



Christoph Baier, 28. März 2006

The Swiss MSA-Policy

for the Digital Tachograph according EU Council Regulation 2135/98

F132-0431

Version

1.00

Date

6th July 2006

Status

under construction

in approval

approved for use

Colophon

Published by	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK Federal Department of the Environment, Transport, Energy and Communications DETEC Bundesamt für Strassen ASTRA Federal Roads Office Abteilung Strassenverkehr Road Traffic Division
Postal address	CH-3003 Bern
Location	Mühlestrasse 2, CH-3063 Ittigen
Phone	+41 (0)31 322 94 11
Fax	+41 (0)31 323 23 03
Office Website	www.astra.admin.ch
Policy published on Website	www.dfs.astra.admin.ch
Version	1.0 (Final)
Date	6 July 2006

Document Revision History

Date	Version	Who	Description
26.04.05	0.14	Peter Stähli	Draft
23.05.05	0.142	Christoph Baier	Enhancements
11.09.05	0.2	Peter Stähli	Reworked Obligations und Responsibilities, consolidation of feedback from ASTRA and BIT
25.10.05	0.31	Peter Stähli	Precisions after meeting with ASTRA
24.02.06	0.41	David Müller / Peter Stähli	Finalization / ready for internal review
10.03.06	0.42	Peter Stähli	Feedback R. Dietschi, BIT
22.03.06	0.50	Peter Stähli	Feedback Ch. Baier, ASTRA
24.03.06	0.90	Peter Stähli	Review R. Dietschi, ready for ASTRA review
28.03.06	0.91	Ch. Baier	Review, different enhancements and changes
23.05.06	0.92	Ch. Baier	Review Ch. Baier with R. Dietschi, BIT
30.05.06	0.93	Ch. Baier	Corrections
02.05.06	0.94	F. Schmid, Ch. Baier	Review, slight corrections Version to be sent to ERCA in JRC, Ispra
07.06.06	0.95	Trüb	Changes
09.06.06		Ch. Baier	Enhancements RMG, Version sent for ERCA approval
26.06.06	0.96	Ch. Baier	Changes after 1 st review of ERCA on 14.6.06 G07-TRVA/JB/jb/(2006)D (registered as A8808), letter D14673, and feedback from R. Keller of Softlab, P. Balsiger and R. Dietschi of BIT
30.06.06	0.97	Ch. Baier	Changes after feedback from R. Dietschi of BIT, R. Keller of Softlab, R. Zimmermann of Trüb AG
05.07.06	0.98	Ch. Baier	Changes after 2 nd review of ERCA on 5.7.06 G07-TRVA/JB/jb/(2006)D16565 (registered as A10188)
05.07.06	0.99	Ch. Baier	Typographical correction
06.07.06	1.00	Ch. Baier	Set to productive version 1.00 after 3 rd review of the Swiss MSA Policy, Version 0.99, 5 th July 2006 (registered as A10242) and the ERCA confirmation letter for the start of services to Switzerland on 6.7.06 G07-TRVA/JB/jb/(2006)D16730

Contents

The Swiss MSA-Policy	1
for the Digital Tachograph according EU Council Regulation 2135/98	1
Colophon.....	2
Document Revision History	3
Document Revision History	3
Contents.....	4
Figures.....	6
Tables	6
1 Introduction	7
1.1 Project background	7
1.1.1 The Digital Tachograph	7
1.1.2 Regulations.....	7
1.2 Key and certificate management in the Digital Tachograph System	8
1.3 Participating entities	9
1.3.1 Organisational Overview	9
1.3.2 Entities Roles and Responsibilities.....	9
1.3.3 Risk Management.....	11
1.3.4 The context of the Digital Tachograph System	12
1.4 Responsible organization: The Member State Authority (MSA)	13
1.5 The MSA Policy.....	13
1.6 The MSA Policy Approval.....	13
1.7 The MSA Availability and Contact Details.....	13
1.8 References	13
2 Obligations and responsibilities	14
2.1 General conditions	14
2.2 Appointments by legislation.....	14
2.3 Member State Authority (MSA) / Card Issuing Authority (CIA)	14
2.3.1 MSA/CIA responsibilities	14
2.3.2 MSA/CIA obligations.....	14
2.3.3 MSA appointed entities.....	15
2.4 Application Provider (AP)	15
2.4.1 AP responsibilities	15
2.4.2 AP obligations.....	15
2.5 Card Application Authorities (CAA)	15
2.5.1 CAA responsibilities.....	15
2.5.2 CAA obligations	15
2.6 Control Bodies / Enforcers (CB).....	16
2.6.1 Control Bodies / Enforcers responsibilities.....	16
2.6.2 Control Bodies / Enforcers obligations	16
2.7 Card Distributor (CD).....	16
2.7.1 CD responsibilities.....	16
2.8 Card Manufacturer and Card Personaliser (CM/CP)	16
2.8.1 CM/CP responsibilities.....	16
2.8.2 CM/CP obligations.....	16
2.9 Certification Authority (DFS-CA)	17
2.9.1 DFS-CA responsibilities.....	17
2.9.2 DFS-CA obligations	17
2.10 European Commission (EU COM).....	18
2.11 European Root Certification Authority (ERCA)	18
2.11.1 ERCA responsibilities	18
2.11.2 ERCA obligations.....	18
2.12 Functional Test Authority (FTA)	18
2.12.1 Functional Test Authority responsibilities	18
2.12.2 Functional Test Authority obligations.....	19
2.13 Type Approval Authority (TAA)	19

2.13.1	Type Approval Authority responsibilities.....	19
2.13.2	Type Approval Authority obligations.....	19
2.14	Security Test Authority (STA)	19
2.14.1	Security Test Authority responsibilities.....	19
2.14.2	Security Test Authority obligations	19
2.15	Interoperability Test Authority (IOTA)	19
2.15.1	Interoperability Test Authority responsibilities	19
2.15.2	Interoperability Test Authority obligations	19
2.16	United Nation Economic Commission for Europe (UN ECE)	19
2.17	Users.....	19
2.17.1	User responsibilities.....	20
2.17.2	User obligations.....	20
3	Additional provisions.....	21
3.1	Liability.....	21
3.2	Financial responsibility	21
3.3	Conformity and approval	21
3.3.1	Certification.....	21
3.3.2	Confidentiality	21
3.3.3	Types of information to be kept confidential.....	22
3.3.4	Types of information considered not to be confidential.....	22
4	Operational requirements	23
4.1	The DFS-CA Certification Practice Statement	23
4.2	DFS-CA Key management.....	23
4.2.1	DFS-CA key generation.....	23
4.2.2	DFS-CA key storage, backup and recovery	23
4.2.3	DFS-CA public key certification by ERCA	24
4.2.4	DFS-CA key usage	24
4.2.5	End of DFS-CA key life cycle	24
4.2.6	Life cycle management of cryptographic hardware devices	25
4.3	Equipment Key Management.....	25
4.3.1	Equipment key generation.....	25
4.3.2	Equipment key storage, backup and recovery	26
4.3.3	Life cycle management of cryptographic hardware devices	26
4.4	Equipment Certificate Management.....	26
4.4.1	Input data.....	26
4.4.2	Certificate Issuing	26
4.4.3	Validity of Certificate.....	27
4.4.4	Certificate contents and formats.....	27
4.4.5	Information duties of the DFS-CA.....	27
4.5	Motion Sensor keys.....	27
4.6	Identification and authentication.....	28
4.6.1	Initial registration.....	28
4.6.2	Certificate generation.....	29
4.6.3	Certificate dissemination	29
4.6.4	Certificate renewal.....	29
4.6.5	Certificate revocation and suspension.....	29
4.6.6	Dissemination of terms and conditions.....	29
4.7	Personnel security.....	29
4.8	Operational requirements.....	30
4.9	Audit	30
4.10	The MSA Policy change procedures	31
4.10.1	Items that may change without notification	31
4.10.2	Changes with notification.....	31
4.10.3	Comment period	31
4.10.4	Whom to inform	31
4.10.5	Period for final change notice	31
4.10.6	Changes requiring a new MSA Policy approval	31
4.11	DFS-CA or CP Termination	32
4.11.1	Final termination - MSA responsibility	32

4.11.2	Transfer of DFS-CA or CP responsibility.....	33
5	Conformity to the ERCA Policy.....	34
6	References.....	38
7	Web Links.....	39
8	Glossary/Definitions and Abbreviations.....	40
8.1	Glossary/Definitions.....	40
8.2	List of abbreviations.....	41
9	Letter of Conformity to ERCA Policy.....	43

Figures

Figure 1:	Tachograph system keys, certificates and equipment management.....	8
Figure 2:	Organizational overview.....	9
Figure 3:	Risk Management.....	11
Figure 4:	Overview of the Digital Tachograph systems and entities.....	12

Tables

Table 1:	Roles and responsibilities.....	10
Table 2:	References.....	38
Table 3:	Glossary.....	40
Table 4:	List of abbreviations.....	42

1 Introduction

This document is the Swiss Certification Authority Policy for the digital Tachograph system, hereinafter referred as the **MSA Policy**. This policy is in accordance with the following EU documents:

- a) The Council Regulation of the Tachograph system, 2135/98/EEC
- b) The Commission Regulation 1360/2002/EC [Annex 1 B]
- c) The "Common Security Guidelines" [CSG]

1.1 Project background

1.1.1 The Digital Tachograph

The Digital Tachograph is a control device for recording driver activities, such as driving and rest periods in, e.g. heavy goods vehicles. Four main topics are addressed by the introduction of the Digital Tachograph. The Digital Tachograph

- a) gives transport companies more possibilities to use the equipment as management tool,
- b) provides the drivers with clear and accurate information about their driving and rest periods,
- c) allows effective and efficient enforcement of drivers activities,
- d) reduces the possibilities to fraud.

1.1.2 Regulations

The use of the Digital Tachograph is required by law at the European Union as a result of the following legislation:

- a) The regulation 2135/98/EC of September 1998, amending Regulation 3821/85/EEC on recording equipment in road transport and Directive 88/599/EEC concerning the application of Regulations 3820/85/EEC and 3821/85/EEC.
http://europa.eu.int/eur-lex/en/consleg/pdf/1998/en_1998R2135_do_001.pdf

These regulations have been adopted in the:

- b) SR 0.740.72 Abkommen zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über den Güter- und Personenverkehr auf Schiene und Strasse, Abgeschlossen am 21. Juni 1999, von der Bundesversammlung genehmigt am 8. Oktober 1999, Schweizerische Ratifikationsurkunde hinterlegt am 16. Oktober 2000, in Kraft getreten am 1. Juni 2002).
http://www.admin.ch/ch/d/sr/c0_740_72.html

(Agreement between the European Community and the Swiss Confederation on the Carriage of Goods and Passengers by Rail and Road
Official Journal L 114 , 30/04/2002 P. 0091 – 0131)

and

- c) SR 0.822.725.22 Europäisches Übereinkommen vom 1. Juli 1970 über die Arbeit des im internationalen Strassenverkehr beschäftigten Fahrpersonals (AETR) (mit Anhang und Anlagen).
http://www.admin.ch/ch/d/sr/c0_822_725_22.html

(European Agreement concerning the Work of Crews of Vehicles Engaged in International Road Transport (AETR), done at Geneva on 1 July 1970 and its amendments
<http://www.unece.org/trans/main/sc1/aetr.html>)

Switzerland approved the above agreements as Contracting Party. Nevertheless and in order to be compatible with the original template of this Policy, the terms 'MS' meaning 'Member State' and 'MSA' meaning 'Member State Authority' are used for Switzerland as well but in the meaning of '**Contracting Party**'.

1.2 Key and certificate management in the Digital Tachograph System

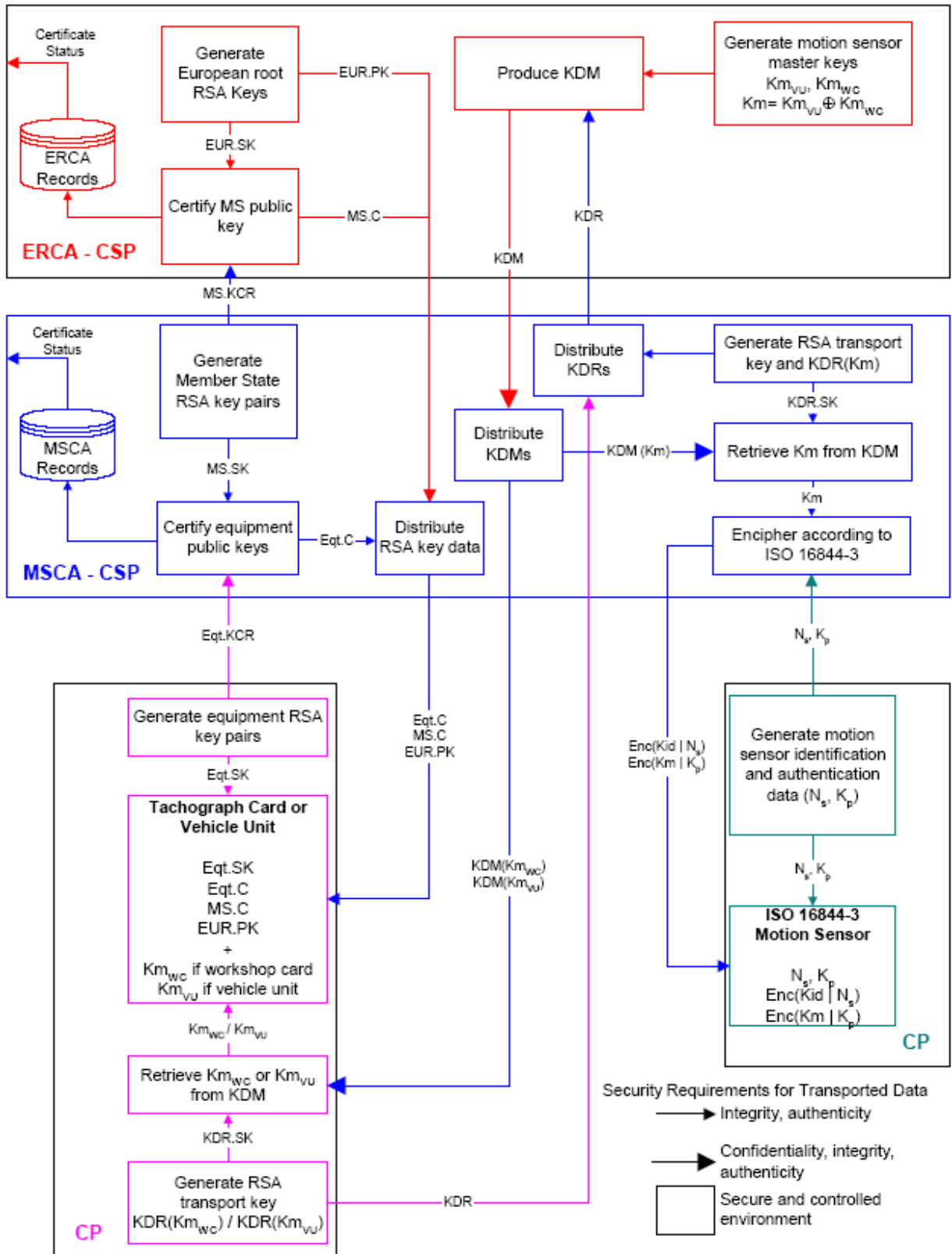


Figure 1: Tachograph system keys, certificates and equipment management

The functionality for the delivery of Digital Tachograph certificates for Vehicle Units (VU) is not implemented, as there are no manufactures of such equipments in Switzerland.

1.3 Participating entities

The Digital Tachograph system consists of several functionalities and services which are provided by different entities, each one of them in a specific role and with separate obligations and responsibilities.

1.3.1 Organisational Overview

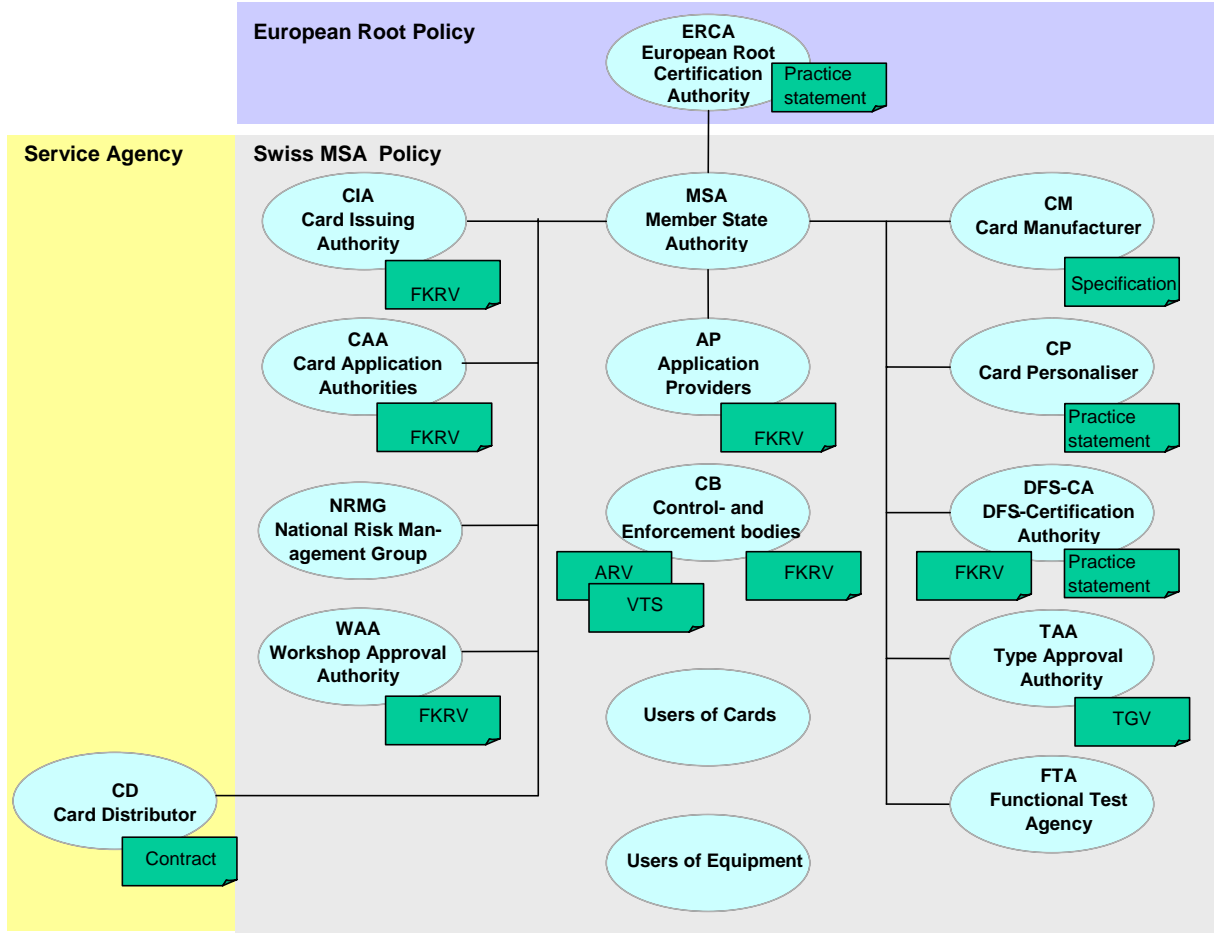


Figure 2: Organizational overview

The European Root Policy rules the Digital Tachograph System throughout the contracting parties.

The MSA Policy, based on the European Root Policy, rules the implementation and management of the Digital Tachograph System in Switzerland. The need for a secure system is laid down in the Swiss regulation [FKRV] (article 3, paragraph 1, letter c).

1.3.2 Entities Roles and Responsibilities

The Digital Tachograph system involves the following entities:

Role	Responsible organization
AP Application Providers	DFS-Application: Federal Office of Information Technology, Systems and Telecommunication FOITT Other AP
CAA Card Application Authorities	Driver card: Cantonal Road Authorities (StVA) Workshop card: Federal Customs Administration FCA Control- and company card: Enforcement bodies for working an resting time and/or the Cantonal Road Authorities
CB	Customs and enforcement bodies for working an resting time

Role	Responsible organization
Control Bodies / Enforcers	
CD Card Distributor	Swiss Post
CIA Card Issuing Authority	Federal Roads Authority FEDRO
CM Card Manufacturer	Trüb AG, Aarau
CP Card Personaliser	Trüb AG, Aarau
DFS-CA DFS Certification Authority	Federal Office of Information Technology, Systems and Telecommunication FOITT
ERCA European Root Certification Authority	Joint Research Center (JRC), Ispra
FTA Functional Test Agency	Landesbetrieb Mess- und Eichwesen NRW (LBME), Munich, Germany and Federal Office of Metrology and Accreditation METAS
KBA German Type Approval Authority	Kraftfahrt-Bundesamt, Federal Bureau of Motor Vehicles and Drivers, Germany
MSA Member State Authority	Federal Roads Authority FEDRO
NRMG National Risk Management Group	Federal Roads Authority FEDRO
TAA Type Approval Authority	Federal Roads Authority FEDRO
Test Labor	Forschungsgesellschaft Druck e.V. (FOGRA), Munich, Germany
User of Card Cardholders of Tachograph cards	Individual person
User of Equipment Mechanics in authorized workshops	Workshops and their employees
WAA Workshop Approval Authority	Swiss Federal Customs Authority FCA

Table 1: Roles and responsibilities

1.3.3 Risk Management

The complex system of the digital tachograph needs to be maintained and to be adapted whenever the objectives of the legislator are at stake.

The risks associated with a potential for harm have to be identified, assessed and managed appropriately.

In that regards, a risk management procedure is implemented at both national and international levels so as to allow the various stakeholders to anticipate risks and to define counter-measures when applicable.

At Swiss level, a national risk management group (NRMG) for the Digital Tachograph System is in charge with these issues.

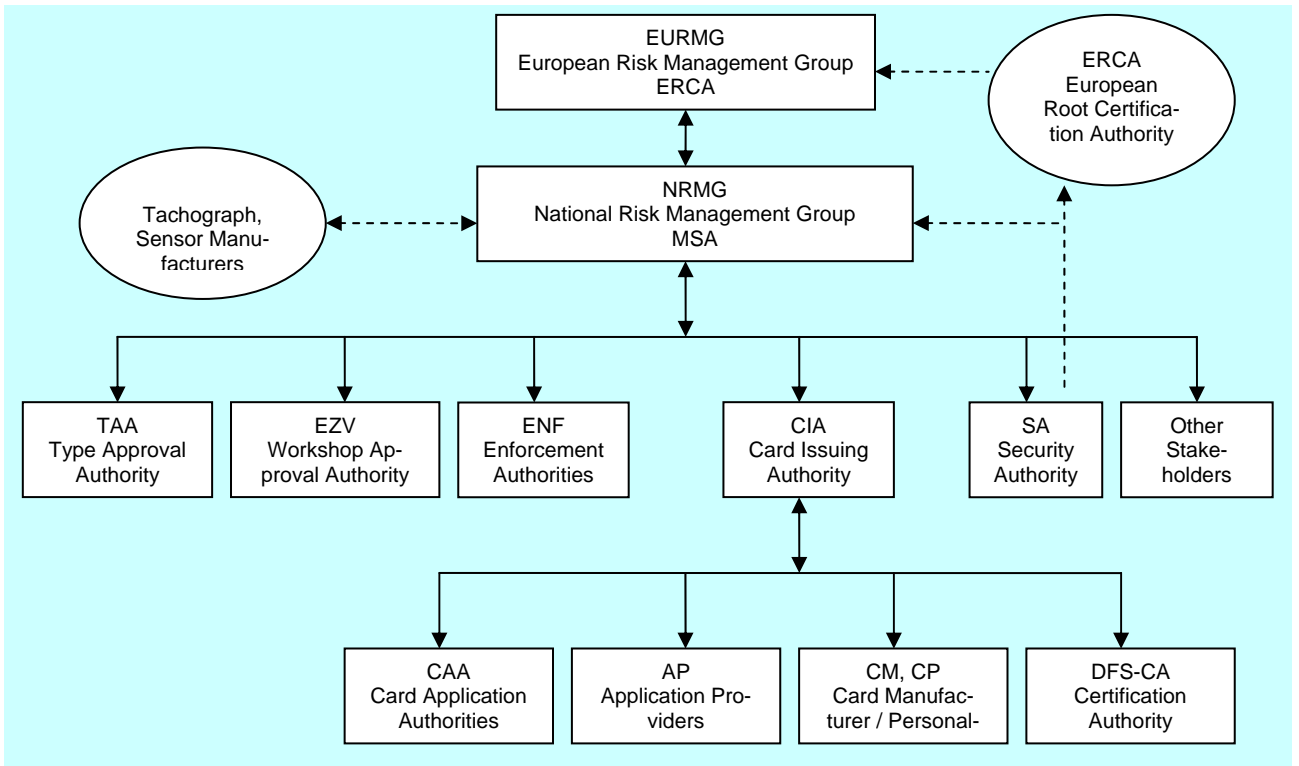


Figure 3: Risk Management

1.3.4 The context of the Digital Tachograph System

The Digital Tachograph uses a hierarchic Public Key Infrastructure (PKI) system, where a Root Certification Authority is established at the European level (ERCA) and is connected to the different participating Member States Certification Authorities, to make a consistent and secure system.

The role of the ERCA is to certify the Member States root keys to establish a trusted certification chain.

The role of the MSA is to manage and to keep track of the overall digital tachograph system in its territory and to identify, assess and manage appropriately the risks associated with a potential for harm in close collaboration with the responsible EU entity.

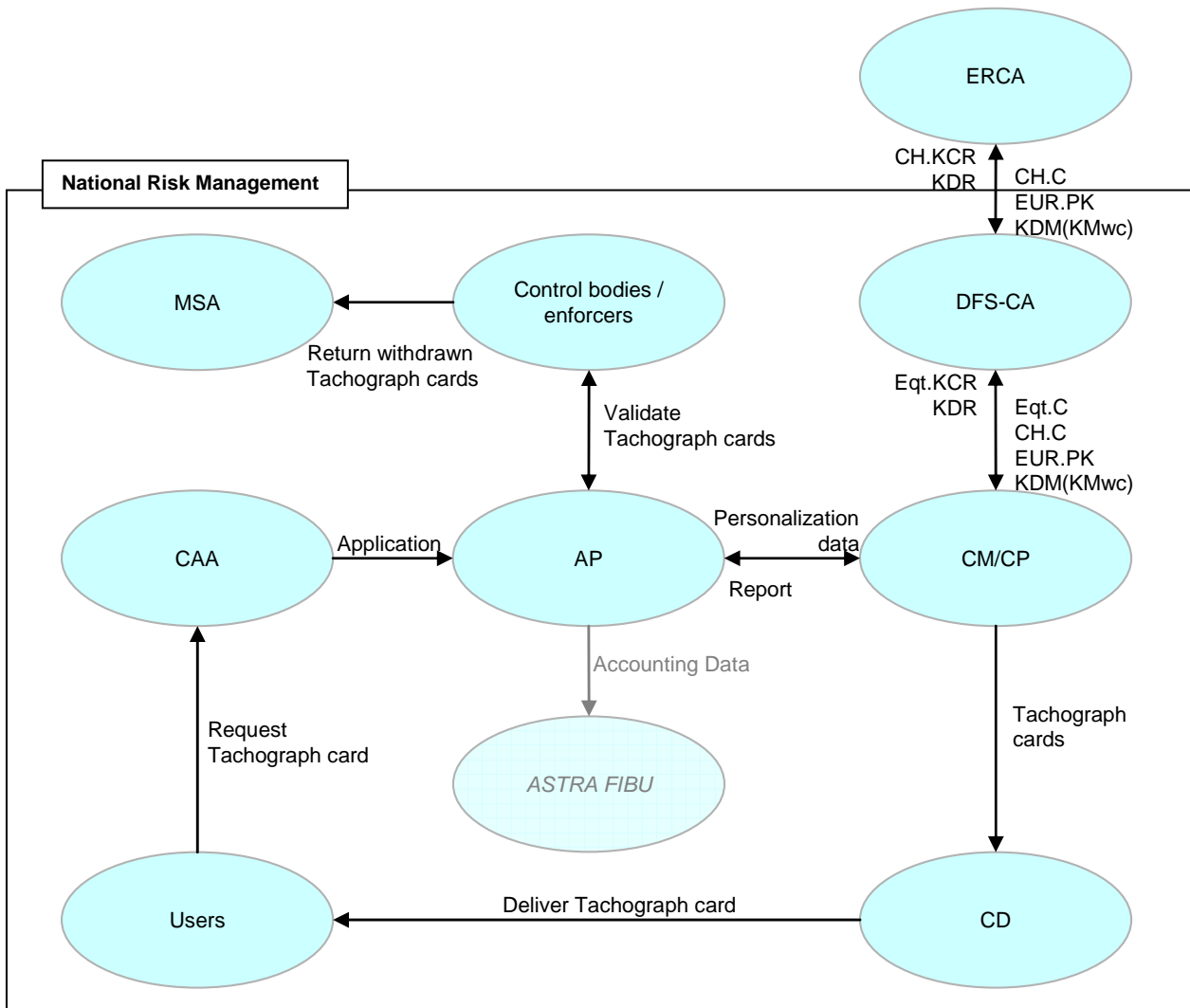


Figure 4: Overview of the Digital Tachograph systems and entities

The equipment (or equipment parts) of the Digital Tachograph system is defined as:

- a) Tachograph card (TC):
 - 1) Driver card
 - 2) Company card
 - 3) Workshop card
 - 4) Control card
- b) Vehicle Unit (VU)
- c) Motion sensor

All Tachograph Cards and Vehicle Units contain digital certificates.

The TC's are based on the type approved German TC's. They are submitted to the German Type Approval Authority KBA for approval.

The Swiss Type Approval Authority FEDRO accepts EU type approved TC's without further testing ([TGV], art. 4, paragraph 5).

1.4 Responsible organization: The Member State Authority (MSA)

Each Member State / Contracting Party has to designate a responsible organisation, the Member State Authority (MSA) for the implementation and exploitation of the Digital Tachograph system.

The Swiss MSA is:

Federal Department of the Environment, Transport, Energy and Communications DETEC

Federal Roads Office

Road Traffic Division

CH-3003 Berne, location: Mühlestrasse 2, CH-3063 Ittigen

1.5 The MSA Policy

This document is the Member State Authority Policy (MSA Policy) for Switzerland for the Digital Tachograph system.

The main processes supported by MSA Policy are:

- a) Generation of national DFS-CA and equipment keys
- b) Generation of national equipment certificates
- c) Dissemination of equipment certificates
- d) Management and dissemination of Motion Sensor keys
- e) Management of the national DFS-CA and the ERCA root keys and certificates
- f) Management of the risks of the overall national DFS-System

1.6 The MSA Policy Approval

This MSA Policy is approved by:

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

at 6th July 2006, ref G07-TRVA/JB/jb/(2006)D16730.

1.7 The MSA Availability and Contact Details

The MSA Policy is publicly available at <http://www.dfs.astra.admin.ch>.

Questions concerning the MSA Policy should be addressed to the MSA, see §1.4.

1.8 References

The MSA Policy document is primarily based upon the following reference documents:

- a) Digital Tachograph system, European Root Policy [ROOTP]
- b) Guideline and Template National CA Policy [TEMP]

2 Obligations and responsibilities

This section contains provisions relating to the respective obligations and responsibilities of the different entities as described in 1.3, according their role within the Digital Tachograph system and other issues pertaining to law and dispute resolution.

2.1 General conditions

- [r1] The MSA Policy is applicable for the Digital Tachograph system only.
- [r2] The keys and certificates issued by the DFS-CA are only for use within the Tachograph system.

2.2 Appointments by legislation

- [r3] The Swiss Regulation for the Register of the Tachograph Cards [FKRV], Article 3, appoints the involved entities within the Swiss Tachograph system.
- [r4] In the [FKRV], the FEDRO is the appointed Swiss MSA.

2.3 Member State Authority (MSA) / Card Issuing Authority (CIA)

2.3.1 MSA/CIA responsibilities

- [r5] The MSA/CIA is responsible for setting up the Tachograph organization in its domain, that is:
 - a) The MSA is responsible for the register and issuing of the digital tachograph cards.
 - b) The MSA is responsible for appointing a CM and a CP.
 - c) The MSA is responsible for appointing a CD.
 - d) The MSA is responsible for appointing a NRMG national risk management committee.

2.3.2 MSA/CIA obligations

- [r6] The MSA/CIA shall:
 - a) Maintain the MSA Policy in accordance with the European Root Policy.
 - b) Set up and manage the register of the digital tachograph cards.
 - c) Issue the tachograph cards.
 - d) Ensure that the appointed DFS-CA correctly implements the MSA Policy requirements.
 - e) Approve the DFS-CA Security Policy (DFS-CA SP).
 - f) Approve the DFS-CA Certificate Practice Statement (DFS-CA CPS).
 - g) Provide the DFS-CA with the Certificate Holder Authorization for TC Equipment keys (Eqt.CHA).
 - h) Provide the DFS-CA with the Certificate Holder Reference for TC Equipment keys (Eqt.CHR).
 - i) Provide the DFS-CA with the Start of Validity and End of Validity for TC Equipment keys (Eqt.SOV and Eqt.EOV).
 - j) Ensure that only correct and relevant certificate holder information is provided as input to the DFS-CA.
 - k) Appoint the CM and the CP (CM/CP).
 - l) Approve the DFS-CM/CP Security Policies (CM/CP SP).
 - m) Ensure that the appointed CM/CP personalizes only type approved TC's in accordance to the Regulation [Annex 1 B] and this MSA Policy.
 - n) Ensure that only correct and relevant personalization data is provided as input to the CM/CP.
 - o) Appoint the CD.

- p) Audit the appointed entities CIA, CAA, AP, CM, CP, DFS-CA.
- q) Provide accurate status information over the life cycle and events of the TC's.
- r) Oblige the card- & certificate holders to fulfill their obligations.
- s) Ensure adequate organizational and financial resources to be able to operate in conformity with the requirements laid down in this policy.

[r7] The MSA shall operate in conformance with the procedures as detailed in this policy.

2.3.3 MSA appointed entities

[r8] The appointed Member State Certification Authority (DFS-CA) is the Swiss Federal Office of Information Technology Systems and Telecommunication FOITT, Monbijoustr. 74, CH-3003 Berne.

[r9] The appointed Card Manufacturer (CM) and Card Personaliser (CP) is Trüb AG, Hintere Bahnhofstrasse 12, CH-5001 Aarau.

[r10] The appointed Card Distributor (CD) is Swiss Post.

[r11] The DFS-CA or CM/CP may subcontract parts of its processes to subcontractors, application providers and application providers.

[r12] The MSA may subcontract parts of its processes to subcontractors, application providers and service providers.

[r13] The subcontracting in no way diminishes the MSA's, DFS-CA's or CM/CP's overall responsibilities.

2.4 Application Provider (AP)

2.4.1 AP responsibilities

The AP is responsible for:

- a) the technical implementation
- b) the security
- c) the data exchange with the EU TACHOnet

of the digital tachograph system.

2.4.2 AP obligations

[r14] The AP shall:

- a) Implement, maintain and enhance the digital tachograph system according to the directives of the MSA.
- b) Ensure that it will never create more than one certificate for each distinct Card Holder Reference (CHR) value.

2.5 Card Application Authorities (CAA)

2.5.1 CAA responsibilities

The CAA is responsible for the card application and management processes of the digital tachograph cards.

2.5.2 CAA obligations

[r15] The CAA shall:

- a) Verify, enter and modify the data of the driver, the company, the control body and workshop.

2.6 Control Bodies / Enforcers (CB)

2.6.1 Control Bodies / Enforcers responsibilities

The Control Bodies / Enforcers are responsible for:

- a) The use of TC information in conformance with the procedures and requirements as detailed in this policy, European Root Policy and Annex 1 B.
- b) The recognition of the genuineness of a TC.
- c) The acceptance of the TC information in legal procedures and processes of enforcing.

2.6.2 Control Bodies / Enforcers obligations

[r16] The Control Bodies / Enforcers shall:

- a) Rely on the information given by the MSA (life-cycle status information and events) and use that information only and exclusively for the enforcement of the Digital Tachograph system.
- b) Develop procedures and take necessary measures for the legal acceptance of TC information.
- c) Return withdrawn TC's to the responsible MSA.

2.7 Card Distributor (CD)

2.7.1 CD responsibilities

CD is responsible for delivering the TC according to the selected mode of delivery.

2.8 Card Manufacturer and Card Personaliser (CM/CP)

2.8.1 CM/CP responsibilities

The CM/CP is appointed by the MSA and is responsible for:

- a) The operation in conformance with the procedures and requirements as detailed in this policy.
- b) Production and personalization of the TC's requested by the MSA, by putting data into and printing visual data onto the cards.
- c) Generation of the TC equipment keys (EqT.SK and EqT.PK).
- d) Packaging and labeling of personalized TC's and the transfer to the CD.

2.8.2 CM/CP obligations

[r17] The Card Personaliser shall:

- a) Correctly implement all requirements on the manufacturing and personalization as detailed in this policy, European Root Policy, and Annex 1 B.
- b) Provide a controlled access to the premises and the Security Policy to be approved by the MSA, with respect to the personalization, key generation and key management processes (TC and Motion Sensor keys).
- c) Use and manage the EUR.PK, and the $K_{m_{wc}}$ received by the DFS-CA, in accordance with the requirements of this policy.
- d) Personalize only type approved TC's based on card requests and personalization data by the AP.
- e) Ensure that the subject has possession of the private key associated with the public key presented for certification.
- f) For each TC to be personalized:
 - 1) Generate an RSA key pair, in accordance with the requirements of this policy.
 - 2) Create a Equipment Key Certification Request (EQT.KCR) and forward that to the DFS-CA.

- 3) Receive from the DFS-CA either a TC Certificate and the MS.C or an error message stating the cause of the error.
 - 4) Store the Tachograph key pair and the corresponding MS.C on the TC and destroy any other existing copy of that key pair from every other storage after TC production.
 - 5) Package and label the personalized TC's for distribution and hand it over to the CD.
 - 6) Inform the AP of either the personalization success or failure.
 - 7) If the TC is a workshop card, store the $K_{m_{wc}}$ as received from the DFS-CA on the workshop card
- g) Keep the AP informed of the personalization and distribution progress of each TC.
 - h) Securely destroy all information of each TC that has been handed over to the CD.
 - i) Maintain adequate organizational and technical resources to operate in conformity with the requirements laid down in this MSA Policy and the Security Policy.

2.9 Certification Authority (DFS-CA)

2.9.1 DFS-CA responsibilities

The DFS-CA is responsible for:

- a) The operation in conformance with the procedures and requirements as detailed in this policy, European Root Policy, and Annex 1 B.
- b) Generation and management of Member State key pair(s) (MS.PK and MS.SK),
- c) Issuing of certificates for equipment public keys (Eq.C) upon request of the CP, but only upon approval from MSA,
- d) Keeping traceable records of all issued certificates,
- e) Managing the symmetric Motion Sensor key ($K_{m_{wc}}$), as received from the ERCA ($K_{m_{wc}}$ is used for personalization of Workshop cards),
- f) Disseminating the symmetric Motion Sensor key ($K_{m_{wc}}$) to card Personaliser upon request,
- g) Disseminating the DFS-CA certificate (MS.C) and ERCA public key (EUR.PK) to card Personaliser upon request.

2.9.2 DFS-CA obligations

[r18] The appointed DFS-CA shall:

- a) Correctly implement all requirements on the DFS-CA as detailed in this policy, European Root Policy and Annex 1 B.
- b) Issue the DFS-CA Certificate Practice Statement (DFS-CA CPS), to be approved by the MSA.
- c) Ensure the confidentiality of the Member State private key (MS.SK), as detailed in this policy.
- d) Ensure the confidentiality of the Motion Sensor key ($K_{m_{wc}}$), as detailed in this policy.
- e) For each MS key pair and matching certificate:
 - 1) Timely generate a new key pair (MS.SK and MS.PK), when the existing key pair's end of validity would prevent the processing of new equipment certification requests (certificate roll-over).
 - 2) DFS-CA should keep – within the scope of the instructions of the European 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 DFS-CA has to ensure that only the correct key is used at all times.
 - 3) Maintain the MS private key (MS.SK).
 - 4) Create an MS Key Certification Request (MS.KCR) for the MS.PK conform to the European Root Policy and forward it to ERCA.
 - 5) Use and manage the MS.C, as received from ERCA, in accordance with the requirements of this policy.

- f) Use and manage the EUR.PK and Km_{wc} as received from ERCA, in accordance with the requirements of this policy.
- g) Use and manage each Eqt.CHR, as received from the card Personaliser, in accordance with the requirements of this policy.
- h) Ensure policy compliance of Eqt.EOV, using Eqt.EOV as received in an Eqt.KCR from the CM/CP as described in the DFS-CA CPS.
- i) Validate the digital signature of each certification request to ensure the authenticity of that request.
- j) Ensure logging of all issued certificates and digitally signing the log to ensure data integrity.
- k) Use the certified MS private keys (MS.SK) only for digitally signing issued equipment certificates.
- l) Disseminate each Eqt.C, each MS.C, each EUR.PK and the Km_{wc} to the CM/CP, in accordance with the requirements of this policy.
- m) A written instruction shall exist, included in the DFS-CA CPS, which states the measures to be taken by security responsible persons at the DFS-CA, if the Member State private keys has become exposed or is otherwise considered or suspected to be compromised. In such case the DFS-CA shall inform the MSA and the ERCA without delay.

2.10 European Commission (EU COM)

The EU COM is consulted for colours or markings, such as national symbols and security features on digital tachograph cards before applying for an EU type approval.

2.11 European Root Certification Authority (ERCA)

2.11.1 ERCA responsibilities

ERCA is responsible for the establishment and maintenance of the trusted and interoperable certification chain between the Member States for the Digital Tachograph system.

2.11.2 ERCA obligations

[r19] ERCA shall:

- a) Provide and maintain the European Root Policy for The Digital Tachograph system in accordance with Council Regulation (EC) 2135/98 and its technical Annex 1 B, as described in Council Regulation (EC) 1360/2002.
- b) Establish and maintain a Root Certification Authority at European level.
- c) Approve the Member State Authority Policy.
- d) Disseminate the ERCA public key (EUR.PK) to the DFS-CA.
- e) Provide the Certificate Holder Reference (MS.CHR) to the DFS-CA.
- f) Certify the Member State Public Key (MS.PK).
- g) Disseminate the DFS-CA certificate (MS.C) to the DFS-CA.
- h) Manage and deliver Motion Sensor key (Km_{wc}) to the DFS-CA upon request.

2.12 Functional Test Authority (FTA)

2.12.1 Functional Test Authority responsibilities

The FTA is responsible for the functional testing of the TC.

2.12.2 Functional Test Authority obligations

[r20] The Functional Test Authority shall:

- a) Conduct the functional tests according to the specifications in Annex 1B.
- b) After successful tests, issue the functional certificate for the TC.

2.13 Type Approval Authority (TAA)

2.13.1 Type Approval Authority responsibilities

The TAA is responsible for the type approval for the digital TC according to Annex 1 B.

2.13.2 Type Approval Authority obligations

[r21] The type approval authority shall

- a) collect the three test certificates of the TC
 - 1) Security Certificate, issued by an ITSEC Organization
 - 2) Functional Certificate, issued by an FTA
 - 3) Interoperability Certificate, issued by the EU JRC
- b) Approve these certificates.
- c) Issue a type approval for the TC or
- d) Approve a valid type approval for the TC issued by another Type Approval Authority.

2.14 Security Test Authority (STA)

2.14.1 Security Test Authority responsibilities

The STA is responsible for the security testing of the TC.

2.14.2 Security Test Authority obligations

[r22] The Security Test Authority shall:

- a) Conduct the security tests according to the specifications in Annex 1B.
- b) After successful tests, issue the security certificate for the TC.

2.15 Interoperability Test Authority (IOTA)

2.15.1 Interoperability Test Authority responsibilities

The IOTA is responsible for the interoperability testing of the TC with the vehicle units of the various manufacturers.

2.15.2 Interoperability Test Authority obligations

[r23] The Interoperability Test Authority shall:

- a) Conduct the interoperability tests according to the specifications in Annex 1B.
- b) After successful tests, issue the interoperability certificate for the TC.

2.16 United Nation Economic Commission for Europe (UN ECE)

The UN ECE secretariat is consulted by the MSA for colours or markings, such as national symbols and security features on digital tachograph cards before applying for an AETR type approval.

2.17 Users

Users are defined as the authorized users of the equipment of the Tachograph system.

2.17.1 User responsibilities

The users are responsible for:

- a) The timely request for the TC at the CAA.
- b) The liability and correctness of the given information.
- c) The correct use of the TC and the confidentiality of the PIN-code (Workshop card only).
- d) Timely notification to the CAA when the TC is lost, stolen, malfunctioning, potentially compromised or becomes inaccurate.

2.17.2 User obligations

[r24] The MSA shall oblige the certificate holders to fulfill the following obligations:

- a) Submit accurate and complete information to the CAA in accordance to the requirements of this policy, in particular with regards to registration.
- b) Exercise reasonable care to avoid unauthorized use of the card.
- c) Only possess one valid driver card.
- d) Not use a damaged or expired card.
- e) Notify the CAA if:
 - 1) The card has been lost, stolen, is malfunctioning or potentially compromised.
 - 2) Control over the card has been lost due to compromise of the PIN-code (Workshop card only).
 - 3) The content of the card is, or becomes, inaccurate.

3 Additional provisions

This section contains additional provisions for the entities relating to other general issues pertaining to law and dispute resolution.

3.1 Liability

- [r25] The DFS-CA bears the responsibility for proper execution of its tasks, even if it subcontracts other parties for the execution of all or some of these tasks. If and when the DFS-CA intends to subcontract other parties, it shall inform the MSA of such intentions and provide the MSA with all the extra resources necessary for the MSA to meet its obligations.
- [r26] The DFS-CA shall ensure the following with respect to the Tachograph certificates:
- a) The information contained in the certificate at the time of issuance is that delivered to the DFS-CA by AP and CM/CP.
 - b) The certificate contains all information required for a Tachograph certificate at the time of issuance.
- [r27] The CM/CP bears the responsibility for proper execution of its tasks, even if it subcontracts other parties for the execution of all or some of these tasks. If and when the CM/CP intends to subcontract other parties, it shall inform the MSA of such intentions and provide the MSA with all the extra resources necessary for the MSA to meet its obligations.
- [r28] The CM/CP holds the private key corresponding to the public key identified in the certificate request. The private key is generated in a HSM and finally stored in the TC.
- [r29] TC's, keys and certificates are only for use within the Tachograph system. Any other certificates present on TC's are in violation of this policy, and hence neither the MSA, the CIA, the DFS-CA nor the CM/CP carries any liability in respect to any such.

Note: The DFS-CA shall issue a specific certificate if and only if it has received an Equipment Key Certification Request (Eqc.KCR) from the CM/CP with a valid digital signature from the AP with an AdminPKI certificate.

3.2 Financial responsibility

- [r30] If and when the CIA, CAA, DFS-CA, CM, CP or AP intend to change their service delivery in such a way that other parties need extra resources to continue meeting their respective responsibilities, they are obliged to inform the MSA of such intentions and, should the MSA approve such a change, they are obliged to provide each affected party with its respective extra resources or financial means to obtain those extra resources.
- [r31] The DFS-CA, CM, CP shall have adequate financial means and stability to fulfill the requirements in accordance to this policy.

3.3 Conformity and approval

3.3.1 Certification

- [r32] The DFS-CA shall have a quality assurance plan, conform ISO 9002 or equivalent.
- [r33] The DFS-CA shall have a security plan, conform ISO 17799 or equivalent.
- [r34] The CM/CP shall have a quality assurance plan, conform ISO 9002 or equivalent.
- [r35] The CM/CP shall have a security plan, conform ISO 17799 or equivalent.

Formal certification is not required.

3.3.2 Confidentiality

Confidentiality is restricted according to Directive [95/46/EC] and corresponding to Swiss law on the protection of individuals with regard to the processing of personal data and on the movement of such data.

3.3.3 Types of information to be kept confidential

- [r36] Any personal or corporate information held by the CIA, CAA, DFS-CA, CM, CP or AP which is not appearing on issued certificates is considered confidential.
- [r37] All private keys used and handled within the DFS-CA operation under this policy are to be kept confidential.
- [r38] All private keys used and handled within the CM/CP operation under this policy are to be kept confidential.
- [r39] Dissemination of any information, including audit logs and records, by the DFS-CA to any party, other than the MSA, shall require written approval by the MSA.

3.3.4 Types of information considered not to be confidential

- [r40] Card Numbers are not considered to be confidential.
- [r41] Certificates are not considered to be confidential.
- [r42] Identification information or other personal or corporate information appearing on certificates is not considered confidential.
- [r43] Certificate status information is not considered to be confidential.

4 Operational requirements

4.1 The DFS-CA Certification Practice Statement

[r44] The DFS-CA shall have a detailed statement of the practices and procedures used to address all the requirements identified in the MSA Policy.

Note: The DFS-CA CPS is written in German.

In particular:

- a) The DFS-CA CPS shall identify the obligations of all external organizations supporting the DFS-CA services including the applicable policies and practices.
- b) The DFS-CA CPS shall detail the respective operational activities resulting from the obligations of all external organizations supporting the DFS-CA services including the applicable policies and practices.
- c) The DFS-CA shall make available to users, upon their request, its approval document of the DFS-CA CPS, issued by the MSA and other relevant documentation, as necessary to assess conformance to the certification policy. The DFS-CA is not required to make the details of its practice public.
- d) The DFS-CA shall ensure the proper implementation of the practices.
- e) The DFS-CA shall define a review process for the DFS-CA CPS including responsibilities for maintaining the DFS-CA CPS.
- f) The DFS-CA shall:
 - 1) Give due notice of changes it intends to make in its DFS-CA CPS,
 - 2) Offer the changed DFS-CA CPS to MSA for approval, and
 - 3) Following approval, make the approval document on the revised DFS-CA CPS immediately available as required under c) above.

Note: The MSA shall disclose to all users the terms and conditions regarding the use of the keys and certificates as specified in this policy.

4.2 DFS-CA Key management

4.2.1 DFS-CA key generation

[r45] The DFS-CA shall ensure that DFS-CA keys are generated in controlled circumstances.

In particular:

- a) DFS-CA key generation shall be undertaken in a physically secured environment by personnel in trusted roles under at least dual control.
- b) DFS-CA key generation shall be carried out in a secure cryptographic device which either:
 - 1) meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS] or,
 - 2) is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408 [CC], to E3 or higher in ITSEC, or equivalent security criteria. This shall be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.
- c) DFS-CA key generation shall be performed in accordance with the specifications in the Regulation (in particular in Annex 1 B, appendix 11, § 2.2 and § 3.2).
- d) DFS-CA is responsible for generating a new DFS-CA key and certification request for every DFS-CA key that, during the DFS-CA public key certification, processed by the ERCA, appears not to be unique or otherwise invalid.

4.2.2 DFS-CA key storage, backup and recovery

[r46] The DFS-CA shall ensure that DFS-CA private keys remain confidential and maintain their integrity during their lifetime.

In particular:

- a) The DFS-CA private signing key(s) shall be held and used within a secure cryptographic device which:
 - 1) meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS]; or
 - 2) is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408 [CC], to E3 or higher in ITSEC, or equivalent security criteria. This shall be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.
- b) The DFS-CA shall ensure that export of its private signing key(s) outside the secure cryptographic device conforms to all of the following requirements:
 - 1) Every private signing key is allowed to be exported outside its secure cryptographic device only to be immediately imported into another secure cryptographic device, which must conform to at least the same techno-organizational security level as the original device.
 - 2) Every private signing key is allowed to be exported outside its secure cryptographic device only for service continuity purposes.
 - 3) Both the export and subsequent import procedures shall be undertaken in a physically secured environment by personal in trusted roles under at least dual control.
 - 4) Technical measure shall ensure that private keys being transported from one secure cryptographic device to the other are kept confidential at all times and that no copy of the key, even in an encrypted form, can be made during transit.

4.2.3 DFS-CA public key certification by ERCA

- [r47] The DFS-CA shall submit keys for certification by the ERCA using the key certification request (KCR) protocol as described in the European Root Policy.
- [r48] The DFS-CA shall recognize the ERCA public key in the distribution format as described in the European Root Policy.
- [r49] The DFS-CA shall use the physical media for key and certificate transport as required by the European Root Policy.
- [r50] The DFS-CA shall ensure that both the Key Identifier (KID) and modulus (n) of the DFS-CA keys submitted to the ERCA for certification, each are unique within the domain of the DFS-CA.
- [r51] The ERCA shall ensure that both the Key Identifier (KID) and modulus (n) of the DFS-CA keys submitted to it for certification are unique within the entire domain of the Digital Tachograph System as specified in EU Regulation 2135/89.

4.2.4 DFS-CA key usage

- [r52] The DFS-CA shall ensure that the DFS-CA private signing keys are only used for the production of national KCR for use within the Digital Tachograph system as specified in EU Regulation 2135/89.
- [r53] The DFS-CA shall ensure that, after certification of the national level keys, the DFS-CA private signing keys are only used for the production of public key certificates for use within the Digital Tachograph system as specified in EU Regulation 2135/89.
- [r54] Key escrow is strictly forbidden.

4.2.5 End of DFS-CA key life cycle

- [r55] The validity period of certificates issued by DFS-CA shall not exceed 7 years.
- [r56] The DFS-CA shall ensure that DFS-CA private signing keys shall not be used beyond the end of their life cycle.

In particular:

- a) ERCA limits the usage of DFS-CA signing keys to 2 years.
- b) Because the expected lifetime of a Driver, Control, or Company Card is not more than five years, DFS-CA certificates for DFS-CA signing keys for certificates of such cards shall have a validity of seven years.

- c) Workshop Cards are reissued each year. Although not really necessary, the validity of DFS-CA certificates for DFS-CA signing keys for certificates of such cards shall also have a validity of seven years.
- d) Because of the above, the same DFS-CA private signing key and corresponding DFS-CA certificate can be used for all TC's, as long as there is a key and certificate rollover every two years.
- e) All copies of DFS-CA private signing keys that have reached the end of their life cycle shall be destroyed such that the private keys cannot be retrieved. Note that the public key and certificate corresponding to a destroyed private key still lives on.
- f) The destruction of DFS-CA private signing keys shall take place in a secure and controlled environment and shall be fully documented.

[r57] With respect to service continuity, DFS-CA shall generate replacement DFS-CA keys in a timely manner (certificate roll-over).

4.2.6 Life cycle management of cryptographic hardware devices

[r58] The DFS-CA shall ensure the security of cryptographic hardware devices throughout the life cycle of these devices.

In particular, the DFS-CA shall ensure that:

- a) Key generation, key storage and certificate signing cryptographic hardware is not tampered during shipment or while stored.
- b) The installation, activation, back up and recovery of the DFS-CA's private signing keys in cryptographic hardware shall be undertaken in a physically secured environment by personnel in trusted roles under at least dual control.
- c) Key generation, key storage and certificate status information signing cryptographic hardware is functioning correctly, and
- d) DFS-CA private signing keys stored within cryptographic hardware are destroyed upon device decommission.

4.3 Equipment Key Management

4.3.1 Equipment key generation

[r59] The CM/CP shall ensure that Equipment Keys are generated in controlled circumstances.

In particular:

- a) Equipment key generation shall be undertaken in a physically secured environment by personnel in trusted roles.
- b) Equipment key generation shall be carried out in a secure cryptographic device which either:
 - 1) meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS]; or
 - 2) is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408 [CC], to E3 or higher in ITSEC, or equivalent security criteria. This shall be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.
- c) Equipment key generation shall be performed in accordance with the specifications in the Regulation (in particular in Annex 1 B, appendix 11, § 2.2 and § 3.2).
- d) CM/CP shall not generate a new equipment key and certification request for any equipment key that, during the equipment public key certification, processed by the DFS-CA, appears not to be unique or otherwise invalid.
- e) Duplicate public keys, generated by the CP, are detected by the DFS-CA and are replied with an error message.
- f) Key escrow is strictly forbidden.

4.3.2 Equipment key storage, backup and recovery

[r60] The CM/CP shall ensure that Equipment private keys remain confidential and maintain their integrity.

In particular:

- a) The CM/CP shall ensure that Equipment private key(s), generated by a secure cryptographic device, will be exported from that device for the sole purpose of immediate and subsequent import into the type approved equipment.
- b) The CM/CP shall ensure that equipment private key(s), exported from a secure cryptographic device and subsequently imported into a type approved equipment remains confidential during transit.
- c) The CM/CP shall ensure that Equipment private key(s), as generated by a secure cryptographic device, shall be removed from that device immediately following their export from that device and subsequent import into the type approved equipment.
- d) The CM/CP shall ensure that their choice of equipment ensures that private signing keys imported into type approved equipment cannot be exported from type approved equipment anymore.

[r61] The CM/CP shall not keep any copies of processed equipment private keys.

4.3.3 Life cycle management of cryptographic hardware devices

[r62] The CM/CP shall ensure the security of cryptographic hardware devices throughout the life cycle of these devices.

In particular, the CM/CP shall ensure that:

- a) Key generation cryptographic hardware is not tampered with during shipment or while stored.
- b) The installation and activation of cryptographic hardware shall be undertaken in a physically secured environment by personnel in trusted roles.
- c) Key generation cryptographic hardware is functioning correctly.

4.4 Equipment Certificate Management

4.4.1 Input data

[r63] Cardholding users do not apply for certificates; their certificates are issued based on the information given in the application for a TC. The public key to be certified is extracted from the key generation process by the CM/CP.

In particular:

- a) The AP shall ensure that the input data contains information which renders the Certificate Holder Reference (CHR) unique.
- b) The DFS-CA shall verify the authenticity and integrity of the certification request.

4.4.2 Certificate Issuing

[r64] The DFS-CA issues certificates if a proper certificate application is presented to the responsible authority and if 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 particular:

- a) The DFS-CA ensures within its domain, that its generated certificates are transferred only to the CM/CP.
- b) The DFS-CA produces certificates only for equipment and cards, for which a component type-approval was issued and is valid.
- c) Key certification requests that rely on transportation of private keys are not allowed.

4.4.3 Validity of Certificate

[r65] The validity period of certificates issued by the DFS-CA shall not exceed the maximum usage period of the corresponding cards and/or equipment.

Certificates for:

- a) Driver Cards not more than 5 years,
- b) Workshop Cards not more than 1 year,
- c) Control Cards not more than 5 years,
- d) Company Cards not more than 5 years.

The periods are calculated from the start of validity date of the card.

4.4.4 Certificate contents and formats

[r66] Contents and formats of the certificates produced by the DFS-CA meet the requirements of Regulations (EC) 3821/85, (EC) 2135/98 and (EC) 1360/2002, especially the specifications mentioned in supplement 11 of appendix 1 B.

In particular:

- a) The DFS-CA signs all the generated certificates with its signature key.
- b) The MSA ensures that the Key Identifier (KID) and modulus (n) of equipment keys submitted to the DFS-CA for certification are unique within the domain of the DFS-CA.

4.4.5 Information duties of the DFS-CA

[r67] The DFS-CA transfers all certificate data to the CM/CP, so that certificates, equipment as well as cards and cardholders are interlinked.

[r68] If the MSA proof a legitimate interest in special, non-public information on the functioning of the DFS-CA or its external contractors, and no rules or security considerations are standing against the delivery of this information, the DFS-CA makes available the information as quickly as possible in coordination with the MSA.

[r69] The operation concept of DFS-CA has to be treated confidentiality. Information contained in it may be viewed with the agreement of the MSA and at the location of the DFS-CA, when there is a proven, legitimate interest and when the confidentiality of the information is also adequately protected at the receiver.

4.5 Motion Sensor keys

[r70] The CP generates the transport key-pair and the KDR.

[r71] The KDR will be forwarded to the ERCA through the DFS-CA by the trusted courier of the MSA.

[r72] The DFS-CA shall, as needed, request the motion Sensor master key $K_{m_{WC}}$ from the ERCA (Regulation Annex 1 B, appendix 11, § 3.1.3) all in accordance with the requirements that are specified in Annex 1 B of the Digital Tachograph System European Root Policy..

In particular, the DFS-CA shall:

- a) Format a Motion Sensor Master Key Distribution Request (KDR) in accordance with section D.1.5 of the European Root Policy;
in particular:
 - 1) The motion Sensor master key type byte of the MRA shall be '27h'.
 - 2) The NationNumeric of the KID shall be '0Ah'.
 - 3) The NationAlpha of the KID shall be '434820h' ('CH').
 - 4) The master key type of the KID shall be '27h'.
- b) Use the KID of a labeled motion sensor key (LKM) to determine the corresponding Motion Sensor Master Key Distribution Request (KDR).
- c) Describe the details of the Motion Sensor Master Key Distribution process in its Certification Practice Statement (DFS-CA CPS).

- [r73] The DFS-CA shall, upon request, forward the workshop key $K_{m_{WC}}$ to the CM/CP for insertion only into the workshop cards.
- [r74] The CM/CP shall ensure that the workshop key $K_{m_{WC}}$ is inserted into all issued Workshop cards (Regulation Annex 1 B, appendix 11, § 3.1.3).
- [r75] The DFS-CA shall, during storage, use and distribution, protect the motion sensor keys with high assurance physical and logical security controls. The keys should be stored in and operated from a specific tamper resistant device which:
- meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS]; or
 - is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408 [CC], to E3 or higher in ITSEC, or equivalent security criteria. This shall be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.
- [r76] The CM/CP shall, during storage and use, protect the motion sensor key with high assurance physical and logical security controls. The motion sensor key should be stored in and operated from a specific tamper resistant device which:
- meets the requirements identified in FIPS 140-2 (or 140-1) level 3 or higher [FIPS]; or
 - is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO 15408 [CC], to E3 or higher in ITSEC, or equivalent security criteria. This shall be to a security target or protection profile that meets the requirements of the current document, based on risk analysis and taking into account physical and other non-technical security measures.

4.6 Identification and authentication

4.6.1 Initial registration

- [r77] The MSA shall ensure that evidence of subjects' identification and accuracy of the names and associated data are properly examined as part of the registration service (card issuing process) and that the associated certificate requests are accurate, duly authorized and complete. In particular:
- The MSA shall inform the users of the terms and conditions regarding the use of the certificates.
 - The MSA shall communicate this information through a durable means of communication in readily understandable language.
 - The MSA shall collect adequate evidence from an appropriate and authorized source of the identity and any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation. Verification of the subject's identity shall be by appropriate means and in accordance with national law.
 - If the subject is a physical person, evidence of the subject identity shall be checked against a nationally recognized identity document, i.e. a driver license.
 - If the subject is a physical person who is identified in association with a legal person or organizational entity, e.g. a Workshop, evidence of the subject identity shall be checked against a nationally recognized identity document, i.e. a driver's license, and evidence that the subject is associated with the legal person or organizational entity,
 - if the subject is an organizational entity, evidence shall be provided by means of checking a recognized registration.
 - The MSA shall ensure that the requirements of the issuing offices are adhered to within the registration process.

4.6.2 Certificate generation

[r78] The DFS-CA shall ensure that it issues certificates securely to maintain their authenticity.

In particular:

- a) The certificate content shall be conform to the requirements of the Regulation Annex 1 B, appendix 11, § 3.3.1.

4.6.3 Certificate dissemination

[r79] The DFS-CA shall ensure that certificates are made available as necessary to the Card Personaliser.

In particular:

- a) Following generation, the complete and accurate certificate will be made available to the CM/CP in a batch file.

4.6.4 Certificate renewal

[r80] The ERCA key pair shall never be renewed.

[r81] The MSA key pair shall never be renewed.

[r82] Equipment key pairs shall never be renewed.

4.6.5 Certificate revocation and suspension

[r83] Equipment certificates are never revoked or suspended.

4.6.6 Dissemination of terms and conditions

[r84] The MSA shall ensure that the terms and conditions are made available to users.

In particular:

- a) The MSA shall make the following information available to users the terms and conditions regarding the use of the certificates:
 - 1) The MSA Policy,
 - 2) any limitation on the use of certificates,
 - 3) the users obligations,
 - 4) any limitations of liability,
 - 5) the period of time during which registration information is retained,
 - 6) if the DFS-CA has been assessed by the MSA to be conform to the MSA Policy.
- b) The information identified in a) shall be available through a durable means of communication, which may be transmitted electronically, and in readily understandable language.

4.7 Personnel security

[r85] The MSA, DFS-CA and CM/CP shall ensure that personnel enhance and support the trustworthiness of their operations.

In particular:

- a) They shall employ a sufficient number of personnel that possess the expert knowledge, experience and qualifications necessary for the offered services.
- b) Security roles and responsibilities shall be documented.
- c) Trusted roles shall be clearly identified.
- d) MSA, DFS-CA and CM/CP personnel shall have job descriptions defined from the point of view of separation of duties.

- e) All MSA, DFS-CA and CM/CP personnel in trusted roles shall have appropriate background screening with positive result (=able to fulfill their duty).
- f) All MSA, DFS-CA and CM/CP personnel in trusted roles shall be free from conflicting interest that might prejudice the impartiality of the MSA, DFS-CA and CM/CP operations.
- g) Trusted roles include roles that involve the following responsibilities:
 - 1) Security Officers: overall responsibility for administering the implementation of the DFS-CA and CM/CP security policies.
 - 2) System Administrator: authorized to install, configure and maintain the DFS-CA and CM/CP trustworthy systems for registration, certificate generation and revocation, TC personalization and key management (national, motion sensor and TC keys).
 - 3) System Operator: responsible for operating the DFS-CA and CM/CP trustworthy systems on a day-to-day basis.
 - 4) System Auditors: authorized to view archives and audit logs of the DFS-CA and CM/CP trustworthy systems.
- h) DFS-CA and CM/CP personnel shall be formally appointed to trusted roles by senior management of the DFS-CA, CM/CP and the MSA.
- i) No single person shall be appointed to more than one role.

4.8 Operational requirements

[r86] The CM/CP and DFS-CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards.

In particular:

- a) The CM/CP security policy considers EMV regulations, outlined by VISA- and MasterCard-Credit Card organization. The security measures and operational procedures are verified regularly by MasterCard and Visa on the occasion of comprehensive audits. The pass of these verifications and tests is a pre-condition for credit card personalization.
- b) The responsibility for all aspects of the provision of key certification services shall be retained, even if some functions are outsourced to subcontractors. Responsibilities of third parties shall be clearly defined and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the DFS-CA or CM/CP.
- c) The CM/CP security policy is based on EMV regulations, required by VISA and MasterCard credit card organization.
- d) The information security infrastructure necessary to manage the security shall be maintained at all times.
- e) The security controls and operating procedures for facilities, systems and information assets providing the certification services shall be documented, implemented and maintained.

4.9 Audit

[r87] The MSA is responsible for ensuring that regular audits of the MSA, DFS-CA and CM/CP take place.

In particular:

- a) The DFS-CA operating under the MSA Policy shall be audited at least once within 12 months for conformance with this policy.
- b) The CM/CP operating under the MSA Policy shall be audited at least once within 12 months for conformance with this policy.
- c) The audit shall cover the DFS-CA's, CM/CP's practices with this MSA Policy.
- d) The audit shall cover the MSA, DFS-CA's, CM/CP's compliance with this MSA Policy.
- e) The audit shall also consider the operations of any AP and Service Agencies.

- f) The MSA is responsible for planning and conducting the audits. The MSA may consult or sub-contract an external certification or accreditation organization for the audit.
- g) The MSA will formally approve the results of the audit.
- h) If irregularities are found in the audit, the MSA shall take appropriate action depending on severity.
- i) Conclusive results of the audits shall be generally available upon request. (Conclusive result is here defined to be information of all irregularities that may affect a user's trust in a certificate, including an adequate judgment of its level of seriousness but excluding detailed information that can be used to attack the system).
- j) The MSA shall report the results of audits as mentioned in this section and provide the audit report, in English, to the ERCA.
- k) The audit reports shall define any corrective actions, including an implementation schedule, required to fulfill the MSA obligations.

4.10 The MSA Policy change procedures

4.10.1 Items that may change without notification

[r88] The only changes that may be made to this policy without notification are:

- a) Editorial or typographical corrections.
- b) Changes to the contact details.

4.10.2 Changes with notification

[r89] Any item in this policy may be changed with 90 days notice.

[r90] Changes to items that, by the judgment of the MSA, will not materially impact a substantial majority of the users using this policy may be adopted with 30 days notice.

4.10.3 Comment period

[r91] Impacted users may place comments concerning a proposed MSA Policy change to the MSA within 15 days of original notice.

4.10.4 Whom to inform

[r92] Information about changes to this policy shall be sent to:

- a) The ERCA,
- b) DFS-CA, CM/CP including application providers.

4.10.5 Period for final change notice

[r93] If the proposed change is modified as a result of comments, notice of the modified proposed change shall be given at least 30 days prior to the change taking effect.

4.10.6 Changes requiring a new MSA Policy approval

[r94] If a policy change is determined by the MSA to have a material impact on a significant number of users of the policy, the MSA shall submit the revised MSA Policy to the ERCA for approval.

Note:

The MSA will in all cases consult the ERCA with respect to the necessity of renewal of the approval as result of the changes in the MSA Policy.

4.11 DFS-CA or CP Termination

4.11.1 Final termination - MSA responsibility

Final termination of the DFS-CA or CP is regarded as the situation where all service associated with a logical entity is terminated permanently. It is not the case where the service is transferred from one organization to another or when the DFS-CA service is passed over from an old State key pair to new State key pair or ERCA key.

[r95] The DFS-CA or CP shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the termination of the DFS-CA's or CP's services, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

In particular:

- a) Before the DFS-CA terminates its services the following procedures shall be executed as a minimum:
 - 1) The DFS-CA or CP shall, without delay, inform the MSA which, without delay, informs all relying parties and the ERCA,
 - 2) The DFS-CA or CP shall terminate all authorization of subcontractors to act on behalf of the DFS-CA or CP in the performance of any functions related to the process of issuing certificates or keys;
 - 3) The DFS-CA or CP shall perform necessary undertakings to transfer obligations for maintaining event log archives for their respective period of time as indicated to the subscriber and relying party,
 - 4) The DFS-CA or CP shall destroy its private keys, motion sensor master key $K_{m_{WC}}$ and any backup of these keys,
 - 5) Under the control of the MSA, the DFS-CA or CP shall perform all necessary undertakings to transfer back to the MSA the hardware systems, licenses, its operating and CA management softwares which are owned by the MSA.
- b) The DFS-CA or CP shall have an arrangement with the MSA to cover the costs to fulfill these minimum requirements in case the DFS-CA or CP becomes bankrupt or for other reasons is unable to cover the costs by itself.
- c) The DFS-CA or CP shall state in its practices the provisions made for termination of service. This shall include:
 - 1) The notification of affected entities,
 - 2) Make publicly available information of its termination at least 3 month prior to termination,
 - 3) The transfer of its obligations to other parties,
 - 4) The handling of the status information for certificates that have been issued.
- d) The DFS-CA or CP shall perform necessary undertakings to maintain and provide continuous access to record archives.

4.11.2 Transfer of DFS-CA or CP responsibility

Transfer of MSCA or CP responsibility occurs when the MSA chooses to appoint a new DFS-CA or CP in place of the former entity.

- [r96] The MSA shall ensure that orderly transfer of responsibilities and assets is carried out.
- [r97] Under the control of the MSA, the DFS-CA or CP shall perform all necessary undertakings to transfer back to the MSA the hardware systems, licenses, its operating and CA management software which are owned by the MSA.
- [r98] The old DFS-CA shall transfer all root keys, motion sensor master key $K_{m_{WC}}$ and all backups to the new DFS-CA in the manner decided by the MSA,
- [r99] The CP shall destroy the motion sensor master key $K_{m_{WC}}$ including any backup of this key,
- [r100] After transfer, the old DFS-CA or CP shall no more be in possession of any key material or backup for/from the DFS-system.

5 Conformity to the ERCA Policy

The requirements for this MSA-Policy are formulated in the European Root Policy § 5.3. The table below provides the rationale between the requirements as formulated in the European Root Policy and the requirements in this MSA-Policy.

Reference ERCA policy	Requirements	Reference in this MSA Policy
5.3.1	The MSA policy shall identify the entities in charge of operations.	2.3.3 MSA appointed entities
5.3.2	Member State Key Pairs for equipment key certification and for motion sensor master key distribution shall be generated and 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 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.	4.2.1 DFS-CA key generation 4.2.2 DFS-CA key storage, backup and recovery 4.5 Motion Sensor keys
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.	4.2.1 DFS-CA key generation
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.	4.2.5 End of DFS-CA key life cycle
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 (see Section 4.2.5).	4.2.5 End of DFS-CA key life cycle [r57]
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.	4.2.3 DFS-CA public key certification by ERCA
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.	4.5 Motion Sensor keys [r72]
5.3.8	The MSA shall recognize the ERCA public key in the distribution format described in Annex B.	4.2.3 DFS-CA public key certification by ERCA [r48]
5.3.9	The MSA shall use the physical media for key and certificate transport described in Annex C.	4.2.3 DFS-CA public key certification by ERCA [r49]
5.3.10	The MSA shall ensure 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 MSCA.	4.2.3 DFS-CA public key certification by ERCA 4.5 Motion Sensor keys
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.	4.2.5 End of DFS-CA key life cycle

5.3.12	<p>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</p> <ul style="list-style-type: none"> • 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; <p>The last two of these requirements on generation shall be met by generating equipment keys within a device which either:</p> <p>a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher [9];</p> <p>b) is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2 [10];</p> <p>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.</p> <p>d) is demonstrated to provide an equivalent level of security.</p>	<p>4.3.1 Equipment key generation</p> <p>4.3.2 Equipment key storage, backup and recovery</p> <p>4.3.3 Life cycle management of cryptographic hardware devices</p> <p>2.3.2 MSA/CIA obligations [r6] m)</p> <p>2.8.2 CM/CP obligations [r17] d)</p>
5.3.13	<p>The MSA shall ensure confidentiality, integrity, and availability of the private keys generated, stored and used under control of the MSA policy.</p>	<p>2.3.2 MSA/CIA obligations</p> <p>2.9.2 DFS-CA obligations</p> <p>2.8.2 CM/CP obligations</p> <p>4.2.2 DFS-CA key storage, backup and recovery</p>
5.3.14	<p>The MSA shall prevent unauthorised use of the private keys generated, stored and used under control of the MSA policy.</p>	<p>2.3.2 MSA/CIA obligations</p> <p>4.2.4 DFS-CA key usage</p>
5.3.15	<p>The Member State private keys may be backed up using a key recovery procedure requiring at least dual control.</p>	<p>4.2.2 DFS-CA key storage, backup and recovery</p>
5.3.16	<p>Key certification requests that rely on transportation of private keys are not allowed.</p>	<p>4.4.2 Certificate Issuing</p>
5.3.17	<p>Key escrow is strictly forbidden (see definition 12.1).</p>	<p>4.2.4 DFS-CA key usage</p> <p>4.3.1 Equipment key generation</p> <p>4.3.2 Equipment key storage, backup and recovery</p>
5.3.18	<p>The MSA shall prevent unauthorised use of its motion sensor keys.</p>	<p>4.5 Motion Sensor keys</p>
5.3.19	<p>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].</p>	<p>Not applicable</p> <p>4.5 Motion Sensor keys</p>

5.3.20	The motion sensor master key (Km) shall never leave the secure and controlled environment of the MSA.	Not applicable 4.5 Motion Sensor keys
5.3.21	The MSA shall forward the workshop card motion sensor key (KmWC) to the component Personaliser (in this case, the card personalization service), by appropriately secured means, for the sole purpose of insertion into workshop cards.	4.5 Motion Sensor keys
5.3.22	The MSA shall forward the vehicle unit motion sensor key (KmVU) to the component Personaliser (in this case, a vehicle unit manufacturer), by appropriately secured means, for the sole purpose of insertion into vehicle units.	Not applicable 4.5 Motion Sensor keys
5.3.23	The MSA shall maintain the confidentiality, integrity, and availability of its motion sensor key copies.	4.5 Motion Sensor keys
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.	4.5 Motion Sensor keys
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.	Not applicable 4.2.5 End of DFS-CA key life cycle
5.3.26	The MSA shall ensure availability of its equipment public key certification service.	2.9.2 DFS-CA obligations e) 2.3.2 MSA/CIA obligations
5.3.27	The MSA shall only use the Member State Private Keys for: a) the production of Annex 1(B) equipment key certificates using the ISO / IEC 9796-2 digital signature algorithm as described in Annex 1(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 method is used for providing certificate status information (see 5.3.31)	2.9.2 DFS-CA obligations 4.2.4 DFS-CA key usage
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).	4.2.2 DFS-CA key storage, backup and recovery
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).	4.4.4 Certificate contents and formats
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.	4.4.1 Input data [r63] b) 4.4.2 Certificate Issuing
5.3.31	The MSA shall maintain and make certificate status information available.	2.3.2 MSA/CIA obligations, [r6] q) 4.6.5 Certificate revocation and suspension
5.3.32	The validity of a Tachograph Card certificate shall equal the validity of the Tachograph Card.	4.4.3 Validity of Certificate
5.3.33	The MSA shall prevent the insertion of undefined validity certificates into Tachograph Cards.	4.4.3 Validity of Certificate

5.3.34	The MSA may allow the insertion of undefined validity Member State certificates into vehicle units.	Not applicable 4.4.3 Validity of Certificate
5.3.35	The MSA shall ensure that users of cards are identified at some stage of the card issuing process.	4.6.1 Initial registration
5.3.36	The MSA shall ensure that ERCA is notified without delay of loss, theft, or potential compromise of any MSA keys.	2.9.2 DFS-CA obligations [r18] m)
5.3.37	The MSA shall implement appropriate disaster recovery mechanisms which do not depend on the ERCA response time.	2.9.2 DFS-CA obligations [r18] e)
5.3.38	The MSA shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved.	3.3.1 Certification 4.8 Operational requirements
5.3.39	The MSA shall ensure that the policies address personnel training, clearance and roles.	4.2.1 DFS-CA key generation 4.7 Personnel security
5.3.40	The MSA shall ensure that appropriate records of certification operations are maintained.	2.9.2 DFS-CA obligations [r18] j)
5.3.41	The MSA shall include provisions for MSCA termination in the MSA policy.	4.2.5 End of DFS-CA key life cycle 4.11 DFS-CA or CP Termination
5.3.42	The MSA policy shall include change procedures.	4.10 The MSA Policy change procedures
5.3.43	The MSA audit shall establish whether the Requirements of this Section are being maintained.	4.9 Audit 5 Conformity to the ERCA Policy
5.3.44	The MSA shall audit the operations covered by the approved policy at intervals of not more than 12 months.	4.9 Audit
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.	4.9 Audit
5.3.46	The audit report shall define any corrective actions, including an implementation schedule, required to fulfill the MSA obligations.	4.9 Audit

6 References

[CC]	Common Criteria. ISO/IEC 15408 (1999): "Information technology - Security techniques - Evaluation criteria for IT security (parts 1 to 3)".
[CEN]	CEN Workshop Agreement 14167-2: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)
[FIPS]	FIPS PUB 140-2 (May 25, 2001): "Security Requirements for Cryptographic Modules". Information Technology Laboratory, National Institute of Standards and Technology (NIST)
[ISO 17799]	BS ISO/IEC 17799: 2005. Information technology -- Code of practice for information security management.
[CSG]	Common Security Guideline, Card Issuing Project. (under construction), owned by the Commission
[TEMP]	Guideline and Template National CA policy, Version 1.0, 31.10.2004, Card Issuing Project, SWG3
[ROOTP]	Digital Tachograph System European Root Policy Version 2.0, Special Publication I.04.131
[Annex 1 B]	Commission Regulation 1360/2002/EC
[FKRV]	SR 822.223, Swiss Regulation for the Card Register of the Tachograph, Verordnung über das Fahrtschreiberkartenregister
[TGV]	SR 741.511, Swiss Regulation for Type Approval of Vehicles (including TC cards), Verordnung über die Typengenehmigung von Strassenfahrzeugen
[95/46/EC]	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Table 2: References

7 Web Links

The Systematic Collection of Swiss Legislation can be found on the web site with the given number (SR nnn.nnn) on address:

<http://www.admin.ch/ch/d/sr/sr.html>

as well as in the official collection of decisions of the Swiss Federal Council

http://www.admin.ch/ch/d/as/2006/index0_18.html

The EU legislation can be found on the web site EUR-Lex, the portal to European Union law:

http://europa.eu.int/eur-lex/en/search/search_lif.html

The ERCA-CP can be found on the web site of the Joint Research Centre:

<http://drc.jrc.it>

All information on the digital tachograph can be found on the following web site:

<http://www.dfs.astra.admin.ch> or <http://dfs.astra.admin.ch>

8 Glossary/Definitions and Abbreviations

8.1 Glossary/Definitions

AdminPKI: AdminPKI is the certification authority of the federal office of information technology and telecommunication.

CA Policy: A named set of rules that indicates the applicability of keys, certificates and equipment to a particular community and/or class of application with common security requirements.

Card/Tachograph Cards: Integrated Circuit equipped card, in this policy this is equivalent to the use of the terms "IC-Card" and "Smart Card".

Card holder: A person or an organization that is a holder and user of a Tachograph Card. Included are drivers, company representatives, workshop workers and control body staff.

Certificate: In a general context a certificate is a message structure involving a binding signature by the issuer verifying that the information within the certificate is correct and that the holder of the certified public key can prove possession of the associated private key.

Certification Authority System (CAS): A computer system in which certificates are issued by signing certificate (user) data with the CA private signing key.

Card Issuing Authority (CIA): Organizations processing Tachograph Cards issuing.

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in issuing certificates and is connected to the actual CA policy. The CPS is in this National CA policy replaced by a Practice Statement, because it has a broader view and connects to keys, certificates and equipment.

Contracting Party: Switzerland is not an EU Member State. Instead, Switzerland is considered as a Contracting Party.

Equipment: In the Tachograph system the following equipment exists: Tachograph Cards, VU (vehicle units) and Motion Sensors.

Key escrow: The submission of a copy of a key to an entity authorised to use this copy for some purpose other than returning it to the originating entity.

Manufacturer / Equipment manufacturer: Manufacturers of Tachograph equipment. In this policy most often used for VU and Motion Sensor manufacturers, since these have distinct roles in the System.

Motion Sensor key: A symmetric key used for the Motion Sensor and VU to ensure the mutual recognition.

Practice Statement (PS): A statement of the security practices employed in the Tachograph processes. A PS is comparable to the standard PKI document CPS.

Private key = Secret key: The private part of an asymmetric key pair used for public key encryption techniques. The private key is typically used for signing digital signatures or decrypting messages.

Public key: The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages to the owner of the private key.

RSA keys: RSA is the cryptographic algorithm used for asymmetric (PKI) keys in the Tachograph system.

Service Agency: An entity that takes over tasks on behalf of a DFS-CA, a subcontractor.

Tachograph Cards/Cards: Four different type of smart cards for use in the Tachograph system: Driver card, Company card, Workshop card, Control card.

User: Users are equipment users and are either Card Holders for card or manufacturers for Vehicle units/Motion Sensors. All users shall be uniquely identifiable entities.

Table 3: Glossary

In this document:

Signed: Where this policy requires a signature, the requirement is met by a secure and verifiable digital signature.

Written: Where this policy requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for the parties concerned.

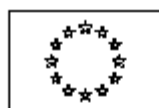
8.2 List of abbreviations

AETR	Accord Européen sur les Transports Routiers, UN ECE Geneva
AP	Application Provider
BIT	Federal Office of Information Technology and Telecommunication (Bundesamt für Informatik und Telekommunikation)
C	Certificate
CA	Certification Authority
CAA	Card Application Agencies
CAR	Certification Authority Reference
CB	Control Bodies
CC	Common Criteria
CD	Card distributing organization
CHA	Certificate Holder Authorisation
CIA	Card Issuing Authority
CM	Card manufacturing organization
CP	Card personalizing organization
CPS	Certification Practice Statement
DFS	Digitale Fahrtschreiber (Digital Tachograph)
DFS-CA	Certification Authority
DFS-CA	Member State CA (Swiss Federal Office for Information Technology and Telecommunication FOITT)
EC	European Community
EQT	Equipment (Tachograph Card)
EqT.CHR	Equipment Certification Holder Reference
EqT.CPI	Equipment Certification Profile Identifier
ERCA	European Root CA
ETEC	Department of the Environment, Transport, Energy, and Communication
EU	European Union
EUR.PK	European Public Key
FEDRO	Federal Roads Authority (Bundesamt für Strassen)
FEDRO	Swiss Federal Roads Authority
FIBU	Financial Book Keeping (Finanzbuchhaltung)
FKR	Swiss Register of Tachograph Cards (Fahrtschreiberkartenregister)
FKRV	Swiss regulation for the Register of the Digital Tachograph (Fahrtschreiberkontrollkartenregister)
FOGRA	Forschungsgesellschaft Druck e.V., Germany
FTA	Functional Test Agency
ISSO	Information System Security Officer
ITSEC	Information Technology Security Evaluation Criteria
JRC	Joint Research Center, Ispra (I)
KBA	Federal Bureau of Motor Vehicles and Drivers (Kraftfahrt-Bundesamt), Germany
KG	Key Generation
KM_{wc}	Motion Sensor Key
METAS	Swiss Federal Office of Metrology and Accreditation
MRA	Message Recipient Authorization

MS	Member State for the Tachograph system (Switzerland)
MSA	Member State Authority (Federal Roads Authority FEDRO, Switzerland)
NRMG	National Risk Management Group
PIN	Personal Identification Number
PK	Public Key
PKI	Public Key Infrastructure
PS	Practice Statement
RSA	A specific Public key algorithm
SA	System Administrator
SK	Secret Key = Private Key
SR	Systematically law collection (Systematische Rechtssammlung)
TAA	Type Approval Authority (Swiss METAS, German KBA)
TC	Tachograph Card
TGV	SR 741.511 Swiss Regulation for Type Approval (Typengenehmigungsverordnung)
UVEK	Department of the Environment, Transport, Energy and Communications
VU	Vehicle Unit

Table 4: List of abbreviations

9 Letter of Conformity to ERCA Policy



EUROPEAN COMMISSION
DIRECTORATE GENERAL JRC
JOINT RESEARCH CENTRE
Institute for the Protection and Security of the Citizen
Traceability and Vulnerability Assessment Unit

06 July 2006
G07-TRVA/JB/jb/(2006)D16730

Federal Department of Environment, Transport,
Energy and Communications (DETEC)
Swiss Federal Roads Authority
Road Traffic Division
Mühlestrasse 2
CH-3063 Ittigen
Switzerland

To the attention of: Mr. Christoph Baier

Subject: Start of services to Switzerland

Dear Mr. Baier,

We confirm the receipt by e-mail of the following documents in response to our letter D16565:

1. Swiss MSA Policy, Version 0.99, 5th July 2006 (registered as A10242);
2. FIPS 140 validation certificate no.363 (device used for transport key generation);
3. FIPS 140 validation certificate no.570 (device used for card key generation).

The Swiss MSA policy has been reviewed for conformity with Chapter 5 of the ERCA policy. All of the change requests defined in our letter D16565 have been addressed in a satisfactory manner, and we confirm the approval of the Swiss MSA policy.

All of the requests for additional information defined in our letter D16565 have been satisfied, and we confirm our readiness to initiate key certification and distribution services to the entities operating under the Swiss MSA policy.

Yours sincerely,

J.W.Bishop

Attachments: None

Copy: J.-M.Cadiou, A.Poucet, J.-P.Nordvik (DG-JRC); L. Huberts (DG-TREN)

J.W.Bishop G07-TRVA
Tel: +39-0332-786225
Fax: +39-0332-786280
e-mail: james.bishop@jrc.it

1/1

D16730 Start of services 2006-07-06.doc