Bundesministerium
für Verkehr, Bau
und Stadtentwicklung

Digital-Tachograph-System in road traffic

German Policy

Version 1.3
24.11.2008

0.1 Document version control15

Titel	Digital-Tachograph-System in road traffic German Policy		
Author	Claus-Christian Brockstedt, Kraftfahrt-Bundesamt (Federal Motor Transport Authority)	Version	1.3
		Date	24.11.2008

Version	Date	Changed Chapters	Description
0.1	12.09.2002	All	Initial draft
0.2	13.11.2002	All	Customisation regarding the tasks of the KBA
0.3	23.07.2004	All	Customisation ERCA-Policy 2.0 / draft for approval by the ERCA
1.0	04.11.2004		approved version 1.0
1.1	16.12.2005	All 3. / 4. 3.1	Renamed from „certification policy D-CA“ to „D-MSA-Policy“ Inclusion of D-CIA-tasks Obligation to draw-up a CPS extended to D-CP and manufacturers of vehicle-units and motion-sensors; Integration of keys and certificates into not yet type-approved equipment
1.2	18.04.2007	0.1 / 0.2 1. 1.2 3.1 9.3 3.2; 9.1; 9.2; 9.3; 10; 10.1 6.	Inclusion of dokument version control and index of contents Inclusion of the addresses of D-CA, D-CP and manufacturers of vehicle-units and motion-sensors amendment: the German version is mandatory [r3.6] letter f (integrate keys and certificates only in type-approved equipment) deleted because such a regulation is not to be found in the policies of France and Sweden erasure of SysA function after combination with CA-Administrator function; inclusion of SysAdmin function for the D-CP extend the scope to D-CP erasure:manufacurer
1.3	24.11.2008	1.1 3.6	New Manufacturer Efkon Letter f) deleted because not available in the policies of France and Sweden

0.2 Index of contents

1. Introduction

This document is the certification policy of the Federal Republic of Germany, hereinafter referred to as **the D-MSA Policy**, for the electronic tachograph as per supplement 11 of appendix I (B) of Regulation (EC) 2135/98 combined with 1360/2002 (CSM_008).

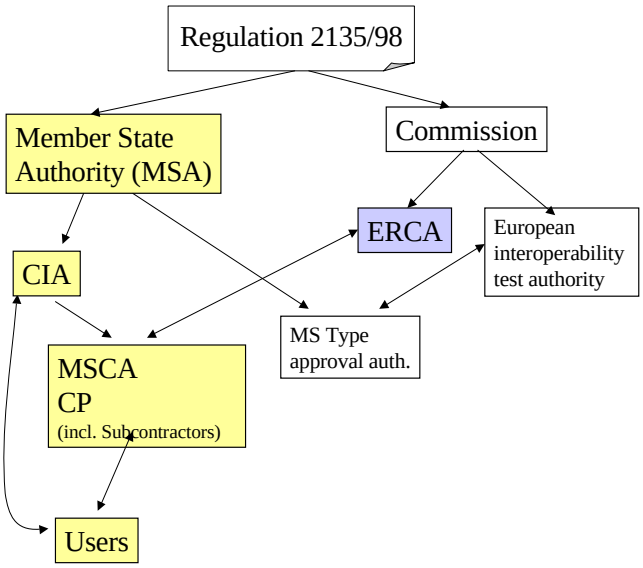
The D-MSA Policy is compatible with

- Digital Tachograph System, - European Root Policy (Version 2.0 – Special Publication I.04.131)
- Regulation (EC) 3821/85
- Regulation (EC) 2135/98
- Regulation (EC) 1360/2002
- Regulation (EC) 561/2006
- "Common Security Guideline"[1]

[1] Common Security Guidelines, v1.0; Card Issuing Group SWG3:
http://forum.europa.eu.int/Public/irc/tren/digtacho/library?l=/commonssecuritysguidelin/commonsecurityguideline1/_EN_1.0_&a=d

1.1. Responsible organisations

The tachograph system has the following organisation[2]:



The authority responsible for implementing Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002 in Germany is referred to as **D-MSA** (Deutschland-Member State Authority) in the following as per international usage and is looked after by the Federal Ministry of Transport, Building and Housing (BMVBS). The official contact is:

D-MSA

Federal Ministry of Transport, Building and Urban Affairs
Referat S36
Robert Schuman-Platz 1
D-53175 Bonn
Telephone: +49 228 300-5365
Fax: +49 228 300-1470

D-CA

The D-MSA assigns the Federal Motor Transport Authority (KBA) with the responsibility of looking after **D-CA tasks**

Kraftfahrt-Bundesamt
Leiter der D-CA
Fördestraße 16
D-24944 Flensburg
Telephone: +49 461 316-1610
Fax: +49 461 316-1767

---

[2] Guideline and Template National D-MSA-Policy, V 1.0
http://forum.europa.eu.int/Public/irc/tren/digtacho/library?l=/commonssecuritysguidelin/tsncapolicysguidelinesv1/_EN_1.0_&a=d

D-CP

The D-MSA assigns the Federal Motor Transport Authority (KBA) with the responsibility of looking after D-CP tasks

Kraftfahrt-Bundesamt
Personalisierungsstelle
Fördestraße 16
D-24944 Flensburg
Telephone: +49 461 316-1240
Fax: +49 461 316-1822

An important part of this is the responsibility for the implementation of the D-MSA-Policy. The D-CA can subcontract (parts of) its tasks to external service providers. By doing so, the responsibility of the D-CA is in no way restricted.

D-CIA

Performing the tasks of **D-CIA** is determined by the Federal States individually.

Manufacturers of vehicle-units and motion-sensors

Siemens AG
Siemens-VDO Automotive
Commercial Vehicles
Heinrich-Hertz-Straße 45
D-78052 Villingen-Schwenningen
Telephone: +49 7721/67-0
Fax: +49 7721/7847

EFKON AG
c/o Flextronics International KFT
Zrinyi ut. 38
H-8900 Zalaegerszeg
Hungry

1.2. Approval

The D-MSA-Policy was submitted to the EU Commission by the D-MSA and approved by

European Commission
Directorate General JRC
Joint Research Centre
Institute for the Protection and Security of the Citizen
Traceability and Vulnerability Assessment Unit
TP 361
I-21020 Ispra (Va)
Italy

on 04.12.2008[3] (reg. A(2008) 18154).

1.3. Availability and contact details

The D-MSA-Policy is available in electronic form from the web site http:/www.kba.de.

Questions and contact details for this D-MSA-Policy should be addressed to:

Federal Ministry of Transport, Building and Urban Affairs
Referat S36
Robert Schuman-Platz 1
D-53175 Bonn
Telephone: +49 228 300-5365
Fax: +49 228 300-1470

[3] The D-MSA-Policy is worded in German and translated into English in order to be sent to ERCA. The German version is the one which is authentic on a legal basis.

2. Scope

[r2.1]

The validity of the D-MSA-Policy exclusively covers performance of tasks within the scope of Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002.

[r2.2]

D-MSA and D-CA ensure that certificates produced and keys generated by the D-CA are used only for those purposes defined in Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002 within the framework of their individual jurisdictions and the relevant valid provisions.

[r2.3]

The scope of this D-MSA Policy is marked in bold in the following overview[4]:

[4] Cp. Digital Tachograph System European Root Policy, V 2.0

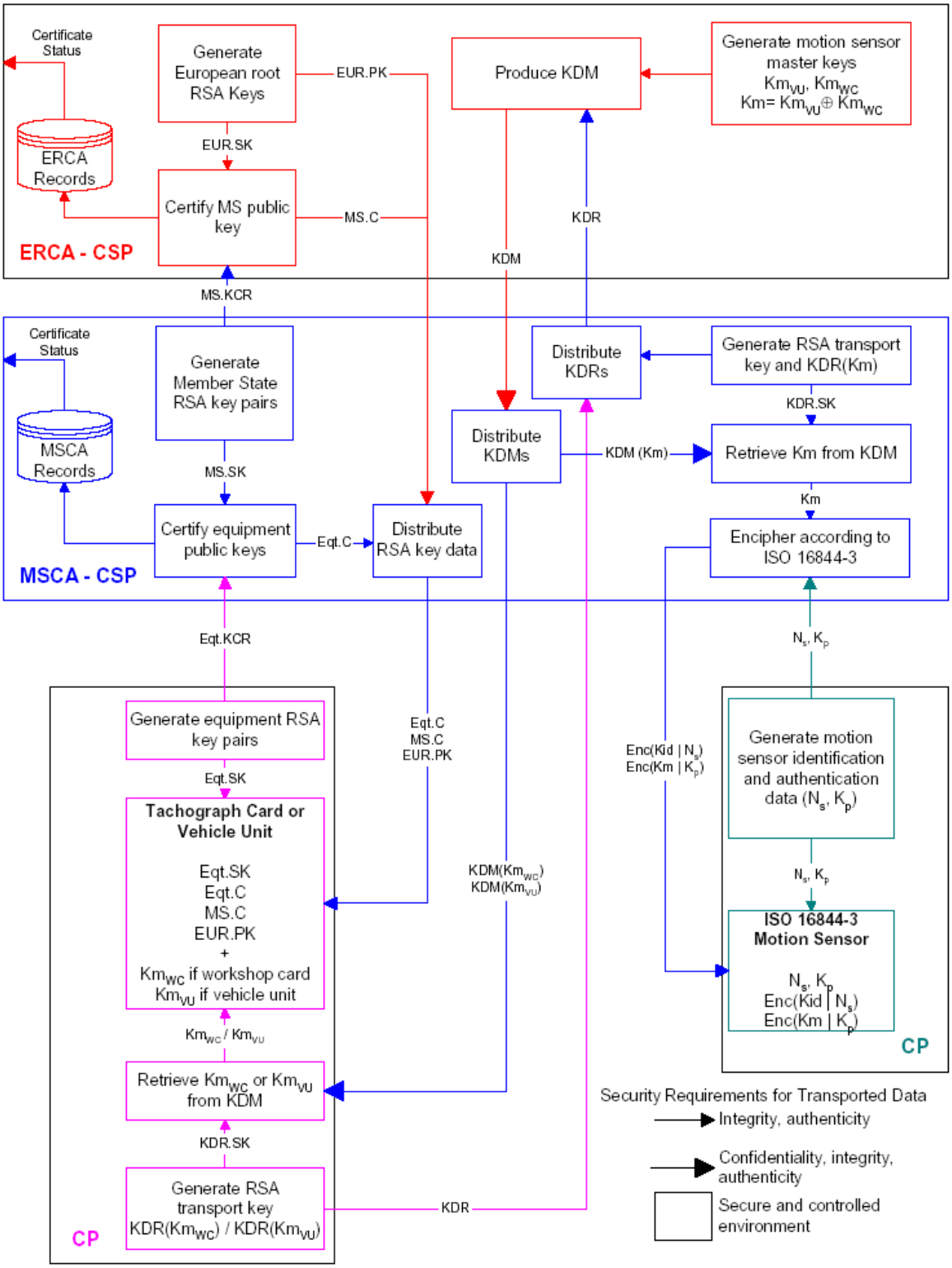


Figure 1 Description of Annex I(B) key management

3. General provisions

3.1. Duties and responsibilities

This section describes the duties and responsibilities of the authorities involved in the implementation of Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002 as long as these concern the scope of the D-MSA-Policy.

[r3.1]

The **D-MSA**:

a) performs its tasks in coordination with the states,
b) is responsible for drawing up and implementation of the D-MSA-Policy and arranges for its approval by the Commission,
c) nominates the D-CA and announces this nomination to the Directorate-General for Energy and Transport of the European Union (DG TREN),
d) nominates the D-CP or subcontracts these tasks to an external service provider,
e) can execute or arrange for inspection of the D-CA, the D-CP, the D-CIA, the manufacturers and further external service providers, if necessary,
f) ensures or arranges that the D-CA receives all information required for its work in a correct manner,
g) approves the Practice Statement (PS) of the D-CA, the D-CP, manufacturers of vehicle units and manufacturers of motion sensors and the PS of other external service providers, if necessary,
h) ensures or arranges that the D-MSA-Policy is made available to the authorities involved.
i) immediately informs the ERCA or one of its authorised agencies about all security-relevant incidents related to production, personalisation and use of their equipment as well as the keys and certificates integrated in them.

[r3.2]

The **D-CA**:

a) carries out, within the scope of its operations, the requirements of Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002, of all the relevant legal provisions, the Root Policy and this D-MSA-Policy,
b) draws up a PS, in which at least the method of implementation of the D-MSA-Policy, Root Policy and legal provisions is explained,
c) provides for personnel and materials required for the proper fulfilment of its tasks,
d) bears the responsibility for proper execution of its tasks also when these or parts of these are subcontracted to external service providers. In this case, it has to ensure that these adhere to the relevant requirements of the D-MSA-Policy and the PS in their operations.
e) immediately informs the D-MSA or one of its authorised agencies and if necessary the ERCA about all security-relevant incidents related to production, personalisation and use of their equipment as well as the keys and certificates integrated in them.

[r3.3]

The **D-CIA**:

a) verifies wether all required documents were produced,
b) verifies whether all prerequisites for the issuing of a tachograph card subject to the Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002, all other relevant legal provisions, the Root Policy and this D-MSA-Policy are fulfilled,
c) verifies before the order of a tachograph card whether a tachograph card was already issued to the applicant in another EU-memberstate,

d) ensures that the application data is transmitted to the D-CP properly according to the produced documents and to the requirements of the D-CP and this Policy,

e) informs all users about the requirements of this policy in an appropriate manner,

f) ensures that the PIN of the workshop card is handed over only to the intended bearer of the workshop card.

g) immediately informs the D-MSA and the D-CA or one of its authorised agencies about all security-relevant incidents.

[r3.4]

The **D-CP**:

a) carries out, within the scope of its operations, the requirements of Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002, all other relevant legal provisions, the Root Policy and this D-MSA-Policy,

b) signs – as long as it deals with an external service provider – a contract with the D-MSA, in which it commits to fulfil its duties as per a),

c) draws up a PS, in which at least the method of implementation of the D-MSA-Policy, Root Policy and legal provisions is explained,

d) shows the D-MSA concrete execution of its duties in its current operations in a suitable manner,

e) permits the D-MSA or one of its authorised agencies to evaluate the practical execution of its duties.

f) immediately informs the D-CA or one of its authorised agencies about all security-relevant incidents related to production, personalisation and use of their equipment as well as the keys and certificates integrated in them.

[r3.5]

The **Card holder/Applicant**:

is obliged:

a) to give true information regarding the application data,

b) to give true information regarding available cards and card varieties at the time of submitting the application.

c) to ensure in an appropriate manner, that his card is used for the stated purpose only and to prevent its misuse especially by third persons.

d) to ensure that he is in possession of a single valid driver card,

e) not to use damaged and expired cards,

f) to inform the responsible authority about loss, theft, damage or misuse of the card and/or of the respective private key or of suspicion of the same.

[r3.6]

Manufacturers of vehicle units and **manufacturers of motion sensors** have to especially ensure that they

a) observe the requirements, which are relevant to them, of Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002, of all other laws and decrees relevant in this regard, especially of this D-MSA-Policy, to the best of their knowledge and according to the respective current technological developments,

   aa) that the integrated keys and certificates or those to be integrated in the equipment manufactured by them can be used only for proper purposes within the scope of Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002,

   ab) take measures in order to ensure the confidentiality of the private as well as secret keys during the complete production process and also during the total service period of the equipment.

b) provide the D-MSA with names of all external service providers subcontracted with the responsibility of production and personalisation of their equipment at all required times and make it obligatory for them to adhere to the corresponding requirements. As long as the manufacturer passes on his tasks to a third party, his rights and duties remain unaffected by the same.

c) draw up a PS, in which at least the method of implementation of the D-MSA-Policy, Root Policy and legal provisions is explained,

d) immediately inform the D-MSA or one of its authorised agencies about all security-relevant incidents related to production, personalisation and use of their equipment as well as the keys and certificates integrated in them.

e) permit the D-MSA or one of its authorised agencies to evaluate the practical execution of their duties.

[r3.7]

Manufacturers of Tachograph Cards or suppliers - so far they have obtained an IT security certificate - have to undergo for the composite smartcard product to an assurance maintenance process for the IT security certificates through the BSI Certification Scheme. This includes surveillance of the certified composite smartcard products on a regular basis (1 year) concerning resistance to relevant attacks in accordance with the Security Targets. The BSI reports the results to the MSA.

3.2. Special provisions

The D-CA/D-CP as well as the service providers authorised by it fulfil their tasks in accordance with applicable law, especially Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002 and the national provisions enacted for its implementation.

The legal provisions mentioned in this section are *not* exhaustive.

[r3.8] **Data protection**

The D-CA/D-CP ensures that the provisions of the Federal Data Protection Act and further relevant data protection provisions for dealing with personal data are adhered to within the scope of their authority.

[r3.9] **Electronic signatures**

The certificates produced by the D-CA are used for verification of electronic signatures as defined by the Act establishing a framework for electronic signatures (Signature Act). The certificates are *not qualified* certificates as defined by the Signature Act. The D-CA ensures that it as well as the external service providers authorised by it adhere to the requirements (§14) of the Signature Act resulting from this.

4. Practice Statement (PS)

[r4.1]

The D-CA, D-CP, manufacturers of vehicle units and manufacturers of motion sensors draws up and maintains a PS, which shows in the form of concrete measures to be implemented, how the adherence to this D-MSA-Policy, the Root Policy and the legal provisions relevant for the work is ensured in the operation. This PS consists of a tabular overview, which indicates where the requirements of this policy are implemented in the PS.

[r4.2]

The PS must provide the names of all the external service providers and their concrete tasks as well as explain which requirements of the D-CA, D-CP, manufacturers of vehicle units and manufacturers of motion sensors have to be adhered to by these service providers.

[r4.3]

The PS must explain how the D-CA, D-CP, manufacturers of vehicle units and manufacturers of motion sensors fulfils its duties regarding the information-management.

[r4.4]

A revision process must be described in the PS which ensures that the PS always corresponds to the current developments in legislation, technology and prevailing conditions at the D-CA, D-CP, manufacturers of vehicle units and manufacturers of motion sensors and its external service providers.

[r4.5]

The D-CA, D-CP, manufacturers of vehicle units and manufacturers of motion sensors submits its PS to the D-MSA for approval. Significant changes in the PS likewise require an approval by the D-MSA. The D-CA, D-CP, manufacturers of vehicle units and manufacturers of motion sensors ensures that the D-MSA is always provided with the latest version of the PS.

[r4.6]

The PS contains a listing of incidents which could lead to compromising of keys. This listing must be treated as confidential.

The creation of single Practice Statements by the D-CIAs is set aside due to the number of more than 600 D-CIAs. Corresponding supplementary regulations for the D-CIAs were included in section 3 and 5 of this D-MSA Policy.

5. Card and equipment management

[r5.1]

The D-CA ensures as per the instructions of the D-MSA and jointly with it within its authority that the certificates produced by it and the secret keys delivered by it are integrated and implemented, corresponding to their intended purpose, only in recording equipment cards and recording equipment which meet the requirements of Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002.

[r5.2]

The D-CA refuses to deliver keys and certificates if there is an increased risk of these keys and certificates being misused.

[r5.3]

The D-CIA guarantees adherence to application and delivery procedures for recording equipment cards defined by the D-MSA according to the instructions of Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002.

[r5.4]

The D-CIA ensures within its authority that issuing of replacement cards and card renewal takes place only as per the prerequisites mentioned in Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002 and that the prescribed time limits can be adhered to.

[r5.5]

The D-CP ensures that the recording equipment cards are personalised logically according to the instructions of Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002. The integrity of the entered data must be especially maintained in this respect.

[r5.6]

The D-CA, D-CP and the manufacturers ensure within their respective authority that private and secret keys are stored and used in a secured production environment.

[r5.7]

The D-CIA makes the relevant data available to the Central Register at KBA in a way that it is traceable to whom which card was issued.

[r5.8]

The D-CIA ensures that personalised cards are safely delivered within the time limits given by Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002 and that they can be traced to their bearer/user. A prerequisite for issuing personalised cards to a bearer/user is that he was personally identified at the time of applying and/or at the time of handing over the card. Inasmuch as the cards are not issued to a physical person, the applicant and the receiver of the cards must be able to show sufficient proof of identity.

[r5.9]

The D-CP ensures that the workshop cards are provided with a PIN as per the instructions of Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002.

[r5.10]

The PIN is generated in a system secured against unauthorised access. This system prevents the possibility of an assignment of the PIN and the Workshop Card after issuing. After generation, the PIN is printed on an online printer, sealed in an envelope (PIN letter) and delivered only to that person to whom the Workshop Card was made out.

The system used for PIN generation and PIN letter generation must at least fulfill the requirements of ITSEC E3, Common Criteria EAL 4, FIPS 140-2 (or 140-1) level 3 or an equivalent IT security criteria document or is demonstrated to provide an equivalent level of security

[r5.11]

PIN letters must be delivered under separate cover and not along with the personalised cards. They can be delivered by mail.

[r5.12]

The reconstruction of a PIN must be impossible.

6. Key management within the D-CA

This section contains the requirements of dealing with the following key material by the D-CA (the abbreviations possibly used in the Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002 are given in brackets):

- the public key of the Root CA (EUR.PK),
- the key pair of the D-CA (MS.SK, MS.PK),
- symmetric keys for distance and motion sensors (Km, $Km_{WC,}$ Km_{VU}),
- if required, transport keys for communication with the Root CA and
- if required, exclusive transport keys of the D-CA.

The D-CA ensures within its domain the confidentiality and integrity of all non-public keys generated, used and/or stored with it and effectively prevents any misuse of these keys. For this purpose, it has to employ suitable technical systems, which fulfil one of the following requirements:

- FIPS 140-2 (or 140-1) level 3 or higher [FIPS],
- CEN Workshop Agreement 14176-2 [CEN],
- certification according to EAL 4 or higher in accordance with ISO 15408 [CC] to level E3 or higher [ITSEC] based on a protection profile or security instructions ("Security Targets"), which encompasses the requirements of this D-MSA-Policy – based on a comprehensive risk analysis – as well as structural and non-technical security measures.
- security criteria, which provide an equivalent level of security.

In the same way, it has to be proved that these systems are operated in an adequately secured operating environment at the D-CA.

The D-CA will sign equipment certificates exclusively within the same device used to store the Member State Private Keys.

6.1. Public key of the Root CA (EUR.PK)

[r6.1]

The D-CA ensures that the integrity and availability of the EUR.PK key is guaranteed in its current operation.

[r6.2]

The D-CP and the manufacturers ensure that EUR.PK is integrated in all recording equipment cards and vehicle units within their authority.

6.2. Key pair of the D-CA (MS.SK, MS.PK)

[r6.3]

The D-CA shall possess different Member State Key Pairs for the production of vehicle unit public key certificates (undefined validity) and tachograph card equipment public key certificates (limited validity).

[r6.4]

The D-CA ensures that MS.SK is used exclusively for generating certificates for recording equipment cards, vehicle units and for production of the ERCA key certification request (KCR). This especially includes secrecy of the private key MS.SK.

[r6.5]

The generation of the D-CA key pair may take place only with the active participation of at least three different individuals within the D-CA. One of these individuals must assume the function of the CA administrator, the other two must each assume an other function, as described in the D-MSA-Policy.

[r6.6]

The D-CA should keep – within the scope of the instructions of the Root Policy – an adequate amount of substitute key pairs with the corresponding certificates, in order to execute a quick change of key, in case of non-availability of the real key, even without active participation of the Root CA. If several real key pairs are available, then the D-CA has to ensure that only the correct key is used at all times.

[r6.7]

Each private MS.SK key should be used for a maximum period of two years. After the end of its usage period, it has to be destroyed by the D-CA in such a manner that no future use or misuse is possible.

[r6.8]

The validity period of the member state public key MS.PK is unlimited.

[r6.9]

The D-CA has to effectively protect all private keys as well as all substitute keys from misuse, modification and unauthorised access using techno-organisational measures.

[r6.10]

The D-CA effectively prevents the access to MS.SK by a single person alone (“4-eyes-principle”) using techno-organisational measures.

[r6.11]

No key escrow of any private keys takes place, i.e. including equipment keys.

[r6.12]

The PS of the D-CA should contain explicit procedures in case the MS.SK is compromised or is potentially compromised. This procedures should also contain instructions for external service providers and information to cardholders and equipment manufacturers.

In case the keys EUR.SK, MS.SK, Km, $Km_{WC,}$ Km_{VU} are compromised or potentially compromised, the D-MSA and the Root CA have to be informed immediately.

In other cases of key-compromise or potential key-compromise appropriate measures are to be taken and information are to be given to the concerned institutions.

[r6.13]

The D-CA ensures in cooperation with the Root CA, that it possesses a valid key pair (MS.SK, MS.PK) with the corresponding certificate at any point of time.

[r6.14]

The D-CA submits MSCA public keys for certification by the ERCA using the key certification request (KCR) protocol described in Annex A of the Digital Tachograph System European Root Policy.

[r6.15]

The D-CA recognises the ERCA public key in the distribution format described in Annex B of the Digital Tachograph System European Root Policy.

[r6.16]

The D-CA uses the physical media for key and certificate transport described in Annex C of the Digital Tachograph System European Root Policy.

6.3. Symmetric keys for workshop cards and distance and motion sensors (Km, Km_{WC}, Km_{VU})

[r6.17]

If the need arises, the D-CA requests the Root CA for the distance and motion sensor keys Km, $Km_{WC,}$ Km_{VU}. Provisions of the Root CA have to be adhered to for the request and delivery of these keys between the Root CA and the D-CA.

[r6.18]

The D-CA, using suitable measures, ensures that the keys Km_{WC} and Km_{VU} are passed on only to the intended receiver and secures their forwarding using suitable measures. The D-MSA controls the security measures of the D-CA.

The D-CA ensures that the key Km is not passed on.

[r6.19]

In case, one of the keys Km_{WC} or Km_{VU} or especially Km is compromised or there is potentially compromised, the D-CA has to immediately inform the D-MSA and the Root CA.

[r6.20]

The D-CA requests motion sensor master keys from the ERCA using the key distribution request (KDR) protocol described in Annex D of the ERCA-Policy.

6.4. Transport keys of the Root CA

[r6.21]

In case the Root CA wants to give cryptographic keys for securing mutual communication to the D-CA, then their confidentiality and integrity has to be effectively protected by the D-CA and any misuse of the same has to be effectively prevented.

6.5. Exclusive transport keys of the D-CA

[r6.22]

In case the D-CA wants to give cryptographic keys to its communication partners (that is Personalisers, equipment manufacturers,...) for securing mutual communication, then their confidentiality and integrity has to be effectively protected by the D-CA and any misuse of the same has to be effectively prevented.

The D-CA requires its communication partners to meet equivalent security measures in their authority for the protection of the keys.

7. Key management of asymmetric card and equipment keys

This section contains requirements for the generation of and dealing with asymmetric cryptographic keys for recording equipment cards and recording equipment as well as the corresponding certificates. Requirements for the symmetric keys Km, $Km_{WC,}$ Km_{VU} can be found in section 6.3.

7.1. General requirements, record

[r7.1]

The D-MSA, D-CA, D-CP and the manufacturers ensure within their domain, that initialising, encrypting and personalising of cards and recording equipment takes place in a specially secured production environment. The access to these areas must be effectively restricted and controlled. Administration of the corresponding systems must necessitate the presence of at least two responsible persons as per the function concept.

Every approach and access to the systems as well as all actions carried out by them must be recorded in such a manner that their unauthorised modification is not possible and that the availability, confidentiality and integrity of the record is ensured even if a key is compromised.

[r7.2]

The D-MSA, D-CA, D-CP and the manufacturers ensure within their domain, that information such as private keys etc., critical for security purposes, is protected while initialising, encrypting and personalising cards and recording equipment as per the requirements of Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002 and the D-MSA-Policy.

[r7.3]

The D-MSA requires all possible external service providers to perform the accepted tasks completely separated from their other activities. This is especially applicable when the service provider undertakes tasks for CA's of other Member States.

The D-MSA requires all possible external service providers to record their activities according to [r7.1] in such a manner that it cannot be modified and to permit the D-MSA to get an overview of the record if required.

[r7.4]

The records made at the time of personalisation of cards and recording equipment must permit an assigning of the respective actions to the corresponding card/equipment number as well as the respective certificate.

7.2. Key generation

[r7.5]

The D-MSA, D-CA, D-CP and the manufacturers ensure within their domain, that the generation of keys takes place in a specially secured production environment, which especially guarantees secrecy of the respective private keys. For equipment to be used for this, the same requirements as for the equipment employed by the D-CA for the generation of the key pair are applicable.

[r7.6]

The D-MSA, D-CA, D-CP and the manufacturers ensure within their domain, that private keys are permanently deleted from the memory of the key generation and personalisation systems immediately after their integration into the respective cards or equipment, if key generation does not take place directly in the chip.

[r7.7]

The D-CA ensures that key duplication is very likely to be excluded within its area of responsibility.

[r7.8]

Key generation is allowed for stock-building (“Batch process”), if it is ensured with techno-organisational measures that a misuse of the stocked key pairs is prevented. The key supply shall not exceed the production quota of one month.

7.3. Key application

[r7.9]

The D-MSA, D-CA, D-CP and the manufacturers ensure within their domain, that the respective private keys can be exclusively used for their intended purpose according to Regulation (EC) (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002. This especially includes that no copies of these keys exist outside the secured environment of the recording equipment cards and recording equipment after the personalisation procedure is done.

[r7.10]

The D-CP, CIA ensures within its domain, that only those cards are delivered, whose optical and logical personalisation refer correctly to the cardholder.

[r7.11]

The Member State private keys may be backed up using a key recovery procedure requiring at least dual control.

[r7.12]

The D-CA and D-CP ensure within their domain, that private keys cannot be reused after expiry of the service period of a recording equipment card..

8. Certificate management

This section contains requirements regarding production and application of certificates created by D-CA during the life cycle of the concerned recording equipment cards and recording equipment.

8.1. Registration

[r8.1]

The D-CA ensures within its authority, that a proper registration of D-CP and manufacturers of vehicle units respectively takes place with responsible authorities before issuing of a certificate.

[r8.2]

Here, the D-CP has to specially ensure that the registration data permits a clear assignment of the “Certificate Holder Reference” as per the requirement CSM_017 from supplement 11 of appendix I (B) of Regulation (EC) 2135/98.

[r8.3]

If key generation takes place outside the D-CA, then the D-CA produces the certificate applied if D-CP and manufacturers of vehicle units respectively proofs by a pre-agreed procedure that he is in possession of the corresponding private key. At this time the private key should not leave the secured environment of key generation.

8.2. Certificate issuing

[r8.4]

The D-CA issues certificates when a proper certificate application is presented to the responsible authority and when all the requirements of Regulation (EC) (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002 and of all other associated legal provisions and agreements have been adhered to at the time of applying.

In case of an automated process, certificate production by manual intervention in the system must be completely prevented.

[r8.5]

The D-CA ensures within its domain, that the certificates produced by it are transferred only to D-CP and manufacturers of vehicle units respectively.

[r8.6]

The D-CA produces certificates only for equipment and cards, for which a component type-approval was issued and is valid or equipment that fulfil the requirements of [r3.6] letter f).

[r8.7]

Key certification requests that rely on transportation of private keys are not allowed.

8.3. Validity of certificate

[r8.8]

The validity period of certificates issued by the D-CA should not exceed the maximum usage period of the corresponding cards and/or equipment. Certificates for:

- Driver Cards not more than 5 years,
- Workshop Cards not more than 1 year,
- Control Cards not more than 5 years,
- Company Cards not more than 5 years,

as calculated from when the respective card is valid.

Certificates for vehicle units have an undefined validity.

8.4. Certificate contents and formats

[r8.9]

Contents and formats of the certificates produced by the D-CA meet the requirements of Regulation (EC) (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002, especially the specifications mentioned in supplement 11 of appendix I (B).

The D-CA creates all certificates with its private signature key.

The MSA ensures that the Key Identifier (KID) and modulus (n) of keys submitted to the ERCA for certification and for motion sensor key distribution are unique within the domain of the D-CA.

8.5. Information duties of the D-CA

[r8.10]

The D-CA transfers all certificate data to the D-CP and the manufacturers, so that certificates, equipment as well as cards and cardholders are interlinked.

[r8.11]

If certain authorities proof a legitimate interest in special, non-public information on the functioning of the D-CA or its external contractors, and no rules or security considerations are standing against the delivery of this information, the D-CA makes available the information as quickly as possible in coordination with the D-MSA.

[r8.12]

The operation concept of D-CA has to be treated with confidentiality. Information contained in it may be viewed in agreement with the D-MSA on location at D-CA, when there is a proven, legitimate interest and when the confidentiality of the information is also adequately protected at the receiver.

[r8.13]

The D-CA maintains and makes certificate status information available.

9. Information security

9.1. Information Security Management System (ISMS)

[r9.1]

The D-CA/D-CP and if necessary all the authorised service providers establish a suitable Information Security Management System (ISMS), which permanently guarantees IT security for all the work relevant to the tasks of the D-CA/D-CP .

The course of action has to meet the requirements of [ISO] 27001:2006 as well as [GSHB].

[r9.2]

The D-CA/D-CP ensures that an assessment of the protection requirement according to [GSHB] is carried out for all IT systems and information relevant to the D-CA/D-CP.

[r9.3]

A security concept must be created for the work of the D-CA/D-CP. This concept must be adapted to the operation concept.

[r9.4]

Drawing up and implementation of the operation concept are a part of Information System Security Management.

9.2. Special requirements of the security concept

The following section summarises the factors to be *particularly* taken care of within the security concept. It is *not* meant to be a definitive listing of its contents.

[r9.5]

The D-CA/D-CP ensures that only trustworthy and sufficiently qualified persons are entrusted with the necessary tasks. This is also applicable for personnel of external contractors.

[r9.6]

IT systems implemented for the work of the D-CA/D-CP and if necessary of external service providers must be operated in such a manner that possible damages due to viruses and other malicious coding are prevented as far as possible and the possible consequences of damages and disturbances are minimised.

The systems must have effective access controls and must particularly implement the functional concepts described in this policy and in the accompanying security and operation concept effectively.

[r9.7]

Initialisation of systems, which contain the private signature key of D-CA or the secret symmetric keys Km_{VU}, Km_{WC} or Km may take place only in cooperation of two persons, which is ensured by organisational measures..

[r9.8]

The D-CA/D-CP should implement trustworthy systems and software for their tasks, which are effectively protected using suitable measures against unauthorised modifications.

If specially developed software or hardware is used, then the relevant security instructions must be taken care of right in the development process.

In case of all modifications to the software and hardware used, documented checking mechanisms must be implemented.

[r9.9]

Networks implemented within the D-CA/D-CP and the data saved and processed there must be protected against external intervention using special protection mechanisms (like e.g. Firewalls).

[r9.10]

All security-relevant actions and processes on IT systems relevant for the work of the D-CA/D-CP must be recorded in such a manner that the respective time and person can be recalled with sufficient certainty. This includes at least:

- Creation of user areas (accounts),
- All transaction requirements (account of the applicant, type, status (successful/not successful), reasons for failure, ...),
- Software installations and updates,
- Hardware modifications,
- System shut down and restart,
- Access to audits and archives

[r9.11]

The records should be protected against modification and unauthorised access. They should be regularly and occasionally evaluated and analysed.

[r9.12]

The record data should be maintained for at least 7 years in such a manner that an evaluation within this time span is possible at any given time.

[r9.13]

The D-CA/D-CP draws up an emergency plan, in which the course of action at the time of serious emergencies like key compromising or loss of relevant data and/or IT system failure is determined.

[r9.14]

The D-CA/D-CP guarantees a sufficient structural and physical protection of its data and IT systems. This especially includes sufficient access protection for security sensitive areas.

Areas, where private and secret keys are generated, stored and processed must be protected using special measures.

9.3. Function separation

[r9.15]

The setting up of function concepts should prevent individual persons from circumventing the security precautions of the D-CA/D-CP. For this purpose, individual functions are assigned restricted rights and duties respectively. The exact organisation depends upon the concrete course of events at the D-CA/D-CP and remains reserved for the operation concept of the D-CA/D-CP.

The following functions must at least be planned within the D-CA:

- D-CA Responsible (CA-R)
- PIN-Administrator (PV)
- Information System Security Officer (ISSO)

No person can take up more than one of these functions at a time.

- CA Administrator (CAA)
- Key Manager (KM)

Every function should be taken up by at least one person and at least one representative must be appointed.

The following functions must at least be planned within the D-CP:

- D-CP Responsible (CP-R)

- System Administrator (SysAdmin)
- Information System Security Officer (ISSO)
- Key Manager (KM)

No person can take up more than one of these functions at a time.

Every function should be taken up by at least one person and at least one representative must be appointed.

The function bearers must be reliably authenticated by IT systems of the D-CA/D-CP.

[r9.16]

The CA-R/C-PR function includes:

- He is responsible for safe and smooth operations of the D-CA/D-CP as an organisation.
- He is a representative of the organisation and is authorised to give instructions within the D-CA/D-CP organisation.
- He is not directly involved in the implementation of business processes, but is responsible for adherence to and evaluation of security measures along with the total management of the D-CA/D-CP.
- He accepts the responsibility for Change Management.

[r9.17]

The KM function includes:

- safe execution of Key Management Processes,
- generation, certification, administration and deletion of asymmetric keys of the D-CA/D-CP as well as the symmetric keys, which are used for encoding data of recording equipment and/or workshop cards.

The function of the Key Manager can be implemented only on the basis of the ‘four-eyes-principle’.

[r9.18]

The CAA function includes:

- Responsible for smooth operations of technical systems of the D-CA.

[r9.19]

The PV function includes:

- the exclusive knowledge of the PIN which safeguards the access to the memberstate keys and the symetric key.
- participating in key generation.
- participating in all activities where access to the memberstate keys or the symetric key for encryption of motion-sensor data is necessary (e.c. key generation, implementing of the keys, replacement of keys).

[r9.20]

The SysAdmin function includes:

He is responsible for smooth operations of the technical network components and IT-systems of the D-CP (Installation, configuration, administration, update, backup, recovery).

[r9.21]

The ISSO function includes:

- examination of security of all business processes in detail and evaluation of security measures.

- examination of all other functions, implementation of the Security Policy, the Change Management and/or the implementation of business processes and instructions within the D-CA/D-CP organisation.
- responsibility for carrying out audits which have to be regularly undertaken within the D-CA/D-CP organisation.
- responsibility for the drawing up and maintaining of the security concept.
- Participating in Member State Key generation.

[r9.21]

If the D-CA/D-CP transfers parts of its tasks to external service providers, then they should draw up a function concept corresponding to their duties.

10. End of D-CA/D-CP operation

10.1. Responsibility of the D-MSA

The D-MSA takes decisions regarding transfer of the responsibility of D-CA/D-CP. D-MSA must appoint a new D-CA/D-CP for the same. In order to execute this transfer, the following points must be fulfilled.

[r10.1]

The D-MSA ensures that the transfer of tasks and duties to the new D-CA/D-CP takes place in a suitable manner.

[r10.2]

The old D-CA/D-CP must transfer all the available D-CA/D-CP keys to the new D-CA/D-CP. The method is determined by the D-MSA.

[r10.3]

All types of copies of keys, which can be associated with the old D-CA/D-CP or which could not be transferred, must be destroyed.

11. Operation audits

11.1. D-CA

[r11.1]

The D-MSA ensures execution of regular and occasional independent audits of the D-CA operations. An appropriate audit should take place at least once every year. The D-MSA can entrust external service providers with this task.

At the time of audit of the D-CA operation, the concurrence of the current operation with the relevant legal provisions, the D-MSA-Policy as well as the current operational concept and the current IT security concept must be especially verified.

External service providers authorised by the D-CA, if necessary, have to be included in the audit.

[r11.2]

The D-MSA ensures that the security of the D-CA operation is not impeded by the process of audit. It especially ensures that the results of these audits are not made available to any unauthorised person.

External service providers are required to maintain secrecy, if necessary.

[r11.3]

The D-MSA includes the results of the evaluation in a report, that defines corrective actions, including an implementation schedule, required to fulfil the D-MSA obligations. The report will be provided, in English, to the ERCA.

[r11.4]

If the evaluations show discrepancies or non-conformities of the functioning of the D-CA, then the D-MSA notifies the D-CA to amend the same. The D-CA reports immediately to the D-MSA about the initiation and conclusion of these measures. The D-MSA can arrange for an independent evaluation of the success of these measures.

11.2. D-CP and manufacturers of vehicle units as well as manufacturers of motion sensors

[r11.5]

Adherence to security guidelines and especially to the German D-MSA-Policy must be proved by

- a certificate issued by BSI or equivalent EU authority,
- at least one audit per year.

The manufacturer and/or the D-CP bears the costs.

[r11.6]

Occasional audits in accordance with Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002 can be demanded by the D-MSA and the D-CA at any time. If irregularities are seen, then the manufacturer and/or the D-CP bears the costs. Otherwise the initiating supervisory authority bears the costs.

12. Modifications and adjustments of the D-MSA-Policy

[r12.1]

Applications for modifications of the D-MSA-Policy have to be addressed to the D-MSA, which decides and takes suitable measures in the positive case in adequate period of time.

13. Conformity to the ERD-MSA-Policy

The requirements for the German D-MSA-Policy are formulated in the ERD-MSA-Policy § 5.3. The table below provides the rationale between the requirements as formulated in the ERD-MSA-Policy and the requirements in the German D-MSA-Policy.

Item	Reference ERD-MSA-Policy	Requirement	Reference D-D-MSA-Policy
1.	§ 5.3.1	The MSA Policy shall identify the entities in charge of operations.	§ 1.1 Responsible organisations
2.	§ 5.3.2	The MSCA key pairs for equipment key certification and for motion sensor key distribution shall be generated and stored within a device which either: • is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher [10]; • is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2 [11]; • is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 [12]; to level E3 or higher in ITSEC [13]; or equivalent security criteria. These evaluations shall be to a protection profile or security target, • is demonstrated to provide an equivalent level of security.	§ 6 Key management within the D-CA (paragraph 2)
3.	§ 5.3.3	Member State Key Pair generation shall take place in a physically secured environment by personnel in trusted roles under, at least dual control.	§ 6 Key management within the D-CA(paragraph 3) § 6.2 Key pair of the D-CA (MS.SK, MS.PK) [r6.5] § 6.2 Key pair of the D-CA (MS.SK, MS.PK) [r6.10] § 7.3 Key application [r7.9] § 9.2 Special requirements of the security concept [r9.7]
4.	§ 5.3.4	The Member State Key Pairs shall be used for a period of at most two years starting from certification by the ERCA.	§ 6.2 Key pair of the D-CA (MS.SK, MS.PK) [r6.7]
5.	§ 5.3.5	The generation of new Member State Key Pairs shall take into account the one month turnaround time required for certification by the ERCA	§ 6.2 Key pair of the D-CA (MS.SK, MS.PK) [r6.13]
6.	§ 5.3.6	The MSA shall submit MSCA public keys for certification by the ERCA using the key certification request (KCR) protocol described in Annex A.	§ 6.2 Key pair of the D-CA (MS.SK, MS.PK) [r6.14]
7.	§ 5.3.7	The MSA shall request motion sensor master keys from the ERCA using the key distribution request (KDR) protocol described in Annex D.	§ 6.3 6.3Symmetric keys for workshop cards and distance and motion sensors (Km, KmWC, KmVU) [r6.20]
8.	§ 5.3.8	The MSA shall recognise the ERCA public key in the distribution format described in Annex B.	§ 6.2 Key pair of the D-CA (MS.SK, MS.PK) [r6.15]
9.	§ 5.3.9	The MSA shall use the physical media for key	§ 6.2 Key pair of the D-CA

Item	Reference ERD-MSA-Policy	Requirement	Reference D-D-MSA-Policy
		and certificate transport described in Annex C.	(MS.SK, MS.PK) [r6.16]
10.	§ 5.3.10	The MSA shall ensure that the Key Identifier (KID) and modulus (*n*) of keys submitted to the ERCA for certification are unique within the domain of the MSCA.	§ 8.4 Certificate contents and formats [r8.9]
11.	§ 5.3.11	The MSA shall ensure that expired keys are not used for any purpose. The Member State private key shall be either: destroyed so that the private key cannot be recovered or retained in a manner preventing its use.	§ 6.2 Key pair of the D-CA (MS.SK, MS.PK) [r6.7]
12.	§ 5.3.12	The MSA shall ensure that an equipment RSA key is generated, transported, and inserted into the equipment, in such a way as to preserve its confidentiality and integrity. For this purpose, the MSA shall • ensure that any relevant prescription mandated by security certification of the equipment is met. • ensure that both generation and insertion (if not onboard) takes place in a physically secured environment; • unless key generation was covered by the security certification of the equipment, ensure that specified and appropriate cryptographic key generation algorithms are used; The last two of these requirements on generation shall be met by generating equipment keys within a device which either: a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher [9]; b) is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2 [10]; c) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 [11]; to level E3 or higher in ITSEC [12]; or equivalent security criteria. These evaluations shall be to a protection profile or security target. d) is demonstrated to provide an equivalent level of security.	§ 7.1 General requirements, record [r7.1] § 7.2 Key generation [r7.5]
13.	§ 5.3.13	The MSA shall ensure confidentiality, integrity, and availability of the private keys generated, stored and used under control of the MSA Policy.	§ 5 Card and equipment management [r5.6] § 6 Key management within the D-CA (paragraph 2) § 7.1 General requirements, record [r7.2]
14.	§ 5.3.14	The MSA shall prevent unauthorised use of the private keys generated, stored and used under control of the MSA Policy.	§ 6 Key management within the D-CA (paragraph 2) § 6.2 Key pair of the D-CA (MS.SK, MS.PK) [r6.9] § 7.2 Key generation [r7.8]
15.	§ 5.3.15	The Member State private keys may be backed up using a key recovery procedure requiring at least dual control.	§ 7.3 Key application [r7.11]

Item	Reference ERD-MSA-Policy	Requirement	Reference D-D-MSA-Policy
16.	§ 5.3.16	Key certification requests that rely on transportation of private keys are not allowed.	§ 8.2 Certificate issuing [r8.7]
17.	§ 5.3.17	Key escrow is strictly forbidden	§ 6.2 Key pair of the D-CA (MS.SK, MS.PK) [r6.11]
18.	§ 5.3.18	The MSA shall prevent unauthorised use of its motion sensor keys.	§ 6.3 Symmetric keys for workshop cards and distance and motion sensors (Km, KmWC, KmVU) [r6.18]
19.	§ 5.3.19	The MSA shall ensure that the motion sensor master key (Km) is used only to encrypt motion sensor data for the purposes of motion sensor manufacturers. The data to be encrypted is defined in the ISO / IEC 16844-3 standard [7].	§ 6 Key management within the D-CA (paragraph 2)
20.	§ 5.3.20	The motion sensor master key (Km) shall never leave the secure and controlled environment of the MSA.	§ 6.3 Symmetric keys for workshop cards and distance and motion sensors (Km, KmWC, KmVU) [r6.18]
21.	§ 5.3.21	The MSA shall forward the workshop card motion sensor key (Km_{WC}) to the component personaliser (in this case, the card personalisation service), by appropriately secured means, for the sole purpose of insertion into workshop cards.	§ 6.3 Symmetric keys for workshop cards and distance and motion sensors (Km, KmWC, KmVU) [r6.18]
22.	§ 5.3.22	The MSA shall forward the vehicle unit motion sensor key (Km_{VU}) to the component personaliser (in this case, a vehicle unit manufacturer), by appropriately secured means, for the sole purpose of insertion into vehicle units.	§ 6.3 Symmetric keys for workshop cards and distance and motion sensors (Km, KmWC, KmVU) [r6.18]
23.	§ 5.3.23	The MSA shall maintain the confidentiality, integrity, and availability of its motion sensor key copies.	§ 6 Key management within the D-CA (paragraph 2)
24.	§ 5.3.24	The MSA shall ensure that its motion sensor key copies are stored within a device which either: a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher [9]; b) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408 [11]; to level E3 or higher in ITSEC [12]; or equivalent security criteria. These evaluations shall be to a protection profile or security target.	§ 6 Key management within the D-CA (paragraph 2)
25.	§ 5.3.25	The MSA shall possess different Member State Key Pairs for the production of vehicle unit and tachograph card equipment public key certificates.	§ 6.2 Key pair of the D-CA (MS.SK, MS.PK) [r6.3] § 7.3 Key application [r7.9]
26.	§ 5.3.26	The MSA shall ensure availability of its equipment public key certification service.	§ 6.2 Key pair of the D-CA (MS.SK, MS.PK) [r6.6]
27.	§ 5.3.27	The MSA shall only use the Member State Private Keys for: a) the production of Annex I(B) equipment key certificates using the ISO / IEC 9796-2 digital signature algorithm as described in Annex I(B) Appendix 11 *Common Security Mechanisms* [6]; b) production of the ERCA key certification request as described in Annex A.. c) issuing Certificate Revocation Lists if this	§ 6.2 Key pair of the D-CA (MS.SK, MS.PK) [r6.4]

Item	Reference ERD-MSA-Policy	Requirement	Reference D-D-MSA-Policy
		method is used for providing certificate status information (see 5.3.30).	
28.	§ 5.3.28	The MSA shall sign equipment certificates within the same device used to store the Member State Private Keys (see 5.3.2).	§ 6 Key management within the D-CA (paragraph 2)
29.	§ 5.3.29	Within its domain, the MSA shall ensure that equipment public keys are identified by a unique key identifier which follows the prescriptions of Annex 1(B) [6].	§ 8.4 Certificate contents and formats [r8.9]
30.	§ 5.3.30	Unless key generation and certification is performed in the same physically secured Environment, the key certification request protocol shall provide proof of origin and integrity of certification requests, without revealing the private key.	§ 8 Registration [r8.3]
31.	§ 5.3.31	The MSA shall maintain and make certificate status information available.	§ 8.5 Information duties of the D-CA [r8.13]
32.	§ 5.3.32	The validity of a tachograph card certificate shall equal the validity of the tachograph card.	§ 8.3 Validity of certificate [r8.8]
33.	§ 5.3.33	The MSA shall prevent the insertion of undefined validity certificates into tachograph cards.	§ 8.3 Validity of certificate [r8.8]
34.	§ 5.3.34	The MSA may allow the insertion of undefined validity Member State certificates into vehicle units.	§ 8.3 Validity of certificate [r8.8]
35.	§ 5.3.35	The MSA shall ensure that users of cards are identified at some stage of the card issuing process.	§ 5 Card and equipment management [r5.8] § 7.3 Key application [r7.10]
36.	§ 5.3.36	The MSA shall ensure that ERCA is notified without delay of loss, theft, or potential compromise of any MSA keys.	§ 6.2 Key pair of the D-CA (MS.SK, MS.PK) [r6.12]
37.	§ 5.3.37	The MSA shall implement appropriate disaster recovery mechanisms which do not depend on the ERCA response time.	§ 6.2 Key pair of the D-CA (MS.SK, MS.PK) [r6.6] § 9 Information security [r9.13]
38.	§ 5.3.38	The MSA shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved.	§ 9.1 Information Security Management System (ISMS) [r9.1]
39.	§ 5.3.39	The MSA shall ensure that the policies address personnel training, clearance and roles.	§ 9.2 Special requirements of the security concept [r9.5] § 9.3 Function separation [r9.15]
40.	§ 5.3.40	The MSA shall ensure that appropriate records of certification operations are maintained.	§ 8.4 Certificate contents and formats [r8.9] § 9 Information security [r9.10] [r9.11] [r9.12]
41.	§ 5.3.41	The MSA shall include provisions for MSCA termination in the MSA Policy.	§ 10.1 Responsibility
42.	§ 5.3.42	The MSA Policy shall include change procedures.	§ 12 Modifications and adjustments of the D-MSA-Policy [r12.1]
43.	§ 5.3.43	The MSA audit shall establish whether the Requirements of this Section are being maintained.	§ 11.1 D-CA [r11.1] 2. Paragraph
44.	§ 5.3.44	The MSA shall audit the operations covered by the approved policy at intervals of not more	§ 11.1 D-CA [r11.1] 1. Paragraph

Item	Reference ERD-MSA-Policy	Requirement	Reference D-D-MSA-Policy
		than 12 months.	
45.	§ 5.3.45	The MSA shall report the results of the audit as mentioned in 5.3.43 and provide the audit report, in English, to the ERCA.	§ 11.1 D-CA [r11.3]
46.	§ 5.3.46	The audit report shall define any corrective actions, including an implementation schedule, required to fulfil the MSA obligations.	§ 11.1 D-CA [r11.3]

Appendix A Abbreviations, Definitions

BMVBS	Bundesministerium für Verkehr, Bau- und Stadtentwicklung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAA	CA Administrator ↑ see The CAA function includes: , page 26
CA-R	D-CA Responsible ↑ see The CA-R/C-PR function includes: , page 26
CP-R	D-CP Responsible ↑ see The CA-R/C-PR function includes: , page 26
D-MSA-Policy	Certification Policy for the Federal Republic of Germany for the electronic tachograph as per supplement 11 of appendix I (B) of Regulation 2135/98
Card personaliser	See D-CP
Certificate	In the asymmetric cryptography, a certificate confirms the link between a ↑ public key and an identity (person, organisation, machine,...) described in the certificate who owns the accompanying ↑ private key. In the context of the ↑ D-MSA-Policy, the certificates defined in supplement 11 of appendix I (B) of ↑Regulation (EC) 2135/98 are understood under this.
Certification authority	An authority, which issues a ↑ certificate. In the context of Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002, the European certification authority (↑ Root CA) and the certification authorities of the member states (for Germany ↑ D-CA) exist, which receive the certificates necessary for their work from the ↑ Root CA.
Change Management	Handling technical, organisational and/or subjective process modifications
D-CA	The ↑ certification authority of the Federal Republic of Germany for the electronic tachograph as per ↑ Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002, Federal Motor Transport Authority (KBA). According to international usage (CA = certification authority) ↑ see The **D-CA:** , page 10
D-CIA	Card issuing authority for tachographcards, ↑ see The **D-CIA:** , page 10
D-CP	Card personaliser. An authority, which brings asymmetric key pairs and the corresponding certificates according to ↑ Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002 on the driver, workshop, inspection and company cards defined in ↑ Regulation (EC) 2135/98. ↑ see The **D-CP:**

	, page 11
D-MSA	Authority responsible for the implementation of the ↑ EU directive in the Federal Republic of Germany, BMVBS. According to international usage (MSA = member state authority) ↑ see [r3.1] , page 10
Digital signature	Procedure for ensuring the non-imitation (integrity) and proof of origin (authenticity) of an electronic document using asymmetric cryptography.
ERCA	European Route Certification Authority
FE	Vehicle units according to definitions of ↑ Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002
ISMS	Information Security Management System
ISSO	Security Officer According to international usage (ISSO = Information System Security Officer) ↑ see The ISSO function includes, page 26
KDR	Key Distribution Request (for motion sensor master key)
KM	Key Manager ↑ see The KM function includes: , page 26
Personalising	Also: **logical P.** Integration of private/secret keys and the accompanying certificates in recording equipment cards and recording equipment. This has to be differentiated from **optical P.** of a card, by which names, photos etc. are brought on to the body of the card.
Private key	Private (secret) part in the asymmetric cryptography of a key pair. This serves the purpose of generation of a ↑digital signature or of decoding a message. (s. also ↑ Public key)
PS	The Practice Statement of the D-CA the D-CP, manufacturers of vehicle units and manufacturers of motion sensors as defined in chapter 4 of the D-MSA-Policy. The designation "*Certification Practice Statement (CPS)"* is common in international context.
Public key	Public part in the asymmetric cryptography of a key pair. This serves the purpose of verification of a ↑ digital signature or of encoding a message. (see also ↑ Private Key)
Root CA	The European ↑ certification authority for the electronic tachograph according to ↑ Regulation (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002.
Root Policy	"Digital Tachograph System – European Root Policy", drawn up by JRC (Joint Research Center) in Ispra
RSA	Special process of asymmetric cryptography. According to supplement 11 of appendix I (B) of Regulation (EC) 2135/98 the RSA process is implemented in the electronic tachograph for the

	generation of ↑ digital signatures.
SysAdmin	System Administrator of the D-CP ↑ see SysA function, page 26

Appendix B Reference documents

[CC] Common Criteria. ISO/IEC 15408 (1999)
[CEN] CEN Workshop Agreement 14167-2: Cryptographic Module for CSP...
[FIPS] FIPS PUB 140-2. NIST
[GSHB] BSI-IT-Grundschutzhandbuch
[ISO] ISO 17799