transmitted in order to use preloaded Pseudonym Certificates. Furthermore, the concept enables the endowment of pseudonym for farther future time intervals by restricting the number of pseudonym that can be used in the near future. In order to decrypt a pseudonym set on the ITS station it can request the symmetric key from a PCA by sending the digest of the pseudonym set as displayed in Figure 31. The PCA forwards this digest to the responsible LTCA which answers with the key if available.

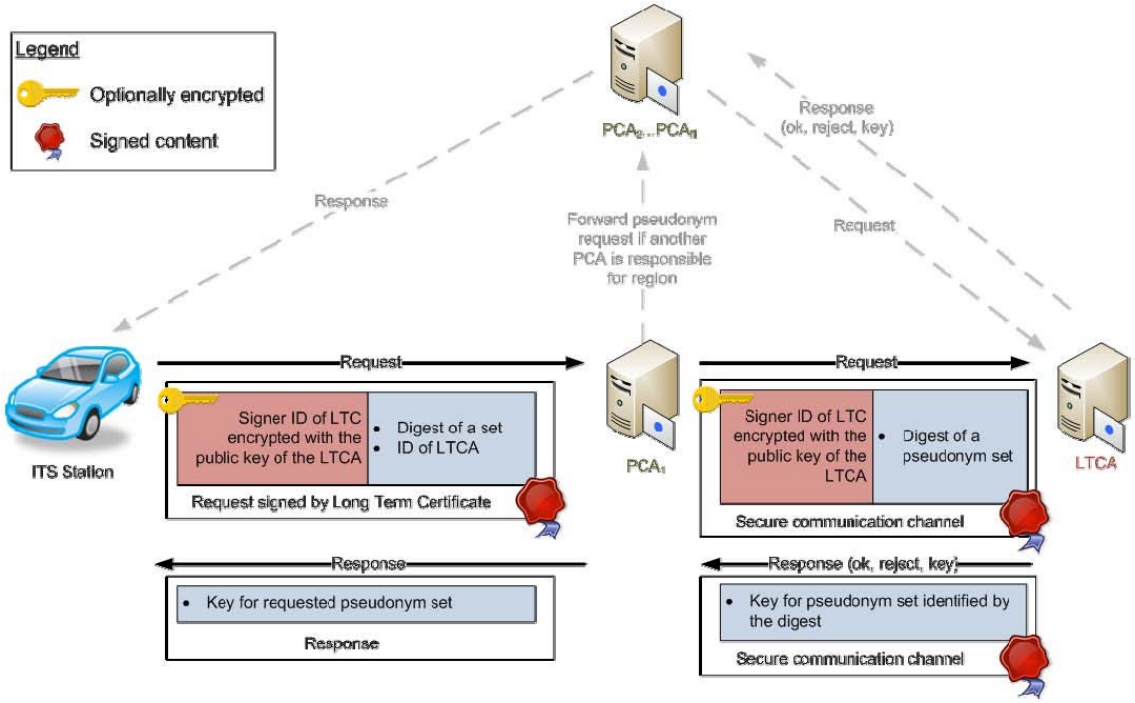


Figure 31: Request of Key in order to decrypt preloaded Pseudonyms

Also if the keys for the pseudonyms are generated on the ITS station they can only be used in the V2X communication if signed certificates are available signed by a CA. In case of encrypted Pseudonym Certificates available on the ITS station messages can be correctly signed with the private key but without an issued certificate the receiver is not able to verify the sender's authenticity.

7.1.18.7 Creation of new CAs

- There must be minimum requirements for a CA.

- Root CA could be operated by an well-respected and specialized entity for PKI and IT security, such as e.g. BSI, Euro PKI or US DOT, etc.
- The C2C-CC should suggest security guidelines in the TF-PKI that can be used by the Root CA operator.
- Policies are the result of a discussion between the C2C-CC, legislation, potential operators, etc.

7.1.18.8 Distribution of new CA certificates

In the first place, distribution of certificates of new CAs should be done over the key store update, e.g. during a reload process of new pseudonyms. Especially, new RCA certificates must only be transferred to ITS stations using the key store update process. Yet, it may happen that a vehicle has not executed an update process for a while. In such a case, if a PCA certificate in the local key / certificate store on an ITS station is not available to verify pseudonyms a decentralized mechanism is approached to retrieve it. As described in section 5.1 Pseudonym Certificates from other ITS stations will only be accepted if a verification up to a Root CA is possible.

If the receiver of a message does not have appropriate certificates to verify the certificate chain from the Pseudonym Certificate up to Root CA certificate then a new message with the Cert-ID of the missing certificate is sent via unicast to the sender. Thereupon, the receiver of this request creates a response and broadcasts the respective PCA certificate.

7.2 Introduction of mobile signature in DT

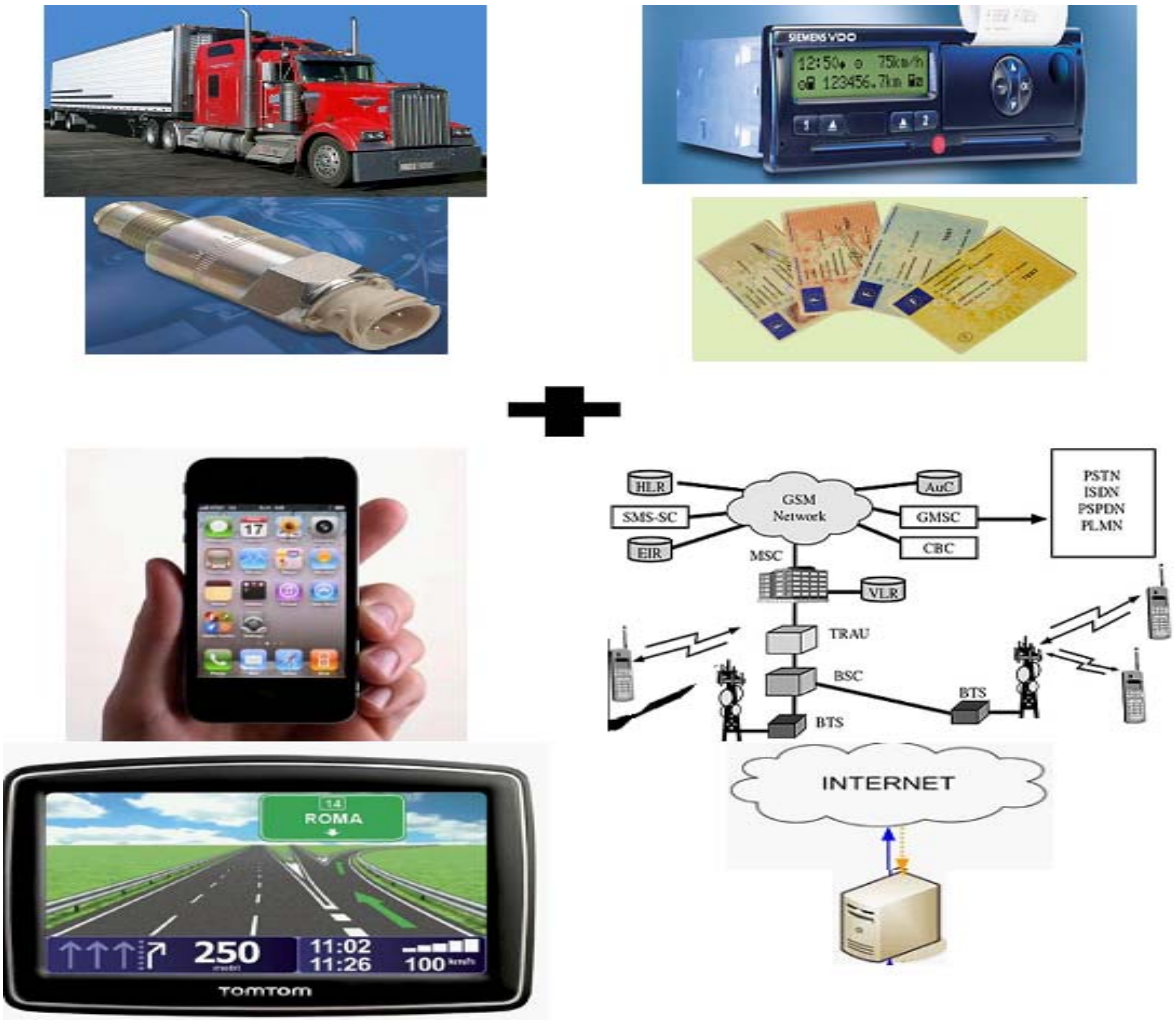


Figure 32 : Mobile signature in DTS

7.2.1 What is Mobile Signature

Mobile Signature is a service which enables the user to fulfill electronic signature processes, which is legally binding signature, in accordance with National Electronic Signature Law which is based on the EU Electronic signature directive [E-SIGN-DIRECTIVE] by using mobile phone and GSM SIM card.

“Signature creation data” of the Qualified Electronic Certificate which can be acquired only after SIM Operator Mobile Signature subscription, formed specially and uniquely to signature holder and stored in the high security area of the SimPlus128 Card.

Mobile Signature service works with the usage of signature creation data stored in the high security area along with the application stored in the same place.

Electronic signature process can be realized securely only when user enter his/her Mobile Signature password. Mobile Signature is used on the SIM card and cannot be sent to anywhere else.

According to the national electronic signature legislation, electronic signature holder's security concerning the signature shall be guaranteed. The related technical infrastructure and the security of the operations are supervised and certified periodically in accordance with ISO/IEC 27001 Information Security Management System standards by independent bodies, e.g., BSI.

The SIM Card that is compatible with Mobile Signature is certified with the highest security CC EAL4+ Security Certificate as required by the related legislations. It is solid against the most advanced attacks. The signature creation data in the card can under no circumstance be copied.

Electronic signature is generated when the user enters his/her Mobile Signature password to the SIM card via their mobile phone's keypad. Thus the messages received or sent are directly addressed to the SIM card and they are stored in the SIM card.

7.2.2 Introduction of Mobile Signatures into DTS

Although Mobile Signature application in DTS needs to be further investigated for a precise proposal, the process can be summarized in the following steps:

- Drivers can authenticate to a central server with a mobile signature through their mobile phones over GSM network.
- The mobile signature is generated on the data: "Driver ID + truck ID + GPS Unit ID + GPS location + GSM time + start indication"
- Driver authenticates to the server when his/her signature is verified on the server.
- GSM and GPS provides speed and location information to the server until the driver sign out from the server by sending mobile signature on the data: "Driver ID + truck ID + GPS Unit ID + GPS location + GSM time + stop indication"
- Driver is signed out from the server when his/her signature is verified on the server.
- The position information is provided by GPS is double checked on the server with the position information provided by GSM
- Public key certificates will be issued by the member state CAs to the drivers rather than the tachograph equipment.
- The key generation on the SIM card and activation of the mobile signature service is provided by a certification authority in agreement with a GSM operator.
- ERCA as the top level authority remains as as the European root CA. Member state CA's provide public key certification service to the persons through a GSM operator.
- Drivers subscribe to a mobile operator for tachograph application on their SIM cards, or the application can be loaded to the SIM card by an online service.
- The mobile digital signatures will comply with the EU electronic signature law.
- Security update of the Mobile Signature enabled tachograph system will be easier as the application on the SIM card will be flexible for updates.
- Public key certificate revocation will be possible as the system will be online.

8 Conclusion

In order for the DTS to be more secure and less vulnerable to threats it must be fully adapted to more standardized technologies.

The technology is developing very fast and as a result the algorithms used in DTS become obsolete. Therefore the DTS must be revised to make it adaptable to new technologies and standards. The advantages of using standardized schemes will be numerous: more interoperability of the system with other systems, availability of off-the-shelf products, easier maintenance and higher system security.

DT security model should recognize that we are dealing with the ERCA/DT as a closed system which hence may face a different scale of risk threats than an open system. Consequently for the update of the system security, e.g., the impact of increasing the key length, must be evaluated according to the closed system.

A generic protection profile which defines abstract functionality including the migration concept for DT, as the flexibility to update the security in DT is crucial, is needed.

An Algo paper "The crypto in demand " for the DT closed system which is revised in certain intervals of time, e.g., every 5 years, is also needed. The Algo paper shall contain detailed information regarding the use of a certain cryptographic algorithm with certain parameters, e.g., key length, for a certain interval of time. The Algo paper could be an appendix to the abstract Protection Profile.

Intelligent Transport Systems (ITS) can be the address of the research on the future Digital Tachograph system. The idea of expansion of Digital Tachograph to ITS must be investigated for that purpose.

During the DT revision process towards the next generation Digital Tachograph, it must be kept in mind that ITS could replace DT in a decade. Working on a generic protection profile for DT which allows eventual expansion to ITS could facilitate the future developments in DT to converge to ITS.

Evolution of ERCA towards a Root CA as central trust anchor for ITS should also to be considered in the research for the future DTS.

The idea of using mobile signature as an alternative solution in the future DTS should be given a chance for further investigation of the idea as it can simplify the management of the system and its infrastructure.

9 Acknowledgements

I would like to thank Stephan LECHNER Institute for the Protection and Security of the Citizen – IPSC director for the opportunity to have a wonderful experience in JRC.

This report would not have been possible unless I have received valuable support from my colleagues and my supervisors.

I am grateful and I owe my deepest gratitude to Mr. Jean Pierre Nordvik for his support.

I am grateful to Dr. James Bishop for his generosity allocating his time to help me implementing Conclusion tachograph card test cases on Java card simulations for analysing the impact of Digital Tachograph security mechanisms. I have learned from Dr. Bishop the Digital Tachograph PKI architecture and its implementation. I owe my deepest gratitude to Dr. Bishop for learning from him the Digital Tachograph Regulation and related standards.

It is a pleasure to thank those who support me with their ideas and guidance.

It is an honor for me to have worked with Mr. David Shaw with whom I had many discussions about PKI. I learned from him about the weaknesses of several PKI applications.

I would like to thank Dr. Vincent Mahieu for his support and availability to share my views and his positive and professional approach.

I would like to thank Mr. Jan Loeschner for his support. He has made available his support in a number of ways. He encouraged me to participate Smart Event Workshop, he supported me with technical contacts about Smart Card programming.

I would like to show my gratitude to Mr Dominique Landat for his support about Interoperability tests.

I am indebted to many of my colleagues to support me with their views and guidance. I have learned a lot from Mr. Stephan Scheer, Ioannis Kounelis, Pasquale Stirparo.

I am grateful having the opportunity to have worked for the Institute for the Protection and Security of the Citizen, Joint Research Center of the European Commission.

References

[ERCA POLICY] The Digital Tachograph System European Root Policy, Version 2.1, Administrative Agreement 17398-00-02(DG-TREN), European Commission

[DT REGULATION] 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 I B, Requirements for Construction, Testing, Installation and Inspection.

[UNECE] United Nations Economic Commission for Europe

[Automotive IT] "Embedded Security in Cars: Securing Current and Future Automotive IT Applications" by Kerstin Lemke, Christof Paar, Marko Wolf, Springer-Verlag Berlin Heidelberg - Jan 2006

[NIST-SP800-67] NIST Special Publication 800-67 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher.

[DT VULNERABILITIES WORKSHOP] PROCEEDINGS of the 1st Working Group Meeting on the Vulnerabilities and limitations of the Digital Tachograph. Authors : James Bishop, Mehmet Colak, Dominique Landat, Vincent Mahieu, Jean-Pierre Nordvik. JRC technical note n°57046 - JRC Ispra - 20-21 January, 2010

[ISO-7816-8] ISO/IEC 7816-8 Identification cards — Integrated circuit cards — Part 8: Commands for security operations

[HENNIGER] O. Henniger, K. Lafou, D. Scheuermann, and B. Struif, "Verifying X.509 Certificates on Smart Cards", World Academy of Science, Engineering and Technology 22 2006

[E-SIGN-DIRECTIVE] Directive 1999/93/EC of the European Parliament and of The Council of 13 December 1999 on a Community framework for electronic signatures

[CWA14890-1] Application interface for smart cards used as Secure Signature Creation Devices – Part 1: Basic requirements, CEN Workshop Agreement CWA 14890-1, 2004

[X509] Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, ITU-T Recommendation X.509, 2000

[ISO-16844-3] ISO / IEC 16844-3 Road vehicles –Tachograph systems – Part 3: Motion sensor interface

[DT PKI] PKI Considerations for the next generation Digital Tachograph (Colak et al. 2011)

[WIKIPEDIA] http://en.wikipedia.org/wiki/Intelligent_transportation_system

[ECC Decision] ECC Decision of 14 March 2008 on the harmonised use of the 5875-5925 MHz frequency band for Intelligent Transport Systems (ITS)

[ISO-24102-3] ISO/NP 24102-3 Intelligent transport systems -- Communications access for land mobiles (CALM) -- ITS station management -- Part 3: Service access points

[IEEE 1609] IEEE 1609 -Family of Standards for Wireless Access in Vehicular Environments (WAVE)

[C2CC PKI] Car 2 Car Communication Consortium Public Key Infrastructure Memo

[ETSI ITS] http://www.etsi.org/website/Technologies/IntelligentTransportSystems.aspx

[H.J. Fischer] H.J. Fischer, Inside architecture, outside architecture, WG2 activities, Joint development of standards for Cooperative ITS International Harmonization, 3rd ITS Workshop, 2011, Venice

[ISO-21217] ISO 21217:2010 Intelligent transport systems -- Communications access for land mobiles (CALM) – Architecture

[CALM-ITS] http://calm.its-standards.info/Public/CALMintroduction.html

[ISO-24102] ISO/NP 24102-2 Intelligent transport systems -- Communications access for land mobiles (CALM) -- ITS station management -- Part 2: Remote management

[ETSI 102 636-3] ETSI TS 102 636-3 V1.1.1 (2010-03) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architecture

[C2C-CC Architecture] B. Villeforceix, Communications in ITS for cooperative systems deployement,,Orange Labs Networks and Carriers Stephane Petti International M2M Center, Orange Business Services Fully Networked Car Conference 2-3 March 2011 -Geneva

[DT VULNERABILITIES] JRC56242 Report on the vulnerability and controllability of the digital tachograph, May 2010

[SECURITY ATTACKS TO DT] Report on the attacks to security of the Digital Tachograph and on the risk associated with the introduction of adaptors to be fitted into light vehicles

[CADZOW] S. Cadzow, ITS – Harmonisation with DT How PKI requirements merge, “Future of the Digital Tachograph System Security” meeting,March 2012, JRC-ISPRA

[GIESSMANN] E. Giessmann, Tachograph Algo Update, “Future of the Digital Tachograph System Security” meeting, March 2012, JRC-ISPRA

[CORTE] CORTE CARD 006 2011 Merging driver licences and tachocards, 2011

[ISO-9796-2] ISO/IEC 9796-2 Information technology -- Security techniques -- Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash function

[PKCS 1.5] RFC 2313, PKCS #1: RSA Encryption Version 1.5

[PKCS 2.1] RSA Laboratories, PKCS #1 v2.1: RSA Cryptography Standard

[ISO-9796-2002] ISO/IEC 9796-2:2002 Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms

[ETSI TR 102 893] ETSI TR 102 893 V1.1.1 Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)

[EN-302665] ETSI EN 302 665 V1.1.1 Intelligent Transport Systems (ITS); Communications Architecture

[C2CC] Armknecht et all., 2007, Cross-layer Privacy Enhancement and Non-repudiation in Vehicular Communication, 4th Workshop on Mobile Ad-Hoc Networks (WMAN), Bern, Switzerland, March 2007

[IPv6] RFC 2460 Internet Protocol, Version 6 (IPv6) Specification

[CVIS] http://www.cvisproject.org/

[802.11p] 802.11p-2010 - IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments

[ITS WG4] WG4 STANDARDIZATION ACTIVITIES, Achim Brakemeier, Daimler AG, ETSI TC ITS WG4 Vice-Chairman, ETSI TC ITS WORKSHOP, 09-11 February 2011 • Venice • Italy

European Commission
EUR 25663 EN– Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: **Cryptographic security mechanisms of the next generation digital tachograph system and future considerations**

Authors: Mehmet Colak, James Bishop, Jean Pierre Nordvik, Vincent Mahieu, Jan Loeschner

Luxembourg: Publications Office of the European Union

2012 – 67 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424 (online), ISSN 1018-5593 (print),

ISBN 978-92-79-27990-4 (pdf)
ISBN 978-92-79-27991-1 (print)

doi:10.2788/74093

Abstract

JRC is in the process of evaluating the impact of update of the cryptographic security mechanisms for the next generation Digital Tachograph.
The purpose of this document is to give background information about the cryptographic security mechanisms and vulnerabilities regarding the security mechanisms of the current Digital Tachograph System along with suggestions for the next generation Digital Tachograph security mechanisms.
This document can be referred as an important reference to update the technical appendixes of the Tachograph regulation and alternative considerations for the future of the system.

LB-NA-25663-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new standards, methods and tools, and sharing and transferring its know-how to the Member States and international community.

Key policy areas include: environment and climate change; energy and transport; agriculture and food security; health and consumer protection; information society and digital agenda; safety and security including nuclear; all supported through a cross-cutting and multi-disciplinary approach.

ISBN 978-92-79-27990-4

Publications Office