TACHOGRAPH CARD ISSUING GROUP SWG 3

EUROPEAN DIGITAL TACHOGRAPH COMMON SECURITY GUIDELINE

VERSION 1.0
5 NOVEMBER 2002

CONTENTS

1. Introduction

1.1 Background

Regulation CCE n° 3820/85 harmonises the social regulations applicable to road transport at European level, placing a focus upon drivers' working hours.

Controls applied by the regulation are based mainly on requirements to record and store data about driver and vehicle activities.

European regulation 3821/85, in its technical annex 1B, defines tachograph equipment i.e. equipment that records and stores driving data.

It recognises that any large-scale fraud or falsification perpetrated on this equipment would enable drivers or enterprises to circumvent directive 3820/85.

European regulation [2135/98] introduces a new concept of tachograph based upon the electronic recording of driving data, and utilising three components:

- Tachograph cards
- Vehicle Unit
- Motion Sensor

The introduction of the new tachograph needs to include security features that dissuade and protect against fraudulent activity and thereby give positive support for:

- social regulations,
- road safety,
- harmonious compliance between enterprises.

Security is therefore an important factor for the system.

1.2 Scope

It is the responsibility of each Member State to set up the means of guaranteeing the security of this new system. Each Member State is therefore required to define its own tachograph organisation and to establish its own national security policy containing the security requirements for each entity involved within its organisation.

This document is a framework to which Member States are advised to refer when defining their organisation and developing their security policies. Compliance with this document is considered by the Member States and the Commission to be an acceptable proof of being in accord with the regulation when asking the European Root Certification Authority for certification of Member State keys.

This compliance underpins the need for consistency across Member States if confidence in all tachograph systems is to be inspired.

This security guideline is inspired by the standard ISO 17799 “Information technology –code of practice for information security management” and ESTI 102042 “Policy requirements for certification authorities issuing public key certificates”.

The system security architecture defined in this document must be understood as a generic and modular scheme that allows compliance with the different implementations and organisations that will be chosen by Member States.

1.3 Document content

The security requirements defined in annex 1B with a focus on the environment of the system products (Tachograph Card, Vehicle Unit, Motion Sensor) and the legal requirements (European directives 95/46) are presented in chapter 2.

The system security architecture is described in a third chapter and focuses upon the different entities of the system, their inter-relationships and the sensitive information exchanged.

The general security principle is presented in a chapter 4 in a set of recommendations derived from the ISO 17799 standard and presented in the context of the Tachograph system.

The specific security requirements, security architecture and the recommendations framework for the security policy of each entity are presented in a fourth chapter.

In the annexes, the sensitive assets inventory, the rational between the security requirements and the entities, the main item of the ISO 17799 and ETSI standard are listed.

1.4 Origin of the document

This document has been provided by the EU member states representatives in the framework of the card issuing working group partly granted by the commission and coordinated by Urba 2000.

1.5 Holder of the document

The Commission holds this document.

1.6 Revision

Member States can submit proposals for modifications to the Commission. The Commission will inform the other Member States of the proposed modifications. If necessary, the Commission shall arrange a meeting of Member States representatives to consider revisions of the document.

1.7 Abbreviations

CA	Certification Authority
CB	Control Body
CBC	Control Body card
CIA	Card Issuing Authorities
CID	CardHolder Identification Data
CKG	Card Key Generation
CM	Card manufacturers
CP	Card Personalisers
CR ID	Certificate Request identification
DC	Divers Card
EQT.C	Equipment Certificate (for card or vehicle unit)
EQT.PK	Equipment Public Key (for card or vehicle unit)
EQT.SK	Equipment Secret Key (for card or vehicle unit)
ERCA	European Root Certification Authority
EUR.PK	European Public Key
EUR.SK	European Secret Key
IDE	Intelligent Dedicated Equipment
IT	Information Technology
KPG	Kp Generation (pairing key)
MO	MOtion sensor
MOM	MOtion sensor Manufacturers
MS	Member State
MSA	Member State Authority
MS.C	Member State Certificate
MS.PK	Member State Public Key
MS.SK	Member State Secret Key
MSCA	Member State Certification Authority
PKI	Public Key Infrastructure
RE	Recording Equipment
RHC	Road Haulage Companies
RHCC	Road Haulage Companies Card
RSA	Rivest, Shamir, Adelmann (asymmetric encryption scheme)
TC	Tachograph Card
TDES	Triple DES (Date Encryption Standard)
TS	Tachograph System
VU	Vehicle Unit
VUKG	Vehicle Unit Key Generation
VUM	Vehicle Unit Manufacturers
W	vehicle manufacturers, fitters or Workshops
WC	Workshops card

1.8 Definitions

Control Body	Control authorities who take charge of checking the driver activities data
Card Issuing Authorities	Entities which manage card holders and issue Tachograph cards (In annexe 1B term "card issuing Member State code" is used)
Card Key Generation	Entities which generate the RSA key pair for the card (Card.SK and card.PK)
CARD Manufacturers	Entities which manufacture Tachograph cards with the integrated circuit and the embedded software
CARD Personalisers	Entities which personalise Tachograph cards with card holders identification data, keys and certificates (In annexe 1B " term card Personalisers ID" is used)
Drivers	Vehicle drivers whose activity must be checked
Driver Activities Data	Data regarding driver activities recorded for checking purposes (included vehicle data).
European Root Certification Authority	The authority designed by the commission for European keys creation (management), for certifying the Member State keys and distributing the certificates
KP Generation	Entities which generate the TDES paring key (Kp) for the motion sensor (description in ISO/CD 16844-3.8 motion sensor interface)
Member State Authority	The authority designated by a Member State to have responsibility for the tachograph system security within its jurisdiction
Member State Certification Authority	The authority designated by the Member State Authority for Member State key creation (management), for certifying the equipment and card keys and for distributing the certificates (CSM_008)
Motion sensor	The part of the recording equipment that provides the signal representing speed and distance travelled
Motion sensor manufacturers	Entities which manufacture/repair motion sensor equipment and "personalise" them with data

Security Label	An attribute given to a sensitive asset to allow "partitioning" of information, such that relevant "partitions" may be accessed by only those who need such access to carry out their work.
Sensitive assets	Information or products which, if their confidentiality, availability or integrity is infringed, will result in a compromise of tachograph system security
Recording Equipment	The recording equipment defined in [annex 1B] and consisting of the vehicle unit and motion sensor
Road Haulage Companies	Entities that operates vehicles (MS, VU) and whose activity must be checked
Smart card	Credit card sized plastic card which has a non volatile memory and a processing unit embedded within it
Tachograph Card	A Smart card carrying the application intended for use with the recording equipment, and defined in [annex 1B]
Tachograph System	The equipment, people and organisations involved in any way with the recording equipment and tachograph card.
Vehicle manufacturers, fitters or Workshops	Entities that provide installation and calibration of the equipment (MS, VU) in the vehicle
Vehicle Unit	The recording equipment unit consisting of all the relevant hardware and software except the sensor and the cables
Vehicle Unit Key Generation	Entities which generate the RSA key pair for the vehicle unit (VU.SK and VU.PK)
Vehicle Unit Manufacturers	Entities which manufacture/repair vehicle unit equipment and "personalise" them with keys and certificates

1.9 References

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991.
IC PP	Smartcard Integrated Circuit Protection Profile – version 2.0 – issued September 1998. Registered at French certification body under the number PP/9806.
ES PP	Smartcard Integrated Circuit With Embedded Software Protection Profile – version 2.0 – issue June 99. Registered at French certification body under the number PP/9911.
Annex 1B	Annex 1B of the council Regulation (EEC) n° 3821/85
2135/98	Council Regulation (EEC) n° 3821/85 of 20 November 1985 modified, about the control system in the road transport domain.
95/46/CE	Directive 95/46/CE of the European Council & Parliament on the principle of protection of physical persons face to treatment of personal data and free circulation of these data
ISO 17799	Information technology –code of practice for information security management First edition 2000-12-01
ISO/CD 16844-3.8	WD 16844-3.8 “Road vehicles – Tachograph systems – part 3: Motion Sensor Interface
ETSI 102 042 V1.1.1	Policy requirements for certification authorities issuing public key certificates

2. Tachograph system security requirements

These security requirements issued from European legislation concern all organisations and people involved in the Tachograph system. Part of these requirements issued from regulation 2135/98 (see point three) have been defined after a risk analysis stated in the security targets of Tachograph card, Vehicle Unit and Motion Sensor.

1) Member State must ensure that organisations in their jurisdiction satisfy security requirements defined in:

    - European directive [95/46/CE] relating to the protection of persons in respect to treatment of their personal data, and the transmission of these data,
    - European regulation [2135/98] of 20 December 1985 modified, about control systems in the road transport domain.

2) In accordance with European regulation [2135/98] and with agreed standards and interpretations for implementation, security measures set-up by the different organisations involved in tachograph system must comply with the following requirements:

    - Article 5 (extract): The system's security must comply with the technical requirements laid down in annex IB.

      The Commission, acting in accordance with the procedure laid down in article 18, shall ensure that the said Annex stipulates that recording equipment may not be granted EC component type-approval until the whole system (the recording equipment itself, driver card and electrical gearbox connections) has demonstrated its capacity to resist attempts to tamper with or alter the data on driving times. the tests necessary to establish this shall be carried out by experts, familiar with up to date tampering techniques.

    - Article 12 (extract): Member States shall take any measure necessary to prevent the cards distributed to approved fitters and workshops from being falsified.

    - Article 14 point 4f : Member States take all necessary measures to prevent any possibility of driver cards being falsified.

    - Requirement 182 of Annex 1B: In order to achieve the system security, the tachograph cards shall meet the security requirements defined in the tachograph cards generic security target (Appendix 10).

    - Requirement 012 of Annex 1B: In order to achieve the requisite system security, the recording equipment shall meet the security requirements specified in the motion sensor and vehicle unit generic security targets (Appendix 10).

- Requirement 270 of Annex 1B: Type approval of MS, VU and TC shall include security related tests, functional tests and interoperability tests. Positive results to each of these tests are stated by an appropriate certificate.

- Requirement 288 of Annex 1B: The type approval authority of the Member State may deliver the type approval certificate as soon as it holds the three required certificates

3) In compliance with appendix 10 of Annex 1B, security measures set up by the different organisations involved in tachograph systems must comply with the following requirements:

M.Activation	Vehicle manufacturers and fitters or workshops must activate the VU after its installation and before the vehicle leaves the premises where installation took place.
M.Approved_Workshops	Installation, calibration and repair of recording equipment must be carried by trusted and approved fitters or workshops.
M.Card_Availability	Tachograph cards must be available and delivered to authorised persons only.
M.Card_Traceability	Card delivery must be traceable (white lists, black lists), and black lists must be used during security audits.
M.Controls	Law enforcement controls must be performed regularly and randomly, and must include security audits.
M.Delivery	Motion sensor (resp. VU) manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of the motion sensor (resp. VU) is done in a manner which maintains IT security.
M.Development	Motion sensor (Resp VU) developers must ensure that the assignment of responsibilities during development is done in a manner which maintains IT security.
M.Driver_Card_Uniqueness	Drivers must possess, at one time, only one valid driver card.
M.Faithful_Calibration	Approved fitters and workshops must enter proper vehicle parameters in recording equipment during calibration.
M.Faithful_Drivers	Drivers must play by the rules and act responsibly (e.g. use their driver cards, properly select their activity for those that are manually selected, …).
M.Manufacturing	Motion sensor (resp VU) manufacturers must ensure that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security, and that during the manufacturing process the motion sensor (resp. VU) is protected from physical attacks which might compromise IT security.
M.Mechanical_Interface	Means of detecting physical tampering with the mechanical interface must be provided (e.g. seals)
M.Regular_Inpections	Recording equipment must be periodically inspected and calibrated.

M.Sec_Data_Generation	Security data generation algorithms must be accessible only to authorised and trusted persons.
M.Sec_Data_Transport	Security data must be generated, transported, and inserted into the motion sensor (Resp VU), in such a way to preserve its appropriate confidentiality and integrity.
M.Software_Upgrade	Software revisions must be granted security certification before they can be implemented in a motion sensor (resp VU).
O.DLV_DATA	The Application Data must be delivered from the Smart card embedded software developer (phase 1) either to the IC Packaging manufacturer, the Finishing Process manufacturer or the Personalisers through a trusted delivery and verification procedure that shall be able to maintain the integrity and confidentiality of the Application Data.
O.TEST_OPERATE	Appropriate functionality testing of the TOE shall be used in phases 4 to 6. During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.
O.USE_DIAG	Secure communication protocols and procedures shall be used between the Tachograph card and the card reader terminal.
O.USE_SYS	The integrity and the confidentiality of sensitive data stored / handled by the system (terminals, communications...) shall be maintained
O.EnvICESPP_CM	The other physical, personal or procedural requirements upon environment that contribute to the security of tachograph card which are listed in [IC PP] and [ES PP] (chapters security objectives for the environment) and concern the card manufacturers. See annexe B of this document for more detail.

3. Tachograph system security architecture

The security functions and mechanisms specified in the Appendices 10 and 11 of Annexe 1B for this system need an environment mainly made up of:

- a three-level Public Key Infrastructure (PKI): a European level, a Member State level and an equipment level. The two last levels are under the supervision of the respective Member State.
- Member State centres for cards management and issue.
- Member State workshops for installation and calibration of the recording equipment
- Member State control systems for driver activities data.

3.1 Tachograph system entities definition and role

The system security architecture defined in this document must be understood as a generic and modular scheme that allows compliance with the different implementations and organisations that will be chosen by Member States.

The system security architecture is then described as a set of logical entities that could be for each of them implemented as an organisational entity or a part of an organisational entity depending on each member state scheme. For example CKP and CP could be implemented in two different organisational entities or in the same organisational entity.

The logical entities relating to the security system are listed below from ERCA to cardholder following the system data-flow :

Logical entity	Description
European Root Certification Authority (ERCA)	The authority designed by the commission for European keys creation (management), for certifying the Member State keys and distributing the certificates
Member State Authorities (MSA)	The authority designated by a Member State to have responsibility for the tachograph system security within its jurisdiction
Member State Certification Authority (MSCA)	The authority designated by the Member State Authority for Member State key creation (management), for certifying the equipment and card keys and for distributing the certificates
CARD manufacturers (CM)	Entities which manufacture Tachograph cards with the integrated circuit and the embedded software
Card Key Generation (CKP)	Entities which generate the RSA key pair for the card (Card.SK and card.PK)
CARD Personalisers (CP)	Entities which personalise Tachograph cards with card holders identification data, keys and certificates
Card Issuing Authorities (CIA)	Entities which manage card holders and issue Tachograph cards
Motion sensor manufacturers (MOM)	Entities which manufacture/repair motion sensor equipment and “personalise” them with data

Logical entity	Description
KP Generation (KPG)	Entities which generate the TDES paring key Kp for the motion sensor
Vehicle Unit Manufacturers (VUM)	Entities which manufacture/repair vehicle unit equipment and "personalise" them with keys and certificates
Vehicle Unit Key Generation (VUKG)	Entities which generate the RSA key pair for the vehicle unit (VU.SK and VU.PK)
Workshop (W)	Installation and calibration of the equipment (MS, VU) in the vehicle
Road Haulage Companies (RHC)	Haulage Companies which own vehicle (MS, VU) whose activity must be checked
Drivers (D)	Vehicle drivers whose activity must be checked
Control Body (CB)	Control authorities who take charge of checking the driver activities data

The role of each logical entity regarding information security is briefly described below with a reference to Annexe 1B [A1B] included the appendix 4 Tachograph Cards Structure [TCS], 10 Generic Security Targets [GST] and 11 Common Security Mechanisms [CSM] when it exists. Information treated is detailed at paragraph 3.2.

If several logical entities are implemented in the same organisational entity then the role of each logical entity will be merged in this organisational entity and the exchange of information might be therefore facilitated and more secure.

logical entity	Role	Annex 1B
ERCA	– Generation and registration of the European keys (EUR.SK, EUR.PK, Km_{VU}, Km_{WC}) – Generation and registration of the Member State keys certificates (MS.C) – Distribution of the European keys and certificates to MSCA – Maintain records of key certification suitable for use in system audits (SHA1 hash of certificates)	– CSM.007 , CSM.036 – CSM.008 – CSM.010
MSA	– Definition, update, control and application of the Member State security policy – Responsible for the security evaluation of the Vehicle Unit, Motion Sensor and tachograph cards and for their type approval – Order security audits on the organisations depending on its jurisdiction and responsible for the approval of the entities – Cards, vehicles and controls status monitoring – Annual report writing about the security status of the tachograph system within the Member State – Providing white and black lists of tachograph cards issued and annual report to other MSA	– A1B.271 – GST

logical entity	Role	Annex 1B
MSCA	– Generation and registration of the Member State keys (MS.SK, MS.PK) – Generation and registration of the Tachograph cards and Vehicle Unit certificates (Card.C, VU.C) – Registration of European keys and certificates (EUR.PK, Km_{VU}, Km_{WC}) – Distribution for certification of the Member State keys to ERCA (MS.PK) – Distribution of the Member State and European keys and certificates to CP (MS.C, Card.C, EUR.PK, Km_{WC}) – Distribution of the Member State and European keys and certificates to VUM (MS.C, VU.C, EUR.PK, Km_{VU}) – Distribution of the Motion Sensor pairing keys and the serial numbers encrypted by the European master key to MOM (Kp, Ns encrypted by Km) – Maintain records of key certification suitable for use in system audits (SHA1 hash of certificates)	– CSM.008 – CSM.009 – CSM.008 – CMS.037 – CMS.037 – CSM.037
CM	– Tachograph cards manufacturing compliant to the ISO norms and Protection Profile [IC PP] and [ES PP] or to the ITSEC security target evaluated E3 – Distribution of the Tachograph cards and card identification to CP	– GST – CSM.017
CKG	– Generation and registration of the Tachograph cards RSA keys pair (Card.SK, Card.PK) – Distribution of the Tachograph cards RSA keys pair to CP	– CSM.009
CP	– Distribution for certification of the Tachograph cards public keys with the card identification associated to MSCA – Tachograph cards personalisation with cardholder identification data, Member State and European keys and certificates – Distribution of the personalised Tachograph cards and workshop card PinCodes to CIA	– CSM.010, CSM.017 – TCS
CIA	– Cardholder identification data management (Tachograph card request, identification checking, acknowledgement) – Tachograph cards management within white and black lists – Distribution of the cardholder identification data to CP – Distribution of the personalised Tachograph cards to the holder (WC, RHCC, DC and CBC) – Distribution of the PinCode to the Workshop holder – Providing white and black lists to MSA and to CB	– GST

logical entity	Role	Annex 1B
MOM	– Motion Sensor manufacturing compliant to the ITSEC security target evaluated E3 – Distribution for encryption of the Motion Sensor pairing keys and serial numbers to MSCA – Motion Sensor personalisation with Motion Sensor pairing keys, serial numbers and these data encrypted by the European master key – Distribution of the personalised Motion Sensor to W	– GST – CSM.037 – CSM.037
KPG	– Generation and registration of the Motion Sensor pairing keys – Distribution of Motion Sensor pairing keys to MOM	– CSM.037
VUM	– Vehicle Unit manufacturing compliant to the ITSEC security target evaluated E3 – Distribution for certification of the Vehicle Unit public keys with the VU identification (VU known) *or the certificate request* identification (VU not known) associated, to MSCA – VU personalisation with Member State and European keys and certificates – *Distribution for registration of the VU identification and the certificate request identification associated, to MSCA* – Distribution of the personalised Vehicle Unit to W	– GST – CSM.010, CSM.017 – CSM.009 – CSM.017
VUKG	– Generation and registration of the Vehicle Unit RSA keys pair (VU.SK, VU.PK) – Distribution of the Vehicle Unit RSA keys pair to VUM	– CSM.009
W	– WC holder – VU Initial calibration and periodic inspection – Driver activities data downloading from VU and printing with their signature – Distribution of calibrated Recording Equipment to the RHC	– A1B.216 – A1B.257 – A1B.260
RHC	– Driver activities data capture and registration (MS and VU) – HC holder – Driver activities data downloading from VU and printing with their signature – Signed Driver activities data storage	– A1B.236 – A1B.237
D	– DC holder – Driver activities data registration on the DC via VU – Driver activities data downloading from VU or DC and printing with their signature	– A1B.195 – A1B.199
CB	– CB holder – Driver activities data downloading VU or DC and printing with their signature – Driver activities data and signature control – Control cards relating to the white and black lists	– A1B.232 – A1B.233 – GST

The material entities intervening in the security of the system are briefly presented with their functionality and the logical entities which manage these material entities (bold type) or which are connected.

Material entity	Material type	Functionality	Logical entities
ERCA PKI (Public Key Infrastructure)	Information system	– RSA and TDES Keys generation – RSA and TDES Keys registration – certificates generation – certificates registration – RSA and TDES Keys, certificates distribution	**ERCA** MSCA
MSCA PKI (Public Key Infrastructure)	Information system	– RSA Keys generation – RSA Keys registration – RSA and TDES Keys registration – certificates generation – certificates registration – Data encryption – RSA and TDES Keys, certificates, Data encrypted distribution	ERCA **MSCA** CP MOM VUM
Card DMT (development, manufacture tools)	sofware-hardware development, testing manufacture tools	– Tachograph Card generation	**CM** CP
Card PKI (Public Key Infrastructure)	Information system	– RSA Keys generation – RSA Keys registration – RSA Keys distribution	**CKG** CP
Card PS (Personalisation System)	Information system	– Tachograph Card personalisation	MSCA CM CKG **CP** CIA
Card MC (Management Centre)	Information system	– Users identification data management – Cards management – White and black lists management – Distribution Users identification data – Providing of white and black lists	MSA **CIA** CP W RHC D CB

Material entity	Material type	Functionality	Logical entities
MO DMT (development, manufacture tools)	sofware-hardware development, testing manufacture tools	– Motion Sensor generation – Motion Sensor personalisation	MSCA **MOM** KPG W
MO TDKI (TDES Key Infrastructure)	Information system	– TDES key generation – TDES key registration – TDES key distribution	**KPG** MOM
VU DMT (development, manufacture tools)	sofware-hardware development, testing manufacture tools	– Vehicle Unit generation – Vehicle Unit personalisation	MSCA **VUM** VUKG W
VU PKI (Public Key Infrastructure)	Information system	– RSA Keys generation – RSA Keys registration – RSA Keys distribution	MSCA **VUKG**
WC	Tachograph card	– Keys and certificates storage – PIN code Identification – VU mutual authentication – MS and VU calibration – Authorisation for the driver activities data downloading	**CP** **CIA** **W**
RHCC	Tachograph card	– Keys and certificates storage – VU mutual authentication – Authorisation for the driver activities data downloading	**CP** **CIA** **RHC**
DC	Tachograph card	– Keys and certificates storage – VU mutual authentication – Driver activities data downloading, signature and storage	**CP** **CIA** **D** CB
CBC	Tachograph card	– Keys and certificates storage – VU mutual authentication – Authorisation for the driver activities data downloading	**CP** **CIA** **CB**
MO	Equipment	– driver activities data capture and transfer to VU	**MOM** **W** **RHC**

Material entity	Material type	Functionality	Logical entities
VU	Equipment	– driver activities data storage – Cards reading and mutual authentication (HCC, WC, DC, CBC) – driver activities writing to DC – VU signed driver activities data downloading on IDE or on paper after a HC/W/CB authentication	**VUM** **W** **RHC** D CB
W-IDE (W Intelligent Dedicated Equipment)	Data media	– Storage of the downloaded driver activities data with their signature	**W**
RHC-IDE (RHC Intelligent Dedicated Equipment)	Data media	– Storage of the downloaded driver activities data with their signature	**RHC**
CB-IDE (CB Intelligent Dedicated Equipment)	Data media	– Storage of the downloaded driver activities data with their signature – Consultation of the white and black lists	**CB**

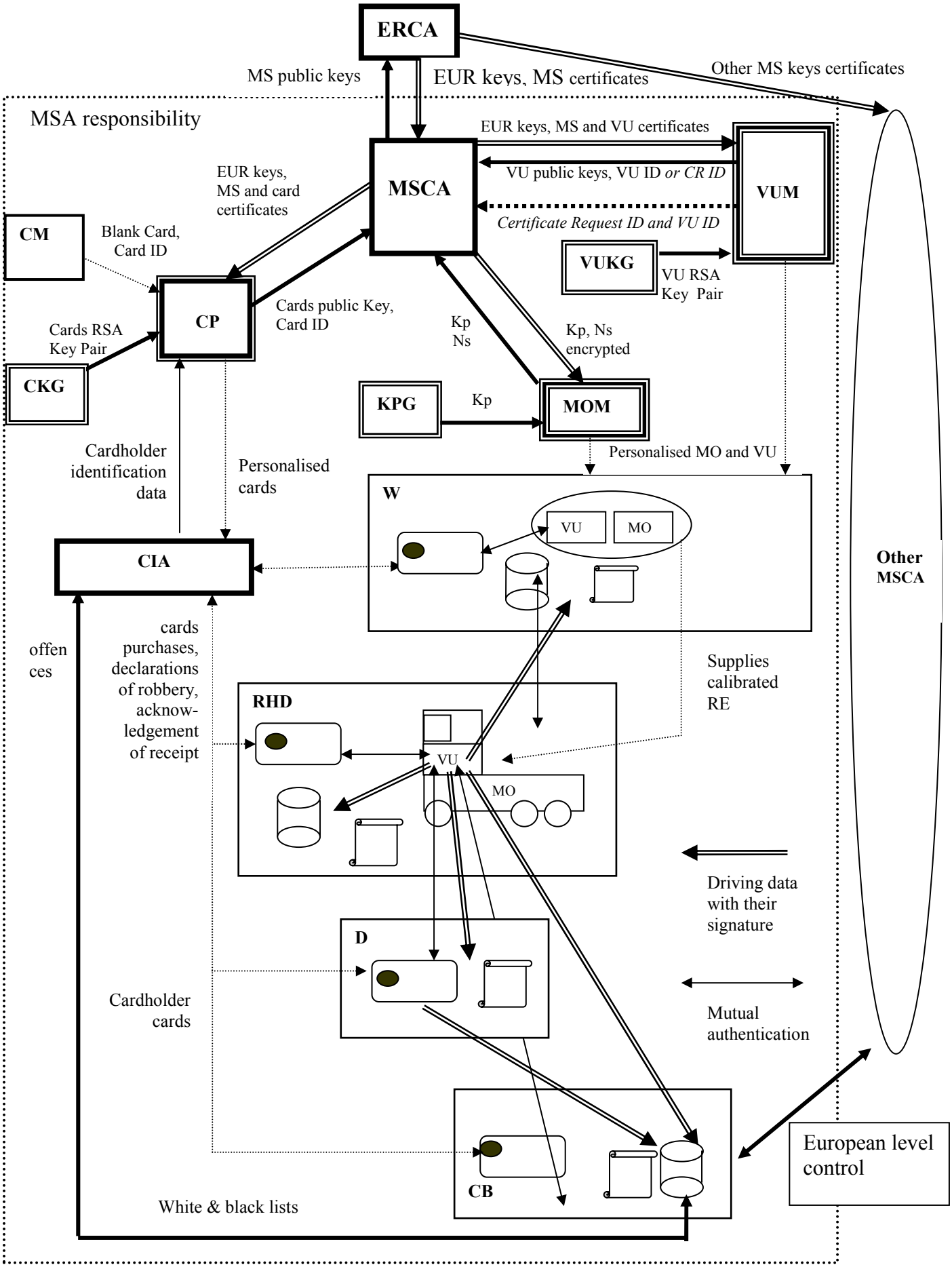

Figure 1.Relations between entities

3.2 Sensitive information and communication between entities

The information which, if their confidentiality, availability, integrity or authenticity is infringed and can be repudiated, will result in a compromise of tachograph system security (see Annex A for the security objectives) are listed below:

Information	Definition
EUR.SK	European secret key
EUR.PK	European public key
MS.SK	Member State secret keys
MS.PK	Member State public keys
Card ID	Card identification
Card.SK	Cards secret key for WC, RHCC, DC, CBC
Card.PK	Cards public key for WC, RHCC, DC, CBC
VU ID	VU identification
CR ID	Certificate Request identification
VU.SK	VU secret key
VU.PK	VU public key
MS.C (EUR.SK[MS.KID, MS.PK])	Member State public keys certificate (signature of the Member State public keys MS.PK and his key identifier MS.KID with the European secret key EUR.SK)
Card.C (MS.SK[Card.KID, Card.PK])	Card public keys certificate (signature of the card public keys Card.PK and his key identifier Card.KID with the Member State secret key MS.SK)
VU.C (MS.SK[Card.KID, Card.PK])	VU public keys certificate (signature of the VU public keys VU.PK and his key identifier VU.KID with the Member State secret key MS.SK)
Km_{VU}	VU European master key
Km_{WC}	Workshop Card European master key
Km= Km_{VU} XOR Km_{WC}	Motion Sensor European master key (XOR of Km_{VU} and Km_{WC}) used to encrypt Kp and Ns
Ns	Motion Sensor serial number
Kp	Motion Sensor pairing key
E_{Km}(Ns, Kp)	Ns, Kp encrypted by Km
PinCode WC	PinCode of the Workshop Card
CID	Cardholder Identification Data
DAD	Driver Activities Data (data related to driver activities)
WL&BL	White list and black list of tachograph card
Annual report	Annual report produce by each MSA about the state of security of the tachograph system within its jurisdiction

The communications between entities are as follow:

Information	From entity	To entity	To entity	To entity	To entity	To entity
EUR.SK	ERCA PKI					
EUR.PK	ERCA PKI	MSCA PKI	Card PS	VU PS	Card	VU
MS.SK	MSCA PKI					
MS.PK	MSCA PKI	ERCA PKI				
Card ID	CM DMT	Card PS	MSCA PKI	Card MC	Card	
Card.SK	Card PKI	Card PS	Card			
Card.PK	Card PKI	Card PS	MSCA PKI	Card		
VU ID	VU DMT	MSCA PKI	VU			
CR ID	VU DMT	MSCA PKI	VU			
VU.SK	VU PKI	VU DTM	VU			
VU.PK	VU PKI	VU DTM	MSCA PKI	VU		
MS.C	ERCA PKI	MSCA PKI	Card PS	VU DTM	Card	VU
Card.C	MSCA PKI	Card PS	Card			
VU.C	MSCA PKI	VU DTM	VU			
Km_{VU}	ERCA PKI	MSCA PKI	VU DTM	VU		
Km_{WC}	ERCA PKI	MSCA PKI	Card PS	WC	VU via WC	
Km	ERCA PKI	MSCA PKI	VU via WC			
Ns	MO DMT	MSCA PKI	MO			
Kp	MO TDKI	MO DMT	MSCA PKI	MO		
$E_{Km}(Ns, Kp)$	MSCA PKI	MO DMT	MO			
PinCode WC	Card PS	Card MC	WC	W (paper)		
CID	Card MC	Card PS	Card			
DAD	VU	DC	RHC-IDE	W-IDE	CB-IDE	
WL&BL	Card MC	CB-IDE	MSA	MSA other MS		
Annual report	MSA	ERCA	MSA other MS			

4. General security principle

4.1 Security policy application field

4.1.1 European Level

4) The commission will designate a European certification authority with responsibility for European key creation (management) and for certifying the Member State keys.

5) The MSA will approve its MSCA and informs the EC of its decision. The EC will inform the ERCA and other MS's. The ERCA will certify keys for MSCAs approved by the MSA. The ERCA will not certify MSCAs.

6) European certification of Member State keys could be periodically renewed. The duration of the validity of a certificate will be the responsibility of the MSA.

4.1.2 Member State level

7) Each Member State will designate an authority responsible for the security of the tachograph system within its jurisdiction. That authority will be called the Member State Authority.

8) The Member State Authority is responsible for defining and approving the national security policy that is applicable to all persons involved in tachograph use and in the creation and maintenance of tachograph equipment.

9) The national security policy should be reviewed and updated regularly, to remain consistent with important modifications in the TS context (whether organisation or requirements).

10) Control bodies within Member States should, through regular, planned and independent reviews, ensure that the national security policy is implemented.

11) Compliance of the national security policy to the TS security requirements is proved when it can be demonstrated that the Member State security policy addresses all the recommendations in this document.

4.2 Security Organisation

Following items could be understood as the security policy of the MSA.

12) A Member State Authority should co-ordinate the national security policy:

- Defining the security policy for the tachograph system, and defining its objectives.
- Ensuring the security policy is kept up-to-date, and remains compliant with the TS security requirements.
- Ensuring the dissemination of the security policy to the TS entities within its jurisdiction.
- Producing recommendations on any question about TS security in its territory.

13) A Member State Authority should provide advice and guidance in respect of all questions relating to security:

- Clarifying the TS security requirements for TS organisations within its jurisdiction.
- Arbitrating on any question about the soundness of implementations intended to apply the national security policy, to ensure that the application is consistent.
- Organising the dissemination of security awareness and training for people.

14) A Member State Authority should ensure there is a clear statement of responsibilities for production of the security elements:

- Defining the process for authorising the Member State Certification of equipment keys (processes described in the Member State security policy).
- Ensuring there are appropriate means for the delivery of the required security elements to the TS entities within its jurisdiction.
- Requesting certification of the Member State key from the European Certification Authority.

15) A Member State Authority should ensure the security policy is applied:

- Carrying out security assessments upon TS organisations in its jurisdiction.
- Producing an annual report about the state of security of the tachograph system within its area of jurisdiction.

16) A Member State Authority should co-operate with other Member State Authorities, the European Root Certification Authority, and the commission:
    - Co-ordinating with the Member State control authority, as defined in article 28 of European directive [95/46/CE].

    - Communicating with other Member State Authorities and the European Root Certification Authority, full details of the required security elements included the national security policy to ensure a mutual recognition of system components managed by these authorities, and keeping the commission informed of these communications.

    - Providing copies of the annual report to the other Member State Authorities, the European Root Certification Authority, and the commission.

4.3 Sensitive Assets classification

4.3.1 Sensitive Assets identification

17) Sensitive assets should receive a security label so that they may be partitioned to allow access only to those people who need such access to carry out their work.

To support this aim, the following labels could be used:
- TACHOGRAPH SECURITY: Applied to a category of data for which an infringement of the security objectives will impact strongly upon the security of the tachograph system,
- TACHOGRAPH PERSONAL: Applied to data of a personal nature, as defined in article 2 of European directive [95/46/CE].

18) The Member State Authority should be responsible for assigning security labels and producing and updating a sensitive assets inventory, as described in Annex A of this document.

19) The Member State Authority should be responsible for prescribing procedures for the handling and labelling of sensitive assets, in accordance with the classification defined above.

20) The Member State Authority should be responsible for modifying and assigning security labels to sensitive assets.

21) The TS entities should maintain a record of all activities carried out upon sensitive assets.

4.3.2 Sensitive assets exchange

22) Each Member State should enter a multiparty agreement with other Member States, when exchange of TS sensitive assets is needed.

23) This multiparty agreement should specify the nature and security label of exchanged assets, and will include security policy agreements for the exchanges between Member States.

24) The agreement should specify the security authority responsible for the security of the exchanges.

4.4 Compliance

4.4.1 Compliance with regulation

25) Member State authorities should ensure that TS entities within its jurisdiction satisfy the TS security requirements listed in section 1.2 of this document.

4.4.2 Security review of IT systems

26) The Member State Authorities should carry out periodically security audits upon organisations and information systems of the entities within their jurisdiction that are involved with tachograph systems.

27) Member State Authorities should define the audit procedures for entities within the jurisdiction of its Member State.

28) Audits should be designed to ensure that security procedures and measures in use in the audited entity are correctly applied by all the entity's personnel and compliant with the national security policy.

29) If audit results reveal vulnerabilities in the security of the tachograph system, the subsequent report should be labelled «TACHOGRAPH SECURITY».

5. Security policy for each entity of the system

For each logical entity which might be implemented in an organisational entity, the specific security requirements, security architecture and the recommendations framework for the security policy are presented.

If Member States decide to implement several logical entities in one organisational entity, the several paragraphs (specific security requirements, security architecture and recommendations framework) of each entity should be merged to provide a security policy for this organisational entity.

Entities which manage sensitive information in an organisational environment (ERCA, MSCA, CM, CKG, CP, CIA, MOM, KPG, VUM, VUKG) should write their own internal security policy taking into account these specific security requirements, security architecture and recommendations framework which refer to the standard ISO 17799 and ETSI 102042.

For others entities which use Tachograph cards (W, RHC, D, CB) this security policy could be included in national laws or regulations. For these entities the reference to ISO 17799 should be applied in a very light way, only few items should be relevant, but this reference provide a consistency in the national security policy.

5.1 Security policy for ERCA

5.1.1 Specific security requirements

30) The goal of the ERCA policy is to fulfil the following TS security requirements:

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

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

5.1.2 Role of ERCA

The role of ERCA regarding information security is briefly described below:

- Generation and registration of the European keys (EUR.SK, EUR.PK, Km_{VU} Km_{WC})
- Generation and registration of the Member State keys certificates (MS.C)
- Distribution of the European keys and certificates to MSCA (EUR.PK, Km_{VU} Km_{WC}, MS.C)
- Maintain records of key certification suitable for use in system audits (SHA1 hash of certificates)

The material architecture is based on a PKI system.

5.1.3 Communication between ERCA and the other entities

31) The sensitive assets exchanged are in a manner that satisfy the security objectives (see Annexe A):

- From ERCA to MSCA (EUR.PK, Km_{VU} Km_{WC}, MS.C)
- From MSCA to ERCA (MS.PK)

5.1.4 Recommendations framework

32) The policy is derived from the draft ETSI technical specification “policy requirements for certification authorities issuing public key certificates” (see annexe D)

33) The measures listed in the section “CA management and operation” of the draft ETSI should match the set of recommendations of the ISO 17799 (see annexe C) and a cross-references should prove it.

5.2 Security policy for MSCA

5.2.1 Specific security requirements

34) The goal of the MSCA policy is to fulfil the following TS security requirements:

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

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

5.2.2 Role of MSCA

The role of MSCA regarding information security is briefly described below:

- Generation and registration of the Member State keys (MS.SK, MS.PK)
- Generation and registration of the Tachograph cards and Vehicle Unit certificates (Card.C, VU.C)
- Registration of European keys and certificates (EUR.PK, Km_{VU}, Km_{WC})
- Distribution for certification of the Member State keys to ERCA (MS.PK)
- Distribution of the Member State and European keys and certificates to CP (MS.C, Card.C, EUR.PK, Km_{WC})
- Distribution of the Member State and European keys and certificates to VUM (MS.C,VU.C, EUR.PK, Km_{VU})
- Distribution of the Motion Sensor pairing keys and the serial numbers encrypted by the European master key to MOM (Kp, Ns encrypted by Km)
- Maintain records of key certification suitable for use in system audits (SHA1 hash of certificates)

The material architecture is based on a PKI system.

5.2.3 Communication between MSCA and the other entities

35) The sensitive assets exchanged are in a manner that satisfy the security objectives (see Annexe A) :

- From MSCA to ERCA (MS.PK)
- From ERCA to MSCA (EUR.PK, Km_{VU} and Km_{WC}, MS.C)
- From CP to MSCA (Card.PK, Card ID)
- From MSCA to CP (MS.C, Card.C, EUR.PK, Km_{WC})
- From MOM to MSCA (Kp, Ns)
- From MSCA to MOM (E_{Km}(Kp, Ns))
- From VUM to MSCA (VU.PK, VU ID *or CR ID*)
- From MSCA to VUM (MS.C, VU.C, EUR.PK, Km_{VU})
- *From VUM to MSCA (CR ID and VU ID)*

5.2.4 Recommendations framework

36) This policy is derived from the draft ETSI technical specification “policy requirements for certification authorities issuing public key certificates”.

37) The measures listed in the section “CA management and operation” of the draft ETSI should match the set of recommendations of the ISO 17799 (see annexe C) and a cross-references should prove it.

5.3 Security policy for Card Manufactures

5.3.1 Specific security requirements

38) The goal of the card manufactures policy is to fulfil the following TS security requirements:

O.DLV_DATA	The Application Data must be delivered from the smart card embedded software developer (phase 1) either to the IC Packaging manufacturer, the Finishing Process manufacturer or the Personalisers through a trusted delivery and verification procedure that shall be able to maintain the integrity and confidentiality of the Application Data.
O.TEST_OPERATE	Appropriate functionality testing of the TOE shall be used in phases 4 to 6. During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.
O.USE_DIAG	Secure communication protocols and procedures shall be used between the smart card and the card reader terminal.
O.USE_SYS	The integrity and the confidentiality of sensitive data stored / handled by the system (terminals, communications...) shall be maintained.
O.EnvICESPP_CM	The other physical, personal or procedural requirements that contribute to the security of tachograph card which are listed in [IC PP] and [ES PP] (chapters security objectives for the environment) and concern the Card manufacturers

5.3.2 Role of Card Manufactures

The role of CM regarding information security is briefly described below:

- Tachograph cards manufacturing compliant to the ISO norms and Protection Profile [IC PP] and [ES PP] or to the ITSEC security target evaluated E3
- Distribution of the Tachograph blank cards with card identification to CP

The material architecture is based on software-hardware development, testing and manufacture tools and TC.

5.3.3 Communication between Card Manufactures and the other entities

39) The sensitive assets exchanged are in a manner that satisfy the security objectives (see Annexe A) :

- From CM to CP (blank cards and Card ID)

5.3.4 Recommendations framework

40) The measures listed in the security policy should match the set of recommendations of the ISO 17799 (see annexe C) and cross-references should prove it.

5.4 Security policy for Card Key Generation

5.4.1 Specific security requirements

41) The goal of the Card Key Generation policy is to fulfil the following TS security requirements:

O.DLV_DATA	The Application Data must be delivered from the smart card embedded software developer (phase 1) either to the IC Packaging manufacturer, the Finishing Process manufacturer or the Personalizer through a trusted delivery and verification procedure that shall be able to maintain the integrity and confidentiality of the Application Data.

5.4.2 Role of Card Key Generation

The role of CKG regarding information security is briefly described below:

- Generation and registration of the Tachograph cards RSA keys pair (Card.Sk, Card.PK)
- Distribution of the Tachograph cards RSA keys pair to CP

The material architecture is based on a PKI system.

5.4.3 Communication between Card Key Generation and the other entities

42) The sensitive assets exchanged are in a manner that satisfy the security objectives (see Annexe A):

- From CKG to CP (Card.SK and Card.PK)

5.4.4 Recommendations framework

43) The measures listed in the security policy should match the set of recommendations of the ISO 17799 (see annexe C) and cross-references should prove it.

5.5 Security policy for Card Personalisers

5.5.1 Specific security requirements

44) The goal of the card Personalisers policy is to fulfil the following TS security requirements:

M.Sec_Data_Generation	Security data generation algorithms must be accessible to authorised and trusted persons only.
M.Sec_Data_Transport	Security data must be generated, transported, and inserted into the motion sensor, in such a way to preserve its appropriate confidentiality and integrity.
O.DLV_DATA	The Application Data must be delivered from the smart card embedded software developer (phase 1) either to the IC Packaging manufacturer, the Finishing Process manufacturer or the Personalizer through a trusted delivery and verification procedure that shall be able to maintain the integrity and confidentiality of the Application Data.
O.TEST_OPERATE	Appropriate functionality testing of the TOE shall be used in phases 4 to 6. During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

And the legal requirements (European directives 95/46/CE).

5.5.2 Role of Card Personalisers

The role of CP regarding information security is briefly described below:

- Distribution for certification of the Tachograph cards public keys with the card identification associated to MSCA
- Tachograph cards personalisation with cardholder identification data, Member State and European keys and certificates
- Distribution of the personalised Tachograph cards and workshop card PinCodes to CIA

The material architecture is based on a personalisation system and TC.

5.5.3 Communication between Card Personalisers and the other entities

45) The sensitive assets exchanged are in a manner that satisfy the security objectives (see Annexe A):

- From CM to CP (blank Card and Card ID)
- From CKG to CP (Card.SK and Card.PK)
- From CP to MSCA (MS.PK, Card ID)
- From MSCA to CP (MS.C, Card.C, EUR.PK, Km_{WC})
- From CIA to CP (CID)
- From CP to CIA (personalised Cards, workshop card PinCodes)

5.5.4 Recommendations framework

46) The measures listed in the security policy should match the set of recommendations of the ISO 17799 (see annexe C) and cross-references should prove it.

5.6 Security policy for Card Issuing Authorities

5.6.1 Specific security requirements

47) The goal of the card issuing authorities policy is to fulfil the security requirements of the annex 1B, more specifically:

M.Card_Availability	Tachograph cards must be available and delivered to authorised persons only.
M.Card_Traceability	Card delivery must be traceable (white lists, black lists), and black lists must be used during security audits.
M.Driver_Card_Uniqueness	Drivers must possess, at one time, only one valid driver card.
O.DLV_DATA	The Application Data must be delivered from the smart card embedded software developer (phase 1) either to the IC Packaging manufacturer, the Finishing Process manufacturer or the Personalizer through a trusted delivery and verification procedure that shall be able to maintain the integrity and confidentiality of the Application Data.

And the legal requirements (European directives 95/46).

5.6.2 Role of Card Issuing Authorities

The role of CIA regarding information security is briefly described below:

- Cardholder identification data management (Tachograph card request, identification checking, acknowledgement)
- Tachograph cards management within white and black lists
- Distribution of the cardholder identification data to CP
- Distribution of the personalised Tachograph cards to the holder (WC, RHCC, DC and CBC)
- Distribution of the PinCode to the Workshop holder
- Providing white and black lists to MSA and to CB

The material architecture is based on an information system and TC.

5.6.3 Communication between Card Issuing Authorities and the other entities

48) The sensitive assets exchanged are in a manner that satisfy the security objectives (see Annexe A):

- From CIA to CP (CID)
- From CP to CIA (personalised Cards)
- From CIA to RHC, D (personalised Cards)
- From CIA to W (personalised Cards, workshop card PinCodes)
- From CIA to CB (personalised Cards, white § black lists)

5.6.4 Recommendations framework

49) The measures listed in the security policy should match the set of recommendations of the ISO 17799 (see annexe C) and cross-references should prove it.

5.7 Security policy for Motion Sensor Manufacturers

5.7.1 Specific security requirements

50) The goal of the Motion Sensor Manufacturers policy is to fulfil the following TS security requirements:

M.Delivery	Motion sensor manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of the motion sensor is done in a manner that maintains IT security.
M.Development	Motion sensor developers must ensure that the assignment of responsibilities during development is done in a manner which maintains IT security
M.Manufacturing	Motion sensor manufacturers must ensure that the assignment of responsibilities during manufacturing is done in a manner that maintains IT security, and that during the manufacturing process the motion sensor is protected from physical attacks which might compromise IT security
M.Sec_Data_Generation	Security data generation algorithms must be accessible only to authorised and trusted persons.
M.Sec_Data_Transport	Security data must be generated, transported, and inserted into the motion sensor in such a way to preserve its appropriate confidentiality and integrity.
M.Software_Upgrade	Software revisions must be granted security certification before they can be implemented in a motion sensor.

5.7.2 Role of Motion Sensor Manufacturers

The role of MOM regarding information security is briefly described below:

- Motion Sensor manufacturing compliant to the ITSEC security target evaluated E3
- Distribution of the Motion Sensor serial numbers and Motion Sensor pairing keys to MSCA
- Motion Sensor personalisation with Motion Sensor pairing keys, serial numbers and these data encrypted by the European master key
- Distribution of the personalised Motion Sensor to W

The material architecture is based on a software-hardware development, testing and manufacture tools, and motion sensor.

5.7.3 Communication between Motion Sensor Manufacturers and the other entities

51) The sensitive assets exchanged are in a manner that satisfy the security objectives (see Annexe A) :

- From KPG to MOM (Kp)
- From MOM to MSCA (Kp, Ns)
- From MSCA to MOM (E_{Km}(Kp, Ns))
- From MOM to W (personalised Motion Sensor)

5.7.4 Recommendations framework

52) The measures listed in the security policy should match the set of recommendations of the ISO 17799 (see annexe C) and cross-references should prove it.

5.8 Security policy for Key Pairing Generation

5.8.1 Specific security requirements

53) The goal of the Key Pairing Generation policy is to fulfil the following TS security requirements:

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

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

5.8.2 Role of Key Pairing Generation

The role of KPG regarding information security is briefly described below:

- Generation and registration of the Motion Sensor pairing keys
- Distribution of the Motion Sensor pairing keys to MOM

The material architecture is based on a TDES Key Infrastructure system.

5.8.3 Communication between Key Pairing Generation and the other entities

54) The sensitive assets exchanged are in a manner that satisfy the security objectives (see Annexe A) :

- From KPG to MOM (Kp)

5.8.4 Recommendations framework

55) The measures listed in the security policy should match the set of recommendations of the ISO 17799 (see annexe C) and cross-references should prove it.

5.9 Security policy for Vehicle Unit Manufacturers

5.9.1 Specific security requirements

56) The goal of the VU manufacturers policy is to fulfil the following TS security requirements:

M.Delivery	VU manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of the VU is done in a manner that maintains IT security.
M.Development	VU developers must ensure that the assignment of responsibilities during development is done in a manner which maintains IT security
M.Manufacturing	VU manufacturers must ensure that the assignment of responsibilities during manufacturing is done in a manner that maintains IT security, and that during the manufacturing process the VU is protected from physical attacks which might compromise IT security
M.Sec_Data_Generation	Security data generation algorithms must be accessible only to authorised and trusted persons.
M.Sec_Data_Transport	Security data must be generated, transported, and inserted into the VU, in such a way to preserve its appropriate confidentiality and integrity.
M.Software_Upgrade	Software revisions must be granted security certification before they can be implemented in a VU.
O.USE_DIAG	Secure communication protocols and procedures shall be used between the smart card and the terminal.
O.USE_SYS	The integrity and the confidentiality of sensitive data stored / handled by the system (terminals, communications...) shall be maintained.

5.9.2 Role of Equipment Vehicle Unit Manufacturers

The role of VUM regarding information security is briefly described below:

- Vehicle Unit manufacturing compliant to the ITSEC security target evaluated E3
- Distribution for certification of the Vehicle Unit public keys with the VU identification (VU known) *or the certificate request identification (VU not known)* associated, to MSCA
- VU personalisation with Member State and European keys and certificates
- *Distribution for registration of the VU identification and the certificate request identification associated, to MSCA*
- Distribution of the personalised Vehicle Unit to W

The material architecture is based on a software-hardware development, testing and manufacture tools and VU.

5.9.3 Communication between Vehicle Unit Manufacturers and the other entities

57) The sensitive assets exchanged are in a manner that satisfy the security objectives (see Annexe A) :

- From VUKG to VUM (VU.SK and VU.PK)
- From VUM to MSCA (VU.PK, VU ID *or CR ID*)
- From MSCA to VUM (VU.C, EUR.PK, Km_{VU}, MS.C)
- *From VUM to MSCA (CR ID and VU ID)*
- From VUM to W (personalised VU)

5.9.4 Recommendations framework

58) The measures listed in the security policy should match the set of recommendations of the ISO 17799 (see annexe C) and cross-references should prove it.

5.10 Security policy for Vehicle Unit Key Generation

5.10.1 Specific security requirements

59) The goal of the Vehicle Unit Key Generation policy is to fulfil the following TS security requirements:

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

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

5.10.2 Role of Equipment Vehicle Unit Key Generation

The role of VUKG regarding information security is briefly described below:

- Generation and registration of the Vehicle Unit RSA keys pair (VU.SK, VU.PK)
- Distribution of the Vehicle Unit Vehicle Unit RSA keys pair

The material architecture is based on a PKI system.

5.10.3 Communication between Vehicle Unit Key Generation and the other entities

60) The sensitive assets exchanged are in a manner that satisfy the security objectives (see Annexe A) :

- From VUM to VUKG (VU ID)
- From VUKG to MSCA (VU.PK)
- From VUKG to VUM (VU.SK)

5.10.4 Recommendations framework

61) The measures listed in the security policy should match the set of recommendations of the ISO 17799 (see annexe C) and cross-references should prove it.

5.11 Security policy for workshops

5.11.1 Specific security requirements

62) The goal of the workshops policy is fulfil the following TS security requirements:

M.Activation	Vehicle manufacturers and fitters or workshops must activate the VU after its installation and before the vehicle leaves the premises where installation took place
M.Approved_Workshops	Installation, calibration and repair of recording equipment must be carried by trusted and approved fitters or workshops.
M.Card_Availability	Tachograph cards must be available and delivered to authorised persons only.
M.Delivery	Motion sensor (resp. VU) manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of the motion sensor (resp. VU) is done in a manner, which maintains IT security.
M.Faithful_Calibration	Approved fitters and workshops must enter proper vehicle parameters in recording equipment during calibration
M.Mechanical_Interface	Means of detecting physical tampering with the mechanical interface must be provided (e.g. seals)
M.Regular_Inpections	Recording equipment must be periodically inspected and calibrated.

And the legal requirements (European directives 95/46/CE).

5.11.2 Role of workshops

The role of workshop regarding information security is briefly described below:

- WC holder
- VU Initial calibration and periodic inspection
- Driver activities data downloading from VU and printing with their signature
- Distribution of calibrated vehicles (VU et Motion sensor) to the RHC

The material architecture is based on TC, Motion Sensor, VU and IDE.

5.11.3 Communication between workshops and the other entities

63) The sensitive assets exchanged are in a manner that satisfy the security objectives (see Annexe A):

- From CIA to W (personalised Cards, PinCodes)
- From VUM to W (personalised VU)
- From MOM to W (personalised Motion Sensor)
- From RHC to W (driver activities data)

5.11.4 Recommendations framework

64) The measures listed in the security policy should match a part of the recommendations of the ISO 17799 and a cross-references should prove it:
    - 3. SECURITY POLICY: Management's commitment to enforce security / security principles, rules and organisational security procedures definition
    - 4. SECURITY ORGANIZATION: Define roles and responsibilities as regards security
    - 5. ASSETS CLASSIFICATION AND CONTROL: Information/material classification and protection management procedure
    - 6. PERSONNEL SECURITY: Personnel vetting / Employment contract / signature of an individual non disclosure commitment by the personnel
    - 7. PHYSICAL AND ENVIRONMENTAL SECURITY: Physical security of the premises / physical access control to the equipment
    - 11. BUSINESS CONTINUITY MANAGEMENT: Disaster recovery plan and associated testing procedures
    - 12. COMPLIANCE: Compliance with regulation / periodic security audit

5.12 Security policy for Road Haulage Companies

5.12.1 Specific security requirements

65) The goal of the road haulage companies policy is to fulfil the following TS security requirements:

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

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

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

And the legal requirements (European directives and 95/46/CE).

5.12.2 Role of Road Haulage Companies

The role of road haulage companies regarding information security is briefly described below:

- Driver activities data capture and registration (RE)
- HC holder
- Driver activities data downloading from VU and printing with their signature
- Signed Driver activities data storage

The material architecture is based on Motion Sensor, VU, TC and IDE.

5.12.3 Communication between Road Haulage Companies and the other entities

66) The sensitive assets exchanged are in a manner that satisfy the security objectives (see Annexe A):

- From CIA to RHC (personalised cards)
- From RHC to CB (driver activities data)

5.12.4 Recommendations framework

67) The measures listed in the security policy should match a part of the recommendations of the ISO 17799 and a cross-references should prove it:
    - 3. SECURITY POLICY: Management's commitment to enforce security / security principles, rules and organisational security procedures definition
    - 4. SECURITY ORGANIZATION: Define roles and responsibilities as regards security
    - 5. ASSETS CLASSIFICATION AND CONTROL: Information/material classification and protection management procedure
    - 6. PERSONNEL SECURITY: Personnel vetting / Employment contract / signature of an individual non disclosure commitment by the personnel
    - 7. PHYSICAL AND ENVIRONMENTAL SECURITY: Physical security of the premises / physical access control to the equipment
    - 11. BUSINESS CONTINUITY MANAGEMENT: Disaster recovery plan and associated testing procedures
    - 12. COMPLIANCE: Compliance with regulation / periodic security audit

5.13 Security policy for Vehicle Drivers

5.13.1 Specific security requirements

68) The goal of the drivers policy is to fulfil the following TS security requirements:

M.Card_Availability	Tachograph cards must be available and delivered to authorised persons only.
M.Driver_Card_Uniqueness	Drivers must possess, at one time, only one valid driver card.
M.Faithful_Drivers	Drivers must play by the rules and act responsibly (e.g. use their driver cards, properly select their activity for those that are manually selected, …).

And the legal requirements (European directives 95/46/CE).

5.13.2 Role of Vehicle Drivers

The role of driver regarding information security is briefly described below :

- DC holder
- Driver activities data registration on the DC via VU
- Driver activities data downloading from VU or DC and printing with their signature

The material architecture is based on VU and TC.

5.13.3 Communication between Vehicle Drivers and the other entities

69) The sensitive assets exchanged are in a manner that satisfy the security objectives (see Annexe A) :

- From CIA to D (personalised cards)
- From RHC via the VU to D (driver activities data)
- From D via the card to CB (driver activities data)

5.13.4 Recommendations framework

70) The measures listed in the security policy can be reduced to a commitment letter which engage the driver responsibility :

- card protection (declaration of loss or robbery)
- card using (correct registration of the driving activities data)
- card control (signature of the driving activities data downloaded)

5.14 Security policy for Control Bodies

5.14.1 Specific security requirements

71) The goal of the control bodies policy is to fulfil the following TS security requirements:

M.Card_Availability	Tachograph cards must be available and delivered to authorised persons only.
M.Card_Traceability	Card delivery must be traceable (white lists, black lists), and black lists must be used during security audits.
M.Controls	Law enforcement controls must be performed regularly and randomly, and must include security audits.
M.Driver_Card_Uniqueness	Drivers must possess, at one time, only one valid driver card.
M.Faithful_Drivers	Drivers must play by the rules and act responsibly (e.g. use their driver cards, properly select their activity for those that are manually selected, …).
M.Mechanical_Interface	Means of detecting physical tampering with the mechanical interface must be provided (e.g. seals)
M.Regular_Inpections	Recording equipment must be periodically inspected and calibrated.

And the legal requirements (European directives 95/46/CE).

5.14.2 Role of Control Bodies

The role of driver regarding information security is briefly described below:

- CB holder
- Driver activities data downloading VU or DC and printing with their signature
- Driver activities data and signature control
- Control cards relating to the white and black lists

The material architecture is based on VU, TC and IDE.

5.14.3 Communication between Control Bodies and the other entities

72) The sensitive assets exchanged are in a manner that satisfy the security objectives (see Annexe A):

- From CIA to CB (personalised cards, white § black lists)
- From RHC via the VU to CB (driver activities data)
- From D via the card to CB (driver activities data)

5.14.4 Recommendations framework

73) The measures listed in the security policy should match a part of the recommendations of the ISO 17799 and a cross-references should prove it:

- 3. SECURITY POLICY: Management's commitment to enforce security / security principles, rules and organisational security procedures definition
- 4. SECURITY ORGANIZATION: Define roles and responsibilities as regards security
- 5. ASSETS CLASSIFICATION AND CONTROL: Information/material classification and protection management procedure
- 7. PHYSICAL AND ENVIRONMENTAL SECURITY: Physical security of the premises / physical access control to the equipment
- 11. BUSINESS CONTINUITY MANAGEMENT: Disaster recovery plan and associated testing procedures
- 12. COMPLIANCE: Compliance with regulation / periodic security audit

Annex(e) A Sensitive Assets Inventory

The sensitive assets inventory contains the sensitive data or products used in the TS with the security objectives and the labels associated. The protection to be implemented during storage or exchange must be compliant with these objectives.

Assets	Security objectives and labels
EUR.SK	– **Confidentiality**: if the key is known, an offender can certify a false MS key, used to certify a false EQT key, itself used to sign false driver activities data (a fraudulent tachograph system can be shoehorned into the legitimate one) – **Integrity**: if the key is modified, ERCA can't certify new MS.PK, used to certify EQT.SK, itself used to sign driver activities data – **Availability**: same as integrity. – Label: **SECURITY**
EUR.PK	– **Authenticity**: if the origin of the key can't be verified, the driver activities data signature can't be trusted – **Availability**: if the key isn't available it can't be inserted in equipment for certificate authentication – Label: **SECURITY**
MS.SK	– **Confidentiality**: if the key is known, an offender can certify a false key EQT.SK, used to certify a false key EQT.SK, itself used to singe false driver activities data (a fraudulent equipment could work into the legitimate system) – **Integrity**: if the key is modified, MSCA can't certify new EQT.SK, itself used to sign driver activities data – Label: **SECURITY**
MS.PK	– **Authenticity**: if the origin of the key can't be verified, the driver activities data signature can't be trusted – **Availability**: if the key isn't available it can't be inserted in equipment for certificate authentication – Label: **SECURITY**
Card ID	– **Integrity**: card keys and certificate won't refer the right card – Label: **SECURITY**
Card.SK	– **Confidentiality**: if the key is known, an offender can sign false driver activities data (false card could be made to work) – **Integrity**: the card will not work – Label: **SECURITY**
Card.PK	– **Authenticity**: if the origin of the key can't be verified, the driver activities data signature can't be trusted – **Availability**: the card will not work – Label: **SECURITY**

Assets	Security objectives and labels
VU ID	– **Integrity**: VU keys and certificate won't refer the right VU – Label: **SECURITY**
CR ID	– **Integrity**: VU keys and certificate won't refer the right VU – Label: **SECURITY**
VU.SK	– **Confidentiality**: if the key is known, an offender can used false VU to generate false driver activities data) – **Integrity**: the VU will not work – Label: **SECURITY**
VU.PK	– **Authenticity**: if the origin of the key can't be verified, the driver activities data signature can't be trusted – **Availability**: the VU will not work – Label: **SECURITY**
MS.C	– **Integrity:** if the certificate is modified, the driver activities data signature can't be verified – **Authenticity**: if the origin of the certificate can't be verified, the driver activities data signature can't be trusted – **Availability**: if the key isn't available it can't be inserted in equipment for key authentication – Label: **SECURITY**
Card.C	– **Integrity:** if the certificate is modified, the driver activities data signature can't be verified – **Authenticity**: if the origin of the certificate can't be verified, the driver activities data signature can't be trusted – **Availability**: if the key isn't available it can't be inserted in equipment for key authentication – Label **SECURITY**
VU.C	– **Integrity:** if the certificate is modified, the driver activities data signature can't be verified – **Authenticity**: if the origin of the certificate can't be verified, the driver activities data signature can't be trusted – **Availability**: if the key isn't available it can't be inserted in equipment for key authentication – Label **SECURITY**
Kvu	– **Confidentiality**: if the key is known, the calibration can't be trusted – **Integrity**: if the key is modified, the calibration won't succeed – **Availability**: if the key is totally unavailable, the system is unavailable – Label **SECURITY**
Kwc	– **Confidentiality**: if the key is known, the calibration can't be trusted – **Integrity**: if the key is modified, the calibration won't succeed – **Availability**: if the key is totally unavailable, the system is unavailable – Label **SECURITY**

Assets	Security objectives and labels
Km	– **Confidentiality**: if the key is known, the calibration can't be trusted – **Integrity**: if the key is modified, the calibration won't succeed – Label **SECURITY**
Ns	– **Integrity**: if Ns is modified, the calibration won't succeed – Label: **SECURITY**
Kp	– **Confidentiality**: if the key is known, the calibration can't be trusted – **Integrity**: if the key is modified, the calibration won't succeed – Label **SECURITY**
E_{Km}(Ns, Kp)	– **Integrity**: if data are modified, the calibration won't succeed – Label: **SECURITY**
PinCode WC	– **Confidentiality**: if the code is known, the calibration could be done by a non trusted people – **Integrity**: if the code is modified, the identification won't succeed – Label **SECURITY**
CID	– **Confidentiality**: the data are nominative – **Integrity**: if the data are modified, they won't refer to the authorised person – Label **PERSONNAL**
DAD	– **Confidentiality** : the data are nominative – **Integrity**: if the data are modified, they won't reflect the reality – **Availability**: if the data are unavailable, they won't be checked – **Authenticity**: if the origin of the data can't be verified, the driver activities data can't be trusted – **Non repudiation**: if the date are repudiable, the driver activities data could be rejected – Label **PERSONNAL**
WL & BL	– **Confidentiality** : the data are nominative – **Integrity**: if the data are modified, a card can be wrongly tested OK or not – **Availability**: if the data are unavailable, the cards can't be controlled – Label **PERSONNAL**
Annual report	– **Confidentiality**: if the data are known, an offender could use them to find some vulnerabilities to hijack the security – Label: **SECURITY**
Tachograph cards	– The objectives are as those for the data stored and manipulated – Label: **SECURITY** and **PERSONNAL**
MS	– The objectives are as those for the data stored and manipulated – Label: **SECURITY**
VU	– The objectives are as those for the data stored and manipulated – Label: **SECURITY**

Annex(e) B Security Requirement and entities

The purpose of this annex is an argumentation to justify the entities concerned by the TS security requirements. The procedures described regarding the security requirements might be included in the security policy of each entity concerned.

	European Root Certification Authorities	Member State Authorities	Member State Certification Authorities	Cards Manufactures	Card Key Generation	Card Personalisers	Card Issuing Authorities	Motion Sensor Manufactures	Key Pairing Generation	VU Manufactures	VU Key Generation	Workshop	Road Haulage Companies	Drivers	Control Body
	ERCA	MSA	MSCA	CM	CKG	CP	CIA	MOM	KPG	VUM	VUKG	W	RHC	D	CB
M.Activation		X										X			
M.Approved_Workshops		X										X	X		
M.Card_Availability		X					X					X	X	X	X
M.Card_Traceability		X					X								X
M.Controls		X													X
M.Delivery		X						X		X		X			
M.Development		X						X		X					
M.Driver_Card_Uniqueness		X					X							X	X
M.Faithful_Calibration		X										X			
M.Faithful_Drivers		X												X	X
M.Manufacturing		X						X		X					
M.Mechanical_Interface		X										X			X
M.Regular_Inpections		X										X	X		X
M.Sec_Data_Generation	X	X	X			X		X	X	X	X				
M.Sec_Data_Transport	X	X	X			X		X	X	X	X	X			
M.Software_Upgrade		X						X		X					
O.DLV_DATA		X		X	X	X	X								
O.TEST_OPERATE		X		X		X									
O.USE_DIAG				X						X					
O.USE_SYS				X						X	X				
O.EnvICESPP_CM		X		X											

ID	Requirements	Concerned entities
M.Activation	Vehicle manufacturers and fitters or workshops must activate the VU after its installation and before the vehicle leaves the premises where installation took place .	MSA: the Member State Authority carry out regularly and randomly security assessments upon the entities within its jurisdiction W : Vehicle manufacturers and fitters or workshops activate the VU after the calibration with their workshop card.
M.Approved_ Workshops	Installation, calibration and repair of recording equipment must be carried by trusted and approved fitters or workshops.	MSA: the Member State Authority is responsible for the approval of the vehicle manufacturers and fitters or workshops W: fitters or workshops set up an organisation able to obtain and maintain the require approval RHC: the company is responsible for using vehicle manufacturers and fitters or workshops approved
M.Card_Availability	Tachograph cards must be available and delivered to authorised persons only.	MSA: a trusted process of delivery will be defined by MSA. An acknowledgement process after receiving the card or a face to face communication between an authority and the cardholder might be required by MSA W, RHC, D, and CB: Each card request is processed with the holder identification data, the cardholder may be required to present himself for the card delivery or send an acknowledgement of receipt and to sign the card. CIA: The card issuing authority control the holder identification data and the acknowledgement of receipt if it is required.
M.Card_Traceability	Card delivery must be traceable (white lists, black lists), and black lists must be used during security audits.	MSA/CIA: The card issuing authority and the Member State Authority will make available to control bodies and other Member States detail of valid and invalid cards. MSA : the Member State Authority use this information for audits. CIA: The card issuing authority manage this information CB: the control bodies use this information for when they control the cards.

ID	Requirements	Concerned entities
M.Controls	Law enforcement controls must be performed regularly and randomly, and must include security audits.	MSA: the Member State Authority is responsible for the applicability of the security policy and carry out regularly and randomly security assessments upon the entities within its jurisdiction CB: control bodies are in charge to control regularly and randomly driver activities on the road and in the company
M.Delivery	Motion sensor (resp. VU) manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of the motion sensor (resp. VU) is done in a manner which maintains IT security.	MSA: the Member State Authority is responsible for the approval of the MOM, VUM manufacturers and fitters or workshops MOM, VUM: Motion sensor and VU manufacturers set up the security measures, which maintains IT security when the Motion sensor and VU personalisation is done. W: fitters or workshops set up the security measures, which maintains IT security when calibration is done.
M.Development	Motion sensor (Resp VU) developers must ensure that the assignment of responsibilities during development is done in a manner which maintains IT security.	MSA: the Member State Authority is responsible for the approval of Motion sensor and VU manufacturers MOM, VUM: Motion sensor VU manufacturers set up the organisation, which maintains IT security during the development of Motion sensor and VU.
M.Driver_Card_Uniqueness	Drivers must possess, at one time, only one valid driver card.	MSA: the Member State Authority produce an annual report CIA: The card issuing authority manage the issue, the replacement, the renewal and the exchange of the cards D: Driver report to CIA the loss or robbery of their card or send back cards which have malfunction CB: control bodies detect and report the offence at the CIA
M.Faithful_Calibration	Approved fitters and workshops must enter proper vehicle parameters in recording equipment during calibration.	MSA: the Member State Authority is responsible for the approval of fitters or workshops W: fitters or workshops set up the security measures, which check the parameters entered during calibration.

ID	Requirements	Concerned entities
M.Faithful_Drivers	Drivers must play by the rules and act responsibly (e.g. use their driver cards, properly select their activity for those that are manually selected, …).	MSA: the Member State Authority produce an annual report D: drivers must apply the law or regulation and might sign a commitment paper. They are responsible of the use of their card. CB: control bodies detect and report the offence at the NA
M.Manufacturing	Motion sensor (resp VU) manufacturers must ensure that the assignment of responsibilities during manufacturing is done in a manner, which maintains IT security, and that during the manufacturing process the motion sensor (resp. VU) is protected from physical attacks, which might compromise IT security.	MSA: the Member State Authority is responsible for the approval of Motion sensor and VU manufacturers MOM, VUM : Motion sensor and VU manufacturers set up the organisation which maintains IT security during the manufacturing of Motion sensor and VU, and set up the security measures which protect this equipment form physical attacks
M.Mechanical_Interface	Means of detecting physical tampering with the mechanical interface must be provided (e.g. seals)	MSA: the Member State Authority produce an annual report W: fitters or workshops set up the security measures which protect the Motion sensor and VU form physical attacks after the calibration CB: control bodies detect and report the offence at the NA
M.Regular_Inpections	Recording equipment must be periodically inspected and calibrated.	MSA: the Member State Authority produce an annual report W: fitters or workshops inspect periodically the vehicle and report the offence at the NA RHC: company are responsible of the periodic inspection of their vehicle by approved fitters or workshops CB: control bodies detect and report the offence at the MSA on the road or in the company
M.Sec_Data_Generation	Security data generation algorithms must be accessible only to authorised and trusted persons.	MSA: the Member State Authority carry out regularly and randomly security assessments upon the entities within its jurisdiction ERCA, MSCA, CP, MOM, KPG, VUM, VUKG: these entities set up the security measures to protect security data concerning Motion sensor or VU generation algorithms from unauthorised and trusted persons

ID	Requirements	Concerned entities
M.Sec_Data_Transport	Security data must be generated, transported, and inserted into the motion sensor (Resp VU), in such a way to preserve its appropriate confidentiality and integrity.	MSA: the Member State Authority and carry out regularly and randomly security assessments upon the entities within its jurisdiction ERCA, MSCA, CP, MOM, KPG, VUM, VUKG: these entities set up the security measures to protect security data generated, transported and inserted in the MS and VU
M.Software_Upgrade	Software revisions must be granted security certification before they can be implemented in a motion sensor (resp VU).	MSA: the Member State Authority is responsible for the approval of the modification MOM, VUM: Motion Sensor and VU manufacturers notify the modification at the MSA and are responsible for the upgrade.
O.DLV_DATA	The Application Data must be delivered from the Tachograph card embedded software developer (phase 1) either to the IC Packaging manufacturer, the Finishing Process manufacturer or the Personalizer through a trusted delivery and verification procedure that shall be able to maintain the integrity and confidentiality of the Application Data.	MSA: the Member State Authority carry out regularly and randomly security assessments upon the entities within its jurisdiction CM: cards manufacturers have trusted procedure concerning delivery of blank TC, CKG : cards key generation have trusted procedure concerning delivery of card Secret Key to CP CP: cards Personalisers have trusted procedure concerning delivery of personalised TC, CIA: cards issuing authorities have trusted procedure concerning delivery of PinCode and personalised TC
O.TEST_OPERATE	Appropriate functionality testing of the TOE shall be used in phases 4 to 6. During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.	MSA: the Member State Authority carry out regularly and randomly security assessments upon the entities within its jurisdiction CM, CP: cards manufacturers and cards Personalisers have security procedures concerning protection of manufacturing data and test operation (including personalisation keys).
O.USE_DIAG	Secure communication protocols and procedures shall be used between the Tachograph card and the card reader terminal.	CM and VUM: cards manufacturers and equipment manufacturers implement the common security mechanisms (Appendix 11 of Annexe 1B) in the TC and VU
O.USE_SYS	The integrity and the confidentiality of sensitive data stored / handled by the system (terminals, communications...) shall be maintained	CM and VUM: cards manufacturers and equipment manufacturers implement the common security mechanisms (Appendix 11 of Annexe 1B) in the TC and VU

ID	Requirements	Concerned entities
O.EnvICESPP_CM	The other physical, personal or procedural requirements upon environment that contribute to the security of tachograph card which are listed in [IC PP] and [ES PP] (chapters security objectives for the environment) and concern the card manufacturers	CM: Card manufacturers have the procedure that ensure protection on software - hardware development and testing programs and tools, protection during the manufacturing delivery of raw cards. MSA: the Member State Authority carry out regularly and randomly security assessments upon the entities within its jurisdiction

Detail of the other physical, personnel or procedural requirements that contribute to the security of the tachograph card which are listed in [IC PP] and [ES PP] (chapters security objectives for the environment) and concern the card manufacturers.

IC PP	
O.DEV_DIS	The IC designer must have procedures to control the sales, distribution, storage and usage of the software and hardware development tools and classified documentation, suitable to maintain the integrity and the confidentiality of the assets of the TOE. It must be ensured that: • tools are only delivered to the parties authorized personnel, • confidential information such as data sheets and general information on defined assets are only delivered to the parties authorized personnel on the need to know basis.
O.SOFT_DLV	The smartcard embedded software must be delivered from the smartcard embedded software developer (Phase 1) to the IC designer through a trusted delivery and verification procedure that shall be able to maintain the integrity of the software and its confidentiality, if applicable.
O.SOFT_MECH	To achieve the level of security required by a given security target based on this Protection Profile, the smartcard embedded software shall use IC security features and security mechanisms as specified in the smartcard IC documentation (e.g. sensors,...).
O.DEV_TOOLS	The smartcard embedded software shall be designed in a secure manner, by using exclusively software development tools (compilers, assemblers, linkers, simulators etc...) and software-hardware integration testing tools (emulators) that will grant the integrity of program and data.
O.SOFT_ACS	Smartcard embedded software shall be accessible only by authorized personnel within the IC designer on the need to know basis.
O.DESIGN_ACS	IC specifications, detailed design, IC databases, schematics/layout or any further design information shall be accessible only by authorized personnel within the IC designer on the basis of the need to know (physical, personnel, organisational, technical procedures).
O.DSOFT_ACS	Any IC dedicated software specification, detailed design, source code or any further information shall be accessible only by authorized personnel within the IC designer on the need to know basis.
O.MASK_FAB	Physical, personnel, organisational, technical procedures during photomask fabrication (including deliveries between photomasks manufacturer and IC manufacturer) shall ensure the integrity and confidentiality of the TOE.
O.MECH_ACS	Details of hardware security mechanisms specifications shall be accessible only by authorized personnel within the IC designer on the need to know basis.
O.TI_ACS	Security relevant technology information shall be accessible only by authorized personnel within the IC designer on the need to know basis.

O.TOE_PRT	The manufacturing process shall ensure the protection of the TOE from any kind of unauthorized use such as tampering or theft. During the IC manufacturing and test operations, security procedures shall ensure the confidentiality and integrity of the TOE manufacturing data and security relevant test programs, test data, databases and specific analysis methods and tools.
O.IC_DLV	The delivery procedures from the IC manufacturer shall maintain the integrity and confidentiality of the TOE and its assets.
O.DLV_AUDIT	Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non conformance to this process.
O.DLV_RESP	Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and to act to be fully in accordance with the above expectations.

ES PP	
O.DEV_DIS_ES	The Embedded Software developer shall use established procedures to control storage and usage of the classified development tools and documentation, suitable to maintain the integrity and the confidentiality of the assets of the TOE. It must be ensured that tools are only delivered and accessible to the parties authorized personnel. It must be ensured that confidential information on defined assets is only delivered to the parties authorized personnel on a need to know basis.
O.INIT_ACS	Initialization Data shall be accessible only by authorized personnel (physical, personnel, organizational, technical procedures).
O.SAMPLE_ACS	Samples used to run tests shall be accessible only by authorized personnel.
O.DLV_PROTECT*	Procedures shall ensure protection of TOE material/information under delivery including the following objectives: • non-disclosure of any security relevant information, • identification of the element under delivery, • meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment), • physical protection to prevent external damage • secure storage and handling procedures (including rejected TOE's) • traceability of TOE during delivery including the following parameters: • origin and shipment details • reception, reception acknowledgement, • location material/information.

Annex(e) C Main items of ISO 17799

This standard gives a set of recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organisation:

- 3. SECURITY POLICY: Management's commitment to enforce security / security principles, rules and organisational security procedures definition
- 4. SECURITY ORGANIZATION: Define roles and responsibilities as regards security
- 5. ASSETS CLASSIFICATION AND CONTROL: Information/material classification and protection management procedure
- 6. PERSONNEL SECURITY: Personnel vetting / Employment contract / signature of an individual non disclosure commitment by the personnel
- 7. PHYSICAL AND ENVIRONMENTAL SECURITY: Physical security of the premises / physical access control to the equipment
- 8. COMMUNICATIONS AND OPERATIONS MANAGEMENT: Networks, operating systems and software security / security problem reporting and corrective action procedure
- 9. ACCESS CONTROL. : Passwords management / access rights management / access logging / remote access
- 10. SYSTEMS DEVELOPMENT AND MAINTENANCE: Securing development process / system testing and validation / maintenance
- 11. BUSINESS CONTINUITY MANAGEMENT: Disaster recovery plan and associated testing procedures
- 12. COMPLIANCE: Compliance with regulation / periodic security audit

Annex(e) D Main items of ETSI 178 T2

This standard defines a set of policy requirements on the operation and management practices of certification authorities issuing public key certificates:

- 5. INTRODUCTION TO CERTIFICATES POLICIES: effectiveness, identification, applicability of the certificate policy and conformance with this standard
- 6. OBLIGATIONS AND LIABILITY: certification authority, subscriber, relying party obligations and liability
- 7.1. CERTIFICATION PRACTICE STATEMENT: reliability for providing certification services
- 7.2. PUBLIC KEY INFRASTRUCTURE – KEY MANAGEMENT LIFE CYCLE: certification authority key generation / storage, backup and recovery / distribution / escrow / usage, end of key life cycle, life cycle management of cryptographic hardware used to sign certificates
- 7.3. PUBLIC KEY INFRASTRUCTURE – CERTIFICATE MANAGEMENT LIFE CYCLE: subscriber certificate request control and registration, certificate renewal / generation / dissemination/ revocation and suspension
- 7.4. CA MANAGEMENT AND OPERATION: security management, asset classification and management, personnel security, Physical and environmental security, operations management, system Access management. Trustworthy Systems development and maintenance, Business continuity management and incident handling, CA termination, Compliance with legal requirements, Recording of information concerning certificate
- 7.5. ORGANISATIONAL: reliability and independence of the organisation