Bundesministerium
Verkehr, Innovation
und Technologie

Digital Tachograph System im Straßenverkehr für die Republik Österreich

Austrian Member State Authority Policy

Version 3.1.2

07.05.2019

Freigegeben durch das
Bundesministerium für Verkehr, Innovation und Technologie
in Erfüllung der Aufgaben als österreichische Member State Authority (A-MSA)

Wien, am 7.5.2019

Franz Mahrhauser

Franz Mahrhauser

Inhalt

1 Einleitung

Aus Gründen der leichteren Lesbarkeit wird im vorliegenden Dokument die gewohnte männliche Sprachform bei personenbezogenen Substantiven und Pronomen verwendet. Dies impliziert jedoch keine Benachteiligung des weiblichen Geschlechts, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen sein.

Dieses Dokument ist die Member State Authority Policy der Republik Österreich, im Folgenden kurz als die A-MSA Policy bezeichnet, für das digitale Kontrollgerät gemäß

- der Verordnung [VO (EU) Nr. 165/2014] idgF,
- des [Annex 1B] [VO (EG) Nr. 1360/2002],
- des [Annex 1C] Durchführungsverordnungen [VO (EU) Nr. 2016/799] und [VO (EU) Nr. 2018/502] (technische Anpassung)

Diese A-MSA Policy setzt die gesetzlichen Anforderungen und die Anforderungen der [ERCA Policy Gen 1] und [ERCA Policy Gen 2] auf die österreichische Implementierung des Digital Tachograph Systems um. Damit umfasst diese A-MSA Policy sowohl die erste als auch die zweite Generation des Digital Tachograph Systems. Sie beschreibt die Beantragung und Handhabung von Kontrollgerätekarten/Fahrtenschreiberkarten der zweiten Generation, welche kryptographische Objekte sowohl von der ersten als auch der zweiten Generation enthalten.

Diese Version dieser A-MSA Policy tritt abhängig vom jeweiligen Kartentyp mit dem Zeitpunkt der Umstellung auf Kontrollgerätekarten/Fahrtenschreiberkarten der zweiten Generation in Kraft. Die bis zu dieser Umstellung auf die zweite Generation der Kontrollgerätekarten/Fahrtenschreiberkarten ausgestellten Kontrollgerätekarten/ Fahrtenschreiberkarten der ersten Generation sind durch A-MSA Policy Version 2.7 abgedeckt.

Diese A-MSA Policy beschreibt das Umfeld für die Beantragung, Erzeugung und Ausgabe der benötigten Kontrollgerätekarte/Fahrtenschreiberkarte an die jeweilige Person sowie die Aufgaben

- der Austrian-Card Issuing Authorities (A-CIA)
- der Austrian-Member State Certification Authority (A-MSCA)
- des Austrian-Component Personalizer (A-CP)

Die innerhalb dieser A-MSA Policy geregelten Kontrollgerätekarten/Fahrtenschreiberkarten dürfen nur im Sinne der oben genannten Bestimmungen eingesetzt werden.

Bestimmungen, die sich auf Fahrzeugeinheiten, Bewegungssensoren und externe GNSS-Einrichtungen beziehen sind derzeit durch diese A-MSA Policy nicht abgedeckt. Diese A-MSA Policy bezieht sich auf das Management der Kontrollgerätekarten/Fahrtenschreiberkarten für die digitalen Fahrzeugeinheiten innerhalb Österreichs. Im Bedarfsfall ist diese A-MSA Policy anzupassen.

1.1 Überblick

Ziel des Digital Tachograph System ist, die Umsetzung des europaweiten Vorhabens einer verbesserten Kontrolle der Lenk- und Ruhezeiten der Fahrer von Lastwagen und Bussen.

Dies soll durch die Verwendung von elektronischen Aufzeichnungsgeräten (oder Fahrzeugeinheiten) erreicht werden, gegenüber welchen sich Fahrer, Kontrollorgane, etc. mittels Chipkarte und kryptographisch gesichertem Zertifikat authentisieren.

Die Erweiterung des Digital Tachograph Systems der ersten Generation um die Funktionalität der zweiten Generation entspricht der Unterstützung einer neuen PKI. Um die Kompatibilität der Kontrollgerätekarten/Fahrtenschreiberkarten und Kontrollgeräte/Fahrtenschreiber zwischen den beiden Generationen des Digital Tachograph Systems zu gewährleisten, werden die kryptographischen Objekte der ersten Generation und der zweiten Generation auf die Kontrollgerätekarten/Fahrtenschreiberkarten aufgebracht.

Im System werden 4 Kartentypen verwendet:

- Die Fahrerkarte wird für einen Fahrer persönlich ausgestellt. Die Fahrerkarte ermöglicht die Speicherung von Tätigkeitsdaten. Die von den Fahrzeugeinheiten aufgezeichneten Daten werden eindeutig einem Fahrer zugeordnet.
- Die Unternehmenskarte wird für Unternehmen ausgestellt, die Fahrzeuge mit digitalen Fahrzeugeinheiten einsetzen. Mit dieser Karte werden Aufzeichnungen aus der Fahrzeugeinheit ausgelesen und das Auslesen dieser Daten durch andere Unternehmen verhindert.
- Die Werkstattkarte wird an geeignete Mitarbeiter einer Werkstatt persönlich ausgestellt und ist für den Einbau und die Kalibrierung der Bewegungssensoren und Fahrzeugeinheiten nötig. Die Verwendung der Werkstattkarte ist durch einen PIN-Code gesichert.
- Die Kontrollkarte wird an nationale Kontrollbehörden, gemäß §123a im [KFG], ausgegeben und dient dem Auslesen, Ausdrucken und/oder Herunterladen der im Massenspeicher gespeicherten Daten. Sie ermöglicht außerdem den Zugriff auf die Funktion straßenseitige Kalibrierungsüberprüfung sowie auf die Daten im Fernabfragegerät.

Eine notwendige Voraussetzung für die Ausgabe einer Fahrerkarte ist, dass ein Fahrer im Besitz maximal einer einzigen, gültigen Fahrerkarte sein darf.

1.2 Name und Kennzeichnung des Dokuments

Dieses Dokument ist die Austrian-Member State Authority Policy (A-MSA Policy), die von der A-MSA erstellt wurde. Diese A-MSA Policy hat keinen ASN.1 Object Identifier, da die Zertifikate des Digital Tachograph Systems keine Referenz auf diese A-MSA Policy beinhalten.

Version: 3.1.2, 07.05.2019

1.3 PKI Teilnehmende

Die nationale Gesamtverantwortung für das System der Kartenausgabe und die Umsetzung der [VO (EU) Nr. 165/2014] idgF in Österreich trägt die im Folgenden als A-MSA (Austrian-Member State Authority) bezeichnete Stelle. Offizieller Ansprechpartner ist:

Bundesministerium für Verkehr, Innovation und Technologie
IV/ST 5 Technisches Kraftfahrwesen

Radetzkystraße 2
1030 Wien
Österreich

Die A-MSA

1. ist zuständig für die Erstellung und Aktualisierung der A-MSA Policy und veranlasst deren Genehmigung durch die ERCA;

2. bestimmt die A-MSCA und gibt diese Entscheidung der Generaldirektion für Verkehr und Energie der Europäischen Union (DG TREN) bekannt;
3. bestimmt den A-CP;
4. überwacht die im Rahmen eines Gesetzes bzw. einer Verordnung ermächtigte A-CIA;
5. erstellt eine Richtlinie für das [A-CIA PS];
6. veranlasst Überprüfungen der A-MSCA, des A-CP und der A-CIA oder führt diese Überprüfungen selbst durch;
7. stellt sicher oder veranlasst, dass der A-MSCA, dem A-CP und der A-CIA in angemessener Zeit alle für ihre Tätigkeit benötigten Informationen in korrekter Weise zur Verfügung gestellt werden;
8. genehmigt die Practice Statements der A-MSCA, des A-CP und der A-CIA sowie ggf. das Practice Statement weiterer externer Dienstleister, sofern diese von A-MSCA und A-CP referenziert werden;
9. stellt die von der ERCA genehmigte A-MSA Policy den beteiligten Stellen zur Verfügung; das sind: A-MSCA, A-CP, A-CIA;
10. hält die zur ordnungsgemäßen Erfüllung ihrer Aufgabe notwendigen personellen und materiellen Ressourcen bereit, im speziellen um durch Haftungen verursachte Aufwendungen abzudecken;
11. Informiert die A-MSCA, den A-CP und die A-CIA über Schlüsselerzeugungen bei der ERCA.

Für die A-MSCA, die A-CIA und den A-CP gilt:

1. sie halten die zur ordnungsgemäßen Erfüllung ihrer Aufgaben notwendigen personellen und materiellen Ressourcen bereit, im speziellen um durch Haftungen verursachte Aufwendungen abzudecken;
2. sie weisen der A-MSA gegenüber die konkrete Umsetzung ihrer Verpflichtungen im laufenden Betrieb in geeigneter Weise nach;
3. sie gestatten der A-MSA oder einer von ihr beauftragten Stelle, die praktische Umsetzung ihrer Verpflichtungen zu überprüfen.

Werden von den genannten Organisationen externe Dienstleister zur Erbringung von Aufgaben, die in dieser A-MSA Policy festgelegt sind, verpflichtet, so gelten für sie dieselben Regelungen wie für die beauftragenden Organisationen. Die Verantwortung der beauftragenden Organisationen wird in keiner Weise eingeschränkt.

Folgende Kontaktadressen werden für sicherheitsrelevante Kommunikation verwendet:

Organisation	Mail-Adresse
A-MSA	st5@bmvit.gv.at
A-MSCA	a-msca@brz.gv.at
A-CP	digitaltacho@austriacard.at
A-CIA	tacho@asfinag.at

1.3.1 Zertifizierungsstellen (Certification Authorities, CAs)

Die Ausstellung der kryptographisch gesicherten Zertifikate erfolgt in der als A-MSCA (Austrian-Member State Certification Authority) bezeichneten Stelle. Im Fall der Bundesrechenzentrum GmbH (BRZ GmbH) ist das [KFG] die Grundlage für die Beauftragung.

Kontaktadresse der A-MSCA:

Bundesrechenzentrum GmbH

Hintere Zollamtstrasse 4
1030 Wien
Österreich

Die A-MSCA

1. erfüllt in ihrem Betrieb die Anforderungen dieser A-MSA Policy, die die Anforderungen der unter Abschnitt 1 Einleitung genannten Bestimmungen, aller hierfür relevanten Rechtsvorschriften und die Anforderungen der [ERCA Policy Gen 1] und [ERCA Policy Gen 2] beinhaltet;
2. erstellt das [A-MSCA PS], in dem mindestens die Art der Umsetzung dieser A-MSA Policy, der [ERCA Policy Gen 1], der [ERCA Policy Gen 2] und der gesetzlichen Regelungen erläutert wird, und lässt es von der A-MSA genehmigen;
3. stellt sicher, dass die von der A-CIA über das ZKR gesendeten Antragsdaten korrekt und entsprechend den Anforderungen empfangen werden, entsprechende Zertifikate erstellt werden und diese Zertifikate mit den entsprechenden privaten Schlüsseln über das ZKR an den A-CP übermittelt werden.

Die Bereitstellung, Personalisierung und Auslieferung der Karten erfolgt über die im Folgenden als A-CP (Austrian-Component Personalizer) bezeichnete Stelle. Die A-MSA beauftragt die AUSTRIA CARD Plastikkarten und Ausweissysteme Gesellschaft m.b.H. die Aufgaben des A-CP wahrzunehmen.

Kontaktadresse des A-CP:

AUSTRIA CARD Plastikkarten und Ausweissysteme Gesellschaft m.b.H.

Lamezanstraße 4-8
1230 Wien
Österreich

Der A-CP

1. erfüllt in seinem Betrieb die Anforderungen dieser A-MSA Policy, die die Anforderungen der unter Abschnitt 1 Einleitung genannten Bestimmungen, aller hierfür relevanten Rechtsvorschriften und die Anforderungen der [ERCA Policy Gen 1] und [ERCA Policy Gen 2] beinhaltet;
2. erstellt das [A-CP PS], das sich auf diese A-MSA Policy bezieht und von der A-MSA genehmigt werden muss;
3. stellt sicher, dass die PIN der Werkstattkarte nur an die Person ausgeliefert wird, für die die Werkstattkarte ausgestellt wurde.

1.3.2 Registrierungsstellen (Registration Authorities, RAs)

Die Beantragung von neuen Karten und alle Meldungen bezüglich des Kartenstatus (z.B. Diebstahl, Verlust, Defekt, etc.) erfolgen über die im Folgenden als A-CIA bezeichnete Stelle. Die Verwaltung sämtlicher Kartendaten und die Bereitstellung dieser für Auskünfte, liegt ebenfalls im Bereich der A-CIA. Das Bundesministerium für Verkehr, Innovation und Technologie (BMVIT) beauftragt die ASFINAG Maut Service GmbH (MSG), die Aufgaben der A-CIA für Werkstatt- und Kontrollkarten wahrzunehmen. Die A-CIA für Fahrer- und Unternehmenskarten sind die Autofahrerklubs ÖAMTC und ARBÖ, die vom BMVIT für diese Aufgaben beauftragt und ermächtig wurden. Das BMVIT übernimmt die behördlichen Aufgaben und das Monitoring des Kartenausgabesystems. Im Fall der Bundesrechenzentrum GmbH (BRZ GmbH) ist das [KFG] die Grundlage für die Beauftragung.

Kontaktadressen der A-CIA (Kartenantragstellen):

ASFINAG Maut Service GmbH

Alpenstraße 99
5020 Salzburg
Österreich

ARBÖ, Auto-, Motor- und Radfahrerbund Österreichs, Bundesorganisation
Johann-Böhm-Platz 1
1020 Wien
Österreich

Österreichischer Automobil-, Motorrad- und Touringclub (ÖAMTC)

Baumgasse 129
1030 Wien
Österreich

Bundesrechenzentrum GmbH (ZKR)

Hintere Zollamtstrasse 4
1030 Wien
Österreich

Die A-CIA ist in diesem Dokument als Überbegriff für die Funktionen und Aufgaben der Kartenantragstellung und des ZKR zu verstehen. Die A-CIA entscheidet, in welchem Umfang Funktionen und Aufgaben an Auftragnehmer weitergegeben werden. Dabei können auch einzelne Anforderungen dieser A-MSA Policy an die A-CIA eingeschränkt werden.

Abhängig von den überantworteten Aufgaben sind im [A-CIA PS] die Anforderungen, insbesondere alle Einschränkungen zur A-MSA Policy, dementsprechend getrennt auszuweisen.

Die A-CIA

1. erfüllt in ihrem Betrieb die Anforderungen dieser A-MSA Policy, die die Anforderungen der unter Abschnitt 1 Einleitung genannten Bestimmungen, aller hierfür relevanten Rechtsvorschriften und die Anforderungen der [ERCA Policy Gen 1] und [ERCA Policy Gen 2] beinhaltet;
2. stellt sicher, dass die Kontrollgerätekarten-/Fahrtenschreiberkartenantragsdaten korrekt an die A-MSCA geliefert werden, die von der A-MSCA erzeugten Zertifikate empfangen werden und die Daten für die Kartenpersonalisierung an den A-CP übertragen werden;
3. informiert in geeigneter Weise alle Kartenantragsteller über die Anforderung dieser A-MSA Policy;
4. prüft, ob alle Voraussetzungen für die Ausgabe einer Kontrollgerätekarte/Fahrtenschreiberkarte gegeben sind;
5. stellt sicher, dass alle relevanten Informationen und Bedingungen, sowie Teile des [A-CIA PS] den Kartenantragstellern zur Verfügung gestellt werden;
6. stellt sicher, dass die Kontrollgerätekarten/Fahrtenschreiberkarten den Kartenantragstellern zur Verfügung gestellt werden;
7. erfasst Daten zum Kartenstatus und stellt diese via TACHOnet allen Mitgliedsstaaten zur Verfügung.

1.3.3 Zertifikatsinhaber (Subscribers)

Die Zertifikatsinhaber werden in dieser A-MSA Policy auch als Kartenantragsteller, Karteninhaber oder Antragsteller bezeichnet. Kartenantragsteller können Fahrer-, Unternehmens-, Werkstatt- und Kontrollkarten beantragen (siehe auch Abschnitt 1.1 Überblick).

Der Kartenantragsteller ist verpflichtet die Bestimmungen des [KFG] einzuhalten. Insbesondere hat der Kartenantragsteller

1. wahrheitsgemäße und vollständige Angaben über die Antragsdaten zu machen;
2. bei der Antragstellung wahrheitsgemäße Angaben über vorhandene Kontrollgerätekarten/Fahrtenschreiberkarten und Kontrollgerätekarten-/Fahrtenschreiberkartenarten zu machen;
3. auf geeignete Weise sicherzustellen, dass seine Kontrollgerätekarte/Fahrtenschreiberkarte nur für den vorgesehenen Zweck benutzt wird und Missbrauch, insbesondere durch Dritte, verhindert wird;
4. beschädigte und abgelaufene Kontrollgerätekarten/Fahrtenschreiberkarten nicht zu verwenden;
5. die Annahme des PIN-Kuverts der Werkstattkarte zu verweigern, wenn der Sicherheitsschutz der PIN bei der Übernahme verletzt ist;
6. Verlust, Diebstahl, Beschädigung oder Missbrauch der Kontrollgerätekarte/Fahrtenschreiberkarte der zuständigen Stelle zu melden.

1.3.4 Vertrauende Parteien (Relying Parties)

Bei vertrauenden Parteien handelt es sich um alle Bürger, Unternehmen, und sonstige Organisationen der am Digital Tachograph System beteiligten Nationen.

1.3.5 Andere Parteien

Keine Angaben.

1.4 Schlüssel- und Zertifikatsnutzung

1.4.1 Zulässige Verwendung

Die Schlüssel und Zertifikate der A-MSCA werden ausschließlich ihrem Zweck und den Vorgaben aus [ERCA Policy Gen 2], Kapitel 1.4, entsprechend verwendet.

Die A-MSCA verwendet ihre privaten MSCA Schlüssel (MS.SK, MSCA_Card.SK) ausschließlich zum:

- Signieren von Zertifikaten für Kontrollgerätekarten/Fahrtenschreiberkarten entsprechend Vorgabe aus [Annex 1B] und [Annex 1C]
- Signieren von MSCA Zertifikatsrequests (MS.CSR, MSCA_Card.CSR)

Die von der A-MSCA ausgestellten Zertifikate und die ausgelieferten geheimen Schlüssel dürfen ihrem Verwendungszweck entsprechend ausschließlich in Kontrollgerätekarten/Fahrtenschreiberkarten und Kontrollgeräten/Fahrtenschreibern innerhalb des Digital Tachograph Systems eingebracht und eingesetzt werden. Die A-MSA stellt dies durch geeignete Überwachungs- und Zwangsmaßnahmen sicher.

Ausgenommen von dieser Regelung sind Zertifikate und Schlüssel, welche zur Überprüfung der korrekten Funktionsweise des Systems ausgestellt werden. Diese Testkarten werden über einen eigenen getrennten Nummernkreis gekennzeichnet und dürfen ausschließlich ihrem Zweck entsprechend eingesetzt werden.

Die Gültigkeitsdauer der von der A-MSCA ausgestellten Kontrollgerätekarten-/Fahrtenschreiberkartenzertifikate für sowohl Generation 1 (EQT.C) als auch Generation 2 (Card_MA.C und Card_Sign.C) des Digital Tachograph Systems darf die maximale Verwendungsdauer der zugehörigen Kontrollgerätekarten/Fahrtenschreiberkarten nicht überschreiten.

Maximale Gültigkeit der einzelnen Zertifikate je Kartentyp gerechnet vom Zeitpunkt des Beginns der Gültigkeit der jeweiligen Kontrollgerätekarte/Fahrtenschreiberkarte:

Kartentyp	EQT.C	Card_MA.C	Card_Sign.C
Fahrerkarte	5 Jahre	5 Jahre	5[1] Jahre
Unternehmenskarte	5 Jahre	5 Jahre	-
Kontrollkarte	2 Jahre	2 Jahre	-
Werkstattkarte	1 Jahr	1 Jahr	1[1] Jahr

1.4.2 Nicht zulässige Verwendung

Kontrollgerätekarten/Fahrtenschreiberkarten, Schlüssel und Zertifikate sind nur zur Verwendung innerhalb des Digital Tachograph Systems zugelassen. Jede Veränderung der Kontrollgerätekarte/Fahrtenschreiberkarte (z.B. Aufbringen von zusätzlichen Schlüsseln, Zertifikaten oder anderen Daten) ist nicht zulässig. Zertifikate dürfen nach Ablauf der Gültigkeit nicht mehr verwendet werden.

A-MSA und A-MSCA stellen im Rahmen ihrer jeweiligen Zuständigkeiten und der jeweils geltenden Rechtsvorschriften sicher, dass die von der A-MSCA erstellten Zertifikate und Schlüssel nur im Sinne der unter Abschnitt 1 Einleitung genannten Bestimmungen eingesetzt werden.

1.5 Verwaltung der A-MSA Policy

1.5.1 Verantwortliche Organisation

Diese A-MSA Policy wird durch die A-MSA verwaltet.

1.5.2 Ansprechpartner

Ansprechpartner für die Policy ist die A-MSA (siehe Abschnitt 1.3 PKI Teilnehmende)

1.5.3 Zuständigkeit für die Eignung des A-MSCA PS, des A-CP PS und des A-CIA PS

Das [A-MSCA PS], das [A-CP PS] und das [A-CIA PS] müssen die Vorgaben dieser A-MSA Policy, von [ERCA Policy Gen 1] und [ERCA Policy Gen 2] berücksichtigen. Die Überprüfung der Einhaltung dieser Vorgaben obliegt der A-MSA, welche die Überprüfung direkt durchführen oder entsprechend qualifizierte Dritte dafür beauftragen kann.

1.5.4 Genehmigungsverfahren der A-MSA Policy

Diese A-MSA Policy wird von der A-MSA bei der ERCA zur Genehmigung vorgelegt.

1.6 Abkürzungen und Referenzen

1.6.1 Abkürzungen

Abkürzung	Definition
AES	Advanced Encryption Standard
A-CIA	Austrian-Card Issuing Authority

[1] Ein Daten-Download ist bis 1 Monat nach dem Gültigkeitsablauf der Karte möglich

A-CIA PS	A-CIA Practice Statement
A-CP	Austrian-Component Personalizer
A-CP PS	A-CP Practice Statement
A-MSA	Austrian-Member State Authority
A-MSCA	Austrian-Member State Certification Authority
A-MSCA PS	A-MSCA Practice Statement
BMVIT	Bundesministerium für Verkehr, Innovation und Technologie
BRZ	Bundesrechenzentrum GmbH
Card_MA.C	Equipment Certificate für Mutual Authentication (Generation 2)
Card_MA.KP	Equipment Key Pair für Mutual Authentication (Generation 2)
Card_MA.PK	Equipment Public Key für Mutual Authentication (Generation 2)
Card_MA.SK	Equipment Secret Key für Mutual Authentication (Generation 2)
Card_Sign.C	Equipment Certificate zum Signieren von Daten (Generation 2)
Card_Sign.KP	Equipment Key Pair zum Signieren von Daten (Generation 2)
Card_Sign.PK	Equipment Public Key zum Signieren von Daten (Generation 2)
Card_Sign.SK	Equipment Secret Key zum Signieren von Daten (Generation 2)
DG TREN	Generaldirektion für Verkehr und Energie der Europäischen Union
DSRC	Dedicated Short Range Communication
ECC	Elliptic Curve Cryptography
EG	Europäische Gemeinschaft
EQT	Equipment
EQT.C	Equipment Certificate (Generation 1)
EQT.KP	Equipment Key Pair (Generation 1)
EQT.PK	Equipment Public Key (Generation 1)
EQT.SK	Equipment Secret Key (Generation 1)
ERCA	European Root Certification Authority

EU	Europäische Union
EUR.C	ERCA Certificate (Generation 2)
EUR.LC	ERCA Link Certificate (Generation 2)
EUR.PK	ERCA Public Key (Generation 1)
EWG	Europäische Wirtschaftsgemeinschaft
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
IPRG	Internationales Privatrechtsgesetz
ISMS	Information Security Management System
ISO	International Standardization Organization
KDM	Key Distribution Message
KDR	Key Distribution Request
KFG	Kraftfahrgesetz
KM	Key Manager
KonGV	Kontrollgerätekartenverordnung
$K_{M\text{-}DSRC}$	DSRC Master Key – AES Schlüssel (Generation 2)
$K_{M\text{-}WC}$	Motion Sensor Master Key Workshop Card – AES Schlüssel (Generation 2)
Km_{WC}	Motion Sensor Master Key Workshop Card – TDES Schlüssel (Generation 1)
MS	Member State
MS.C	MSCA Certificate (Generation 1)
MS.CSR	MSCA Certificate Signing Request (Generation 1)
MS.KP	MSCA Key Pair (Generation 1)
MS.PK	MSCA Public Key (Generation 1)
MS.SK	MSCA Secret Key (Generation 1)
MSCA	Member State Certification Authorithy
MSCA.KT	MSCA Transport Key
MSCA_Card.C	MSCA Certificate (Generation 2)
MSCA_Card.CSR	MSCA Certificate Signing Request (Generation 2)

MSCA_Card.KP	MSCA Key Pair (Generation 2)
MSCA_Card.PK	MSCA Public Key (Generation 2)
MSCA_Card.SK	MSCA Secret Key (Generation 2)
OCSP	Online Certificate Status Protocol
PCI	Payment Card Industry
PIN	Persönliche Identifikationsnummer
PKI	Public Key Infrastructure
PRZ	Parallelrechenzentrum (des BRZ)
RFC	Request For Comment
RSA	Rivest Shamir Adleman
SPG	Sicherheitspolizeigesetz
SSO	System Security Officer
SW	Software
TACHOnet	Das TACHOnet ist ein EU-weites System, das einen automatisierten Informationsaustausch zwischen den Mitgliedstaaten des Digital Tachograph Systems ermöglicht.
TDES / 3DES	Triple Data Encryption Standard
ZKR	Zentrales Kartenregister

1.6.2 Referenzen

Referenz	Dokument
Annex 1B	Anhang 1B der Verordnung (EWG) Nr. 1360/2002
Annex 1C	Anhang 1C der Durchführungsverordnung (EU) Nr. 2016/799
A-CIA PS	Austrian-Card Issuing Authority Practice Statement in der gültigen Fassung
A-CP PS	Austrian-Component Personalizer Practice Statement in der gültigen Fassung
A-MSCA PS	Austrian-Member State Certification Authority Practice Statement in der gültigen Fassung
DSG	Österreichisches Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999
ERCA Policy Gen 1	Digital Tachograph System - European Root Policy Version 2.1

ERCA Policy Gen 2	Smart Tachograph - European Root Certificate Policy and Symmetric Key Infrastructure Policy Version 1.0
FIPS 140-2	Federal Information Processing Standard 140-2
ISO 27001	International Standardization Organization 27001
ISO/IEC 15408	ISO/IEC 15408
ISO/IEC 19790	ISO/IEC 19790
KFG	Kraftfahrgesetz 1967 in der gültigen Fassung
KonGV	Kontrollgerätekartenverordnung in der gültigen Fassung
Richtlinie 2006/22 (EG)	Richtlinie 2006/22 (EG)
VO (EG) Nr. 561/2006	Verordnung (EG) Nr. 561/2006
VO (EG) Nr. 1360/2002	Verordnung (EG) Nr. 1360/2002
VO (EU) Nr. 165/2014	Verordnung (EU) Nr. 165/2014
VO (EU) Nr. 2016/679	Verordnung (EU) Nr. 2016/679
VO (EU) Nr. 2016/799	Durchführungsverordnung (EU) Nr. 2016/799
VO (EU) Nr. 2018/502	Durchführungsverordnung (EU) Nr. 2018/502

2 Veröffentlichungen und Informationsdienste

2.1 Informationsdienste

Diese A-MSA Policy und weitere Informationen zum Digital Tachograph System in Österreich sind unter http://www.digitaltacho.at/ veröffentlicht. Die Practice Statements [A-MSCA PS] und [A-CP PS] werden nicht öffentlich zur Verfügung gestellt.

Fragen betreffend dieser A-MSA Policy sind an die Adresse der A-MSA zu richten (siehe Abschnitt 1.3 PKI Teilnehmende)

2.2 Veröffentlichung von Informationen zu Zertifikaten und Kontrollgerätekarten/Fahrtenschreiberkarten

Informationen zu den A-MSCA Zertifikaten werden auf der Webseite des JRC (https://dtc.jrc.ec.europa.eu/) veröffentlicht.

Zertifikatsinformationen (und Statusinformationen über Kontrollgerätekarten/Fahrtenschreiberkarten) können über das ZKR und das TACHOnet abgefragt werden.

Diese Informationen zu den Zertifikaten der Kontrollgerätekarten werden nicht öffentlich zur Verfügung gestellt. Es sind auch keine CRLs und OCSP Responder vorgesehen.

2.3 Häufigkeit der Aktualisierung von Informationen

Öffentliche Informationen werden bei Bedarf aktualisiert. Für die Veröffentlichung dieser A-MSA Policy wird das Vorgehen unter Abschnitt 9.12 Änderungen der A-MSA Policy herangezogen.

2.4 Zugriffskontrolle der Informationsdienste

Die Webseiten http://www.digitaltacho.at/ und https://dtc.jrc.ec.europa.eu/ sind öffentlich verfügbar. Für die über die Website verfügbaren Informationen ist ausschließlich Lesezugriff zulässig. Alle auf der Webseite http://www.digitaltacho.at/ veröffentlichten Informationen müssen über eine sichere Verbindung verfügbar sein.

Der Zugriff auf das ZKR ist auf die A-CIA eingeschränkt. Zusätzlich bestehen Leserechte für Kontrollorgane.

3 Identifizierung und Authentifizierung

3.1 Namensregeln

Zertifikate und Zertifikatsrequests des Digital Tachograph Systems werden anhand der Certification Authority Reference (CAR) und der Certificate Holder Reference (CHR) identifiziert. Der Aufbau der Zertifikate entspricht den Vorgaben von [Annex 1C], Appendix 11, CSM_017 und CSM_136:

Entität	Identifikator	Aufbau CAR	Aufbau CHR
MSCA	Certification Authority Key Identifier (KID)	Nation numeric (‘1’) Nation alpha (EC) Key serial number Additional info CA identifier (‘01’)	Nation numeric (‘1’) Nation alpha (A) Key serial number Additional info[2] CA identifier (‘01’)
EQT	Certification Authority Key Identifier (KID)	Nation numeric (‘1’) Nation alpha (A) Key serial number Additional info CA identifier (‘01’)	Equipment serial number Date Type[3] Manufacturer(‘12’)

[2] Enthält den Wert des aktuell verwendeten MSCA Schlüssels (‘00 0A’ („A“) oder ‘00 0B’ („B“) für das Ersatzschlüsselpaar)
[3] Der Wert des Feldes `Type` wird entsprechend [Annex 1C], Appendix 11, CSM_017, Punkt 5.1 je Kartentyp gesetzt (Fahrerkarte ‘01’, Werkstattkarte ‘02’, Kontrollkarte ‘03’, Unternehmenskarte ‘04’)

Key Distribution Requests (KDRs) und Key Distribution Messages (KDMs) werden den Vorgaben der [ERCA Policy Gen 1], Annex D und [ERCA Policy Gen 2], 3.1.1.2 entsprechend identifiziert.

Zertifikate, Zertifikatsrequests, KDRS und KDMs, welche für den Interoperbilitätstest verwendet werden, werden entsprechend Vorgabe der [ERCA Policy Gen 2] mit dem Wert '54 4B' („TK") im Feld `additionalInfo` und einem eigenen getrennten Nummernkreis gekennzeichnet.

3.2 Identitätsprüfung bei Neuanträgen

Die Identitätsprüfung von Neuanträgen erfolgt durch die Kartenantragsstellen der A-CIA.

Die bei der Antragsstellung durchgeführten Überprüfungen sind im [KFG] festgeschrieben und werden im [A-CIA PS] definiert.

3.3 Identifikation und Authentisierung bei Schlüsselerneuerungen

Schlüsselerneuerung wird nicht unterstützt. Soll eine neue Kontrollgerätekarte/Fahrtenschreiberkarte verwendet werden, ist ein Neuantrag zu stellen.

3.4 Identifikation und Authentisierung von Widerrufsanträgen

Ein technischer Widerruf der Zertifikate der Kontrollgerätekarten/Fahrtenschreiberkarten ist nicht vorgesehen. Das Vorgehen (und die Identifikation) bei defekten, verlorenen und gestohlenen Kontrollgerätekarten/Fahrtenschreiberkarten ist im [KFG] geregelt.

Fallen Voraussetzungen bei der Beantragung nachträglich weg, muss die Kontrollgerätekarte/Fahrtenschreiberkarte unverzüglich vom Kartenantragsteller zurückgegeben werden.

4 Anforderungen an den Betriebsablauf

4.1 Anforderungen an den Betriebsablauf für Kontrollgerätekarten-/Fahrtenschreiberkartenzertifikate

Dieses Kapitel beschreibt den Betriebsablauf des kompletten Zertifikatslebenszyklus von Zertifikaten von Kontrollgerätekarten/Fahrtenschreiberkarten.

Überblick des gesamten Kartenbeantragungsprozesses:

1. Die Kartenbeantragung erfolgt bei einer Kartenantragsstelle (A-CIA).
2. Die Antragsstelle überprüft die Identität und Berechtigung des Kartenantragstellers.
3. Die Kartenantragsdaten werden im zentralen Kartenregister (ZKR) erfasst.
4. Das ZKR beantragt bei der A-MSCA die Schlüssel und Zertifikate für die Kontrollgerätekarte/Fahrtenschreiberkarte.
5. Die A-MSCA generiert die Schlüssel und Zertifikate für die Kontrollgerätekarte/Fahrtenschreiberkarte und retourniert diese an das ZKR.
6. Das ZKR schickt eine Produktionsdatei mit den Kartenantragsdaten an den A-CP.
7. Der A-CP erstellt die Kontrollgerätekarte/Fahrtenschreiberkarte und bringt alle für die Personalisierung vorgesehenen Daten auf.
8. Der A-CP verschickt die fertige Kontrollgerätekarte/Fahrtenschreiberkarte an den Kartenantragsteller.

4.1.1 Antragstellung

Die A-CIA gewährleistet die Einhaltung des von der A-MSA definierten Antragsverfahrens für Kontrollgerätekarten/Fahrtenschreiberkarten.

Die A-CIA stellt innerhalb ihres Einflussbereichs sicher, dass die Ausstellung von Ersatzkarten und die Kontrollgerätekarten-/Fahrtenschreiberkartenerneuerung nur unter den in Abschnitt 1 Einleitung genannten Bestimmungen erfolgt und dass die dafür vorgeschriebenen Fristen eingehalten werden können.

Die A-CIA informiert den Kartenantragsteller über die Nutzungsbedingungen der Kontrollgerätekarte/Fahrtenschreiberkarte. Die Information hat in leicht verständlicher Form zu erfolgen.

Der Kartenantragsteller akzeptiert durch seinen Kontrollgerätekarten-/Fahrtenschreiberkartenantrag die Benutzungsbedingungen.

Die bei der Antragsstellung erforderlichen Überprüfungen sind im [KFG] festgeschrieben und werden im [A-CIA PS] definiert.

Der Kartenantragsteller ist vertraglich oder per Gesetz verpflichtet folgende Punkte zu erfüllen:

- der Kartenantragsteller stimmt den Bedingungen betreffend dem Gebrauch der Karte zu
- der Kartenantragsteller stimmt zu, und bestätigt, dass ab dem Zeitpunkt der Kartenannahme für den gesamten Gültigkeitszeitraum der Karte, und solange er der A-CIA nichts gegenteiliges mitteilt:
    - keine unautorisierte Person jemals Zugriff auf die Karte hat
    - alle für den Karteninhalt relevanten Informationen, die der A-CIA vom Benutzer mitgeteilt werden, wahrheitsgetreu sind
    - die Karte gewissenhaft in Übereinstimmung mit den Gebrauchsbeschränkungen (siehe Abschnitt 1.4 Schlüssel- und Zertifikatsnutzung) benutzt wird

Die Voraussetzungen zur Ausstellung einer Kontrollgerätekarte/Fahrtenschreiberkarte sind im [KFG] und in der [KonGV] geregelt.

4.1.2 Bearbeitung von Anträgen

Die genehmigten Kartenanträge werden im ZKR erfasst.

Die A-CIA stellt innerhalb ihres Einflussbereichs sicher, dass vor der Ausstellung eines Zertifikats eine ordnungsgemäße Registrierung in den dafür zuständigen Kartenantragstellen stattgefunden hat.

Insbesondere stellt die A-CIA dabei sicher, dass die Registrierungsdaten eine eindeutige Zuweisung der Certificate Holder Reference nach Anforderung von [Annex 1C], CSM_017 und CSM_136 ermöglicht.

4.1.3 Ausstellung von Zertifikaten und Kontrollgerätekarten/Fahrtenschreiberkarten

Die A-MSCA erstellt Zertifikate nur dann, wenn ein ordnungsgemäßer Zertifikatsantrag einer dafür bevollmächtigten Kartenantragstelle (A-CIA) vorliegt und wenn bei der Antragstellung alle Anforderungen der unter Abschnitt 1 Einleitung genannten Bestimmungen und aller damit zusammenhängender Rechtsvorschriften und Vereinbarungen eingehalten worden sind. Bei einem automatisierten Verfahren ist eine Zertifikatserstellung durch manuellen Eingriff in das Digital Tachograph System auszuschließen.

Zur Überprüfung der korrekten Funktionsweise des Digital Tachograph Systems können zusätzliche Zertifikate erstellt werden, die nicht auf Kontrollgerätekarten/Fahrtenschreiberkarten aufgebracht werden und daher auch nicht im ZKR registriert sind. Diese Zertifikate müssen über einen eigenen getrennten Nummernkreis gekennzeichnet werden.

Alle zertifizierten öffentlichen Schlüssel werden von der A-MSCA archiviert.

Organisationen (Sublieferanten, Dienstleister), die neben dem Mitgliedsstaat Österreich auch im Namen anderer Mitgliedsstaaten die Schlüsselerzeugung und Kartenpersonalisierung durchführen, müssen dies in einem klar unterscheidbaren Prozess für jeden Mitgliedstaat machen. Jeder Prozess für einen Mitgliedsstaat muss separat protokolliert werden und die zuständige MSA muss auf Anfrage Zugriff auf diese Protokolle erhalten.

Schlüsselerzeugung und Zertifikatsausstellung

Bei der Ausstellung der Zertifikate werden die unter Abschnitt 1 Einleitung genannten Anforderungen, insbesondere den Aufbau der Zertifikate, die Anwendung des Signaturalgorithmus und des Hashalgorithmus betreffend, eingehalten.

Die A-MSA, die A-MSCA und der A-CP stellen innerhalb ihres Einflussbereiches sicher, dass die Erzeugung der Schlüssel in einer besonders abgesicherten Produktionsumgebung erfolgt, die insbesondere die Geheimhaltung der jeweiligen privaten Schlüssel (EQT.SK, Card_MA.SK und Card_Sign.SK) gewährleistet. Die Signatur der Kontrollgerätekarten-/Fahrtenschreiberkartenzertifikate (EQT.C, Card_MA.C und Card_Sign.C) wird auf jenem HSM durchgeführt, auf dem auch die MSCA- und EQT-Schlüssel erzeugt und gespeichert werden. Somit gelten für die dabei einzusetzenden Geräte die gleichen Anforderungen wie für die zur Erzeugung der Schlüsselpaare der A-MSCA eingesetzten Geräte (siehe Abschnitt 6.2 Anforderung zum Schutz privater und geheimer Schlüssel und für den Einsatz kryptographischer Module).

Die A-MSA, die A-MSCA und der A-CP stellen innerhalb ihres Einflussbereiches sicher, dass die privaten Schlüssel (EQT.SK, Card_MA.SK und Card_Sign.SK) nach Bearbeitung eines Kartenantrags (A-MSCA) und nach der Einbringung in die jeweilige Kontrollgerätekarte (A-CP) dauerhaft aus den Speichern der Schlüsselerzeugungs- und Personalisierungssysteme gelöscht wird. Bei der A-MSCA geschieht das unmittelbar nach der Bearbeitung des Kartenantrags, beim ZKR wird die Produktionsdatei mit den verschlüsselten privaten Schlüsseln betriebsbedingt automatisch nach 14 Tagen gelöscht und beim A-CP wird die Produktionsdatei mit den verschlüsselten privaten Schlüsseln betriebsbedingt spätestens nach 30 Tagen automatisch gelöscht.

Ein Backup der privaten MSCA-Schüssel (MS.SK und MSCA_Card.SK) durch die A-MSCA ist hingegen zulässig.

Die A-MSCA stellt sicher, dass innerhalb ihres Verantwortungsbereiches das Auftreten von Schlüsselduplikaten mit hoher Wahrscheinlichkeit ausgeschlossen ist.

Die A-MSCA übergibt alle benötigten Schlüssel- und Zertifikatsdaten an das ZKR, sodass Schlüssel, Zertifikate, Kontrollgerätekarten/Fahrtenschreiberkarten und Kartenantragsteller miteinander verknüpft werden.

Die A-MSCA verweigert die Auslieferung von Schlüsseln und Zertifikaten, wenn die Gefahr eines Missbrauchs von Schlüsseln und/oder Zertifikaten vorliegt. Die weitere Vorgangsweise liegt in der Verantwortung der A-MSA.

Personalisierung

Die Karten werden entsprechend den unter Abschnitt 1 Einleitung genannten Bestimmungen optisch personalisiert.

Die Daten werden abhängig vom Kartentyp und entsprechend der Struktur spezifiziert in den unter Abschnitt 1 Einleitung genannten Bestimmungen im speziellen des [Annex 1C], TCS_150 und TCS_154, TCS_158 und TCS_162, TCS_166 und TCS_170, und TCS_174 und TCS_178 in den Chip der Karte eingebracht.

Die Schlüssel und Zertifikate werden bei der A-MSCA generiert, gesichert zum A-CP übertragen und vom A-CP auf die Kontrollgerätekarten/Fahrtenschreiberkarten aufgebracht.

Alle sicherheitskritischen Personalisierungsdaten werden in verschlüsselter Form in der Produktionsdatenbank abgelegt. Dies gilt insbesondere für die in den Auftragsdaten übergebenen privaten Schlüssel. Diese Schlüsseldaten dürfen nur zum Zeitpunkt des „Umschlüsselns" innerhalb des HSM kurzzeitig im Klartext vorliegen und müssen danach sofort wieder vollständig gelöscht werden. Die Produktionsdatei mit den Personalisierungsdaten wird nach spätestens 30 Tagen nach Abarbeitung des Personalisierungsrequests automatisch gelöscht.

Die Gültigkeit der Kartenzertifikate (EQT.C, Card_MA.C und Card_Sign.C) entspricht der Gültigkeit der zugehörigen Kontrollgerätekarte/Fahrtenschreiberkarte.

Die Kartenzertifikate EQT.C und Card_MA.C und Kartenschlüssel EQT.SK und Card_MA.SK werden auf alle vier Kartentypen aufgebracht, das Kartenzertifikat Card_Sign.C und der Kartenschlüssel Card_Sign.SK werden auf die Fahrer- und die Werkstattkarte aufgebracht.

Der A-CP stellt sicher, dass die im Zuge der Personalisierung auf die Kontrollgerätekarten/Fahrtenschreiberkarten aufgebrachten visuellen und elektronischen Daten übereinstimmen. Die dabei stattfindenden Vorgänge sind vom A-CP zu beschreiben.

Der A-CP stellt sicher, dass auf den Kontrollgerätekarten/Fahrtenschreiberkarten der öffentliche Schlüssel der ERCA (EUR.PK), die erforderlichen Zertifikate der ERCA (EUR.C und EUR.LC) und die Zertifikate der A-MSCA (MS.C und MSCA_Card.C) entsprechend den unter Abschnitt 1 Einleitung genannten Bestimmungen aufgebracht werden.

Die Motion Sensor Master Keys für Werkstattkarten (Km_{WC} und $K_{M\text{-}WC}$) werden auf die Werkstattkarte, der DSRC Master Key ($K_{M\text{-}DSRC}$) auf die Kontroll- und die Werkstattkarte aufgebracht.

Der A-CP stellt sicher, dass Werkstattkarten mit einer PIN gemäß den Vorgaben der unter Abschnitt 1 Einleitung genannten Bestimmungen ausgestattet werden. Eine PIN muss aus mindestens 6 Ziffern bestehen.

Die Generierung der PIN erfolgt beim A-CP in einem abgesicherten System, das verhindert, dass nachträglich eine Zuordnung von PIN und Werkstattkarte erfolgen kann. Die PIN wird nach ihrer Generierung gesichert an die Adresse der Werkstatt - persönlich an die geeignete Person der jeweiligen Werkstattkarte - ausgeliefert.

Das zur PIN-Erzeugung benutzte IT-System muss zumindest die Anforderungen von [FIPS 140-2], Level 3, oder nachweislich durch andere Maßnahmen eine gleichwertige Sicherheit gewährleisten.

Die Übermittlung der gesicherten PIN muss getrennt von den personalisierten Karten erfolgen.

Die Rekonstruktion des PIN ist auszuschließen.

Der A-CP muss gewährleisten, dass die privaten Schlüssel (EQT.SK, Card_MA.SK und Card_Sign.SK) durch eine Kontrollgerätekarte/Fahrtenschreiberkarte geschützt, und auf diese beschränkt ist, die dem Benutzer auf einem Weg zugeschickt wurde, wie es durch diese A-MSA Policy vorgeschrieben ist.

Kopien des privaten Schlüssel (EQT.SK, Card_MA.SK und Card_Sign.SK) dürfen nur während der Schlüsselerzeugung und Kartenpersonalisierung außerhalb der Kontrollgerätekarte/Fahrtenschreiberkarte nur in einem HSM im Klartext gespeichert sein.

Die privaten Kartenschlüssel sind am Transportweg von der A-MSCA zum A-CP durch Verschlüsselung zu schützen.

Die A-MSA, die A-MSCA und der A-CP stellen innerhalb ihres Einflussbereichs sicher, dass die jeweiligen privaten Schlüssel ausschließlich gemäß der in den unter Abschnitt 1 Einleitung genannten Bestimmungen genutzt werden können. Dies schließt insbesondere ein, dass nach Beendigung des Personalisierungsvorgangs keine Kopien dieser Schlüssel außerhalb der gesicherten Umgebungen der Kontrollgerätekarten/Fahrtenschreiberkarten und Kontrollgeräte/Fahrtenschreiber existieren.

Der A-CP stellt innerhalb seines Einflussbereichs sicher, dass nur solche Kontrollgerätekarten/Fahrtenschreiberkarten ausgeliefert werden, bei denen optische und elektronische Personalisierungsdaten übereinstimmen.

Fehlpersonalisierte und andere ungültige Kontrollgerätekarten/Fahrtenschreiberkarten aus der Produktion sind unter Aufsicht und in der Verantwortung des A-CP zu vernichten. Die Vernichtung jeder Karte ist zu dokumentieren.

Defekte, entzogene, zurückgegebene und andere ungültige Kontrollgerätekarten/Fahrtenschreiberkarten sind unter Aufsicht und in der Verantwortung der A-CIA zu vernichten oder an den ausstellenden Mitgliedstaat zu übermitteln. Die Vernichtung jeder Karte ist zu dokumentieren.

4.1.4 Annahme von Zertifikaten und Kontrollgerätekarten/Fahrtenschreiberkarten

Die A-CIA trägt im ZKR die relevanten Daten ein, damit nachvollzogen werden kann, welche Kontrollgerätekarte/Fahrtenschreiberkarte an welchen Kartenantragsteller versendet wurde.

Die A-MSA stellt sicher, dass personalisierte Kontrollgerätekarten/Fahrtenschreiberkarten innerhalb der durch die unter Abschnitt 1 Einleitung genannten Bestimmungen vorgegebenen Fristen sicher an die Kartenantragsteller verschickt werden. Voraussetzung für die Ausstellung einer mit Lichtbild und Unterschrift personalisierten Kontrollgerätekarte/Fahrtenschreiberkarte an einen Kartenantragsteller ist, dass dieser bei der Antragstellung persönlich identifiziert wurde. Sofern Kontrollgerätekarten/Fahrtenschreiberkarten nicht auf eine natürliche Person ausgestellt werden, muss der Kartenantragsteller und der Empfänger der Kontrollgerätekarten/Fahrtenschreiberkarten eine ausreichende Legitimation nachweisen können.

Der Zeitpunkt der Personalisierung muss so geplant werden, dass die Zeitspanne für die erforderliche sichere Aufbewahrung der personalisierten Karte, bis zur Auslieferung zum Kartenantragsteller auf ein Minimum reduziert wird.

Personalisierte Karten müssen sofort zu einem überwachten Auslieferungsbereich gebracht werden. Lagerung über Nacht erfordert sichere Verwahrung. Es müssen dokumentierte Prozesse für die Behandlung von Fehlersituationen, einschließlich Störungen im Produktionsprozess, nicht erfolgte Zustellung und Verlust von Karten oder Beschädigung von Karten, bestehen.

Personalisierte Karten müssen getrennt von nicht personalisierten Karten aufbewahrt werden.

Die Kontrollgerätekarte/Fahrtenschreiberkarte muss so verteilt werden, dass die Gefahr des Verlustes auf ein Minimum reduziert wird.

Ist bei der Übernahme einer Werkstattkarte der Sicherheitsschutz der PIN verletzt, so hat der Kartenantragsteller die Annahme zu verweigern. In diesem Fall ist die Karte an die zuständige A-CIA zu retournieren. Dieser Umstand ist eine ausreichende Begründung für die Ausstellung einer Ersatzkarte im Sinne der unter Abschnitt 1 Einleitung genannten Bestimmungen.

4.1.5 Verwendung des privaten Schlüssels und des Zertifikats der Kontrollgerätekarte/Fahrtenschreiberkarte

Die zulässige und nicht zulässige Verwendung ist unter Abschnitt 1.4 Schlüssel- und Zertifikatsnutzung definiert. Die korrekte Verwendung von Kontrollgerätekarten/Fahrtenschreiberkarten mit den jeweiligen Kontrollgeräten/Fahrtenschreibern ist in den Benutzerhandbüchern der Kontrollgeräte/Fahrtenschreiber-Hersteller beschrieben.

4.1.6 Erneuerung von Zertifikaten und Kontrollgerätekarten/Fahrtenschreiberkarten

Eine Erneuerung von Zertifikaten ist nicht vorgesehen. Die Bedingungen zur Erneuerung einer Kontrollgerätekarte/Fahrtenschreiberkarte und zum Ersatz von verlorenen, gestohlenen, beschädigten oder fehlerhaften Kontrollgerätekarten/Fahrtenschreiberkarten sind im [KFG] festgelegt.

4.1.7 Erneuerung von Schlüsseln und Kontrollgerätekarten/Fahrtenschreiberkarten

Eine Erneuerung von Schlüsseln ist nicht vorgesehen. Die Bedingungen zur Erneuerung einer Kontrollgerätekarte/Fahrtenschreiberkarte und zum Ersatz von verlorenen, gestohlenen, beschädigten oder fehlerhaften Kontrollgerätekarten/Fahrtenschreiberkarten sind im [KFG] festgelegt.

4.1.8 Änderung von Zertifikaten und Kontrollgerätekarten/Fahrtenschreiberkarten

Eine Änderung von Zertifikaten ist nicht vorgesehen. Die Bedingungen zu Änderung und Austausch einer Kontrollgerätekarte/Fahrtenschreiberkarte sind im [KFG] festgelegt.

4.1.9 Widerruf und Sperrung von Zertifikaten und Kontrollgerätekarten/Fahrtenschreiberkarten

Zertifikate von Kontrollgerätekarten/Fahrtenschreiberkarten werden nicht technisch widerrufen oder gesperrt. Stattdessen werden Kontrollgerätekarten/Fahrtenschreiberkarten von den Kartenantragstellern an die zuständigen Stellen zurückgegeben. Der Rückgabeprozess ist im [A-CIA PS] definiert.

Ist die Ausstellung der Fahrerkarte erfolgt, ohne dass die Voraussetzungen für die Antragstellung vorliegen, oder ist eine der Voraussetzungen nachträglich nicht mehr erfüllt, ist die Fahrerkarte unverzüglich an die A-CIA abzuliefern und dem Bundesminister für Verkehr, Innovation und Technologie zu übermitteln.

Ist die Ausstellung der Werkstattkarte erfolgt, ohne dass die Voraussetzungen für die Antragstellung vorliegen, oder ist eine der Voraussetzungen nachträglich nicht mehr erfüllt, ist die Werkstattkarte unverzüglich vom Landeshauptmann oder der Landeshauptfrau einzuziehen und dem Bundesminister für Verkehr, Innovation und Technologie zu übermitteln.

Die einziehende Stelle hat die Kontrollgerätekarte/Fahrtenschreiberkarte durch Zerstörung des Chips (z.B. Lochung des Chips) zu deaktivieren.

Für die Unternehmenskarte und Kontrollkarte ist keine Deaktivierung vorgesehen.

Kontrollgerätekarten/Fahrtenschreiberkarten, die nicht mehr verwendet werden können oder dürfen, werden von der A-CIA im ZKR als solche gekennzeichnet.

4.1.10 Dienste zur Statusabfrage von Zertifikaten und Kontrollgerätekarten/Fahrtenschreiberkarten

Zertifikatsinformationen entsprechen den Statusinformationen über die Kontrollgerätekarte/Fahrtenschreiberkarte, für welche die Zertifikate ausgestellt wurden, und können über das ZKR und das TACHOnet abgefragt werden.

Die MSCA Software enthält keine Funktionalität zur Verwaltung von Zertifikatsstatusinformationen.

4.1.11 Ende des Vertragsverhältnisses

Das Vertragsverhältnis des Kartenantragstellers mit der Republik Österreich vertreten durch den Bundesminister für Verkehr, Innovation und Technologie endet mit dem Ablauf der Kontrollgerätekarten-/Fahrtenschreiberkartengültigkeit.

4.1.12 Schlüsselhinterlegung und –wiederherstellung

Die privaten Schlüssel der Kontrollgerätekarten/Fahrtenschreiberkarten werden nur temporär (während des Ausstellungsprozesses) gehalten (siehe Abschnitt 4.1.3 Ausstellung von Zertifikaten und Kontrollgerätekarten). Eine darüber hinausgehende persistente Speicherung der privaten Schlüssel der Kontrollgerätekarten/Fahrtenschreiberkarten ist nicht erlaubt.

4.2 Anforderungen an den Betriebsablauf für Master Keys

Da auf nationaler Ebene in Österreich keine Master Keys erzeugt und ausgegeben werden, entfällt dieser Abschnitt im Gegensatz zu [ERCA Policy Gen 2]. Die Handhabung der Master Keys ist in Abschnitt 6 Technische Sicherheitsmaßnahmen enthalten.

5 Sicherheitsmaßnahmen betreffend Infrastruktur, Verwaltung und Betrieb

Die A-MSA, die A-MSCA und der A-CP stellen innerhalb ihres Einflussbereichs sicher, dass bei der Initialisierung, Beschlüsselung und Personalisierung der Kontrollgerätekarten/Fahrtenschreiberkarten und Kontrollgeräte/Fahrtenschreiber sicherheitskritische Informationen wie private Schlüssel u. ä. entsprechend den Anforderungen der unter Abschnitt 1 Einleitung genannten Bestimmungen und dieser A-MSA Policy geschützt werden.

Die Spalten in nachfolgender Tabelle bezeichnen die Sicherheitsanforderungen der Vertraulichkeit (C), Integrität (I) und Verfügbarkeit (A).

Die möglichen Sicherheitsstufen sind:

- X (sehr hoch): Ein Verstoß gegen diese Sicherheitsstufe führt zu einen kompletten Zusammenbruch der gesamten Sicherheit und/oder Funktionalität des Digital Tachograph Systems. Es ist äußerst schwierig beziehungsweise unmöglich, die verursachte Beschädigung zu überwinden.

- H (hoch): Ein Verstoß gegen diese Sicherheitsstufe führt (zumindest vorübergehend) zu schweren Sicherheits- oder Funktionalitätsproblemen des Digital Tachograph Systems. Es ist schwierig und/oder zeitraubend die verursachte Beschädigung zu überwinden.
- M (niedrig bis mittel): Ein Verstoß gegen diese Sicherheitsstufe führt (höchstens) zu begrenzten Sicherheits- oder Funktionalitätsproblemen des Digital Tachograph Systems. Es ist wahrscheinlich, dass die Ursachen dieser Probleme schnell behoben werden können.

Die Spalte Geheimhaltungsklassifizierung beschreibt die Einstufung der Vertraulichkeit, die jedem Objekt zugewiesen wird und wie folgt definiert ist:

- Hoch: Das Objekt verlässt nie eine sichere Umgebung
- Mittel: Das Objekt wird nur mit spezifischer Autorisierung an Dritte weitergegeben
- Niedrig: Das Objekt kann veröffentlicht werden.

Anlage	C	I	A	Geheimhaltungs-klassifizierung	Bemerkung
Krypographische Objekte Generation 1					
EUR.PK		H	M	Niedrig	Empfänger (A-MSCA) benötigt Herkunftsnachweis (ERCA)
Km_{WC}	X	H	M	Hoch	Empfänger (A-MSCA) benötigt Herkunftsnachweis (ERCA)
Km_{WC}.KDR	M	X	M	Niedrig	Empfänger (ERCA) benötigt Herkunftsnachweis (A-MSCA)
Km_{WC}.KDM	M	X	M	Niedrig	Empfänger (A-MSCA) benötigt Herkunftsnachweis (ERCA)
$MS.SK_n$	X	H	M	Hoch	Backup auf Smartcards
$MS.PK_n$		H	M	Niedrig	Backup auf Smartcards
$MS.SK_{n+1}$	X	H	M	Hoch	Backup auf Smartcards Wird nach Backup vom HSM gelöscht
$MS.PK_{n+1}$		H	M	Niedrig	Backup auf Smartcards
$MS.KCR_n$	M	X	M	Niedrig	Empfänger (ERCA) benötigt Herkunftsnachweis (A-MSCA)
$MS.C_n$		M	M	Niedrig	Empfänger (A-MSCA) benötigt Herkunftsnachweis (ERCA)
EQT.SK	H	H	M	Hoch	
EQT.PK		H	M	Niedrig	
EQT.C		M	M	Niedrig	
MSCA.KT	X	H	M	Mittel	Backup auf Smartcards Export in verschlüsselter Form

					zur Übergabe an A-CP
Krypographische Objekte Generation 2					
EUR.C_i		H	M	Niedrig	Empfänger (A-MSCA) benötigt Herkunftsnachweis (ERCA)
EUR.LC_i		H	M	Niedrig	Empfänger (A-MSCA) benötigt Herkunftsnachweis (ERCA)
$K_{M\text{-}WCi}$	X	H	M	Hoch	Empfänger (A-MSCA) benötigt Herkunftsnachweis (ERCA)
$K_{M\text{-}WCi}$.KDR	M	X	M	Niedrig	Empfänger (ERCA) benötigt Herkunftsnachweis (A-MSCA)
$K_{M\text{-}WCi}$.KDM	M	X	M	Niedrig	Empfänger (A-MSCA) benötigt Herkunftsnachweis (ERCA)
$K_{M\text{-}DSRCi}$	X	H	M	Hoch	Empfänger (A-MSCA) benötigt Herkunftsnachweis (ERCA)
$K_{M\text{-}DSRCi}$.KDR	M	X	M	Niedrig	Empfänger (ERCA) benötigt Herkunftsnachweis (A-MSCA)
$K_{M\text{-}DSRCi}$.KDM	M	X	M	Niedrig	Empfänger (A-MSCA) benötigt Herkunftsnachweis (ERCA)
MSCA_Card.SK_n	X	H	M	Hoch	Backup auf Smartcards
MSCA_Card.PK_n		H	M	Niedrig	Backup auf Smartcards
MSCA_Card.SK_{n+1}	X	H	M	Hoch	Backup auf Smartcards Wird nach Backup vom HSM gelöscht
MSCA_Card.PK_{n+1}		H	M	Niedrig	Backup auf Smartcards
MSCA_Card.KCR_n	M	X	M	Niedrig	Empfänger (ERCA) benötigt Herkunftsnachweis (A-MSCA)
MSCA_Card.C_n		M	M	Niedrig	Empfänger (A-MSCA) benötigt Herkunftsnachweis (ERCA)
Card_MA.SK	H	H	M	Hoch	
Card_MA.PK		H	M	Niedrig	
Card_MA.C		M	M	Niedrig	
Card_Sign.SK	H	H	M	Hoch	
Card_Sign.PK		H	M	Niedrig	
Card_Sign.C		M	M	Niedrig	
MSCA.KT	X	H	M	Mittel	Backup auf Smartcards Export in verschlüsselter Form zur Übergabe an A-CP

Sonstige Objekte					
MSCA Software	M	X	M	Mittel	Siehe Vorgabe [ERCA Policy Gen 1]
A-MSA Policy		M	M	Niedrig	Siehe Vorgabe [ERCA Policy Gen 1]
A-MSCA Practice Statement	H	M	M	Mittel	Siehe Vorgabe [ERCA Policy Gen 1]
A-CP Practice Statement	H	M	M	Mittel	Siehe Vorgabe [ERCA Policy Gen 1]
A-CIA Practice Statement	M	M	M	Niedrig	Practice Statement der Kartenantragsstellen
A-CIA (ZKR) Practice Statement	H	M	M	Mittel	Practice Statement des Zentralen Kartenregisters

5.1 Sicherheitsmaßnahmen betreffend Infrastruktur, Verwaltung und Betrieb Allgemein

5.1.1 Physische Sicherheitsmaßnahmen

Die A-MSA, die A-MSCA und der A-CP stellen innerhalb ihres Einflussbereichs sicher, dass Initialisierung, Beschlüsselung und Personalisierung der Kontrollgerätekarten/Fahrtenschreiberkarten in besonders abgesicherten Produktionsumgebungen erfolgen (siehe Vorgaben aus [ERCA Policy Gen 1], Kapitel 7.4 und [ERCA Policy Gen 2], Kapitel 5.1). Der Zutritt zu diesen Bereichen muss wirksam beschränkt und kontrollierbar sein.

Speichermedien wie Festplatten, Smartcards und HSMs, die zum Speichern vertraulicher Informationen verwendet werden, sind vor unbefugter oder unbeabsichtigter Verwendung, Zugriff, Offenlegung oder Beschädigung durch Personen oder andere Bedrohungen (z.B. Feuer, Wasser) zu schützen.

Prozesse zur Entsorgung von Abfällen sind umzusetzen, um die unbefugte Nutzung, den Zugriff oder die Weitergabe vertraulicher Daten zu verhindern.

5.1.2 Organisatorische Sicherheitsmaßnahmen

Die A-MSCA, der A-CP und die A-CIA verwenden ein Rollenkonzept, in welchem die einzelnen Rollen und deren Aufgaben beschrieben sind (siehe Abschnitte 5.2.2 Organisatorische Sicherheitsmaßnahmen A-MSCA, 5.3.2 Organisatorische Sicherheitsmaßnahmen A-CP und 5.4.2 Organisatorische Sicherheitsmaßnahmen A-CIA). Die Administration (Schlüsselmanagement, SW-Upgrades, etc.) der entsprechenden IT-Systeme erfordert die Anwesenheit von mindestens zwei verantwortlichen Personen die dem Rollenkonzept unterliegen.

5.1.3 Personelle Sicherheitsmaßnahmen

Die A-MSA, die A-MSCA, der A-CP und die A-CIA stellen sicher, dass das eingesetzte Personal die für ihre Aufgaben geforderte Qualifikation aufweist. Regelmäßige Ausbildungs- und Schulungsmaßnahmen der Mitarbeiter sind durchzuführen und zu dokumentieren (Details siehe [A-MSCA PS], [A-CP PS] und [A-CIA PS]). Darüber hinaus sind ihrer Rolle entsprechend angemessene personelle Sicherheitsmaßnahmen zu setzen.

5.1.4 Überwachung/Protokollierung

Jeder Zutritt zu den IT-Systemen, jeder Zugriff auf die IT-Systeme sowie alle auf den IT-Systemen vorgenommenen Aktionen müssen so protokolliert werden, dass Verfügbarkeit und Integrität der Protokollierung auch im Falle einer Schlüsselkompromittierung sichergestellt ist.

5.1.5 Archivierung

Die Vorgaben bzgl. der Archivierung leiten sich von der [ERCA Policy Gen 2], Kapitel 5.5 ab.

Die A-MSCA, der A-CP und die A-CIA verwenden geeignete Archivierungsprozesse. Es werden Verfahren eingesetzt, welche die Integrität, Authentizität und Vertraulichkeit der Aufzeichnungen gewährleisten.

Die Archivierungszeiträume für die archivierten Informationen sind unbestimmt. Konkrete Archivierungszeiträume sind im [KFG], dem [A-MSCA PS], dem [A-CP PS] und im [A-CIA PS] angegeben. Die Archivierung erfolgt dabei nach dem Best-Effort-Prinzip.

Es sind Maßnahmen zu treffen, um sicherzustellen, dass die archivierten Informationen so aufbewahrt werden, dass ein Verlust und ein Zugriff von Unberechtigten ausgeschlossen werden kann.

Die in [ERCA Policy Gen 2], Kapitel 5.4 genannten Ereignisse werden regelmäßig auf ihre Integrität überprüft. Diese Inspektionen finden mindestens einmal jährlich statt.

5.1.6 Schlüsselwechsel

Der Schlüsselwechsel des MSCA Schlüsselpaares erfolgt in Abstimmung zwischen A-MSA, A-MSCA, A-CP und A-CIA, damit sichergestellt ist, dass der laufende Betrieb des Digital Tachograph Systems gewährleistet ist.

5.1.7 Kompromittierung und Notfallwiederherstellung

Für die Kompromittierung und Notfallwiederherstellung gelten die Vorgaben der [ERCA Policy Gen 1], Kapitel 7.6 und [ERCA Policy Gen 2], Kapitel 5.7. Folgende Ereignisse werden daher als Katastrophe angesehen:

1. Kompromittierung oder Diebstahl eines privaten Schlüssels und/oder eines Master Keys,
2. Verlust eines privaten Schlüssels und/oder eines Master Keys,
3. IT-Hardwarefehler.

Wird bei einer der beteiligten Stellen eine Kompromittierung von Schlüsseln (MS.SK, MSCA_Card.SK, Km_{WC}, $K_{M\text{-}WC}$, $K_{M\text{-}DSRC}$, MSCA.TK) bekannt, oder besteht ein begründeter Verdacht auf eine Kompromittierung, so wird umgehend (innerhalb von 8 Stunden) der jeweilige Sicherheitsbeauftragte informiert. Der Sicherheitsbeauftragte ist für die unverzügliche Weiterleitung dieser Information an die A-MSA verantwortlich; die A-MSA ihrerseits setzt unverzüglich die ERCA über den Verdacht oder die Kompromittierung in Kenntnis und geben die Umstände an, unter welchen die Kompromittierung stattgefunden hat.

Alle privaten Schlüssel und Master Keys müssen sofort deaktiviert werden (so dass sie nicht verwendet werden können), wenn eine Kompromittierung vermutet wird. Die A-MSCA und/oder der A-CP untersuchen die vermutete Kompromittierung. Das Ergebnis der Untersuchung der Kompromittierung wird der ERCA gemeldet. Wird eine Kompromittierung bestätigt oder kann diese nicht ausgeschlossen werden, werden die Schlüssel vernichtet.

Auch alle Kopien eines kompromittierten Schlüssels werden vernichtet. Wenn eine Kompromittierung ausgeschlossen werden kann, werden die Schlüssel wieder aktiviert.

Die Vernichtung von privaten Schlüsseln und Master Keys erfolgt mit der Funktion des HSM für die Schlüsselvernichtung.

5.1.8 Einstellung des Betriebs

Siehe Abschnitt 9.10 Inkrafttreten und Beendigung der Gültigkeit.

5.2 Sicherheitsmaßnahmen betreffend Infrastruktur, Verwaltung und Betrieb A-MSCA

5.2.1 Physische Sicherheitsmaßnahmen A-MSCA

Die A-MSCA gewährleistet einen ausreichenden infrastrukturellen und physischen Schutz ihrer Daten und IT-Systeme. Dieser umfasst insbesondere einen ausreichenden Zutrittsschutz für sicherheitsrelevante Bereiche (Details siehe [A-MSCA PS]). Bereiche, in denen private und geheime Schlüssel erzeugt, aufbewahrt und verarbeitet werden, müssen durch besondere Maßnahmen geschützt werden. Die Sicherheitsinfrastruktur um die Sicherheit innerhalb der A-MSCA zu gewährleisten, muss jederzeit aufrechterhalten werden.

5.2.2 Organisatorische Sicherheitsmaßnahmen A-MSCA

Die A-MSCA wendet ein geeignetes Information Security Management System (ISMS) an, durch das die informationstechnische Sicherheit aller für ihre Aufgaben relevanten Tätigkeiten dauerhaft gewährleistet ist. Die Vorgehensweisen sollen den Anforderungen von [ISO 27001] genügen.

Die A-MSCA stellt sicher, dass für alle im Zusammenhang mit der A-MSCA relevanten IT-Systeme und Informationen eine Schutzbedarfsfeststellung durchgeführt wird.

Für die Tätigkeit der A-MSCA ist ein Sicherheitskonzept zu erstellen. Dieses Konzept ist mit dem Betriebshandbuch abzustimmen.

Das Betriebshandbuch der A-MSCA ist vertraulich zu behandeln. Informationen daraus dürfen in Absprache mit der A-MSA Vorort bei der A-MSCA eingesehen werden, wenn ein nachgewiesenes, berechtigtes Interesse vorliegt und die Vertraulichkeit der Informationen auch beim Empfänger hinreichend geschützt ist.

Durch die Einrichtung von Rollenkonzepten soll verhindert werden, dass einzelne Personen Sicherheitsvorkehrungen der A-MSCA umgehen. Hierzu werden den einzelnen Rollen jeweils beschränkte Rechte und Pflichten zugewiesen. Die genaue Ausgestaltung und mögliche Aufgliederung einzelner Rollen hängt von den konkreten Abläufen bei der A-MSCA ab und bleibt dem jeweiligen Betriebshandbuch vorbehalten.

Zumindest folgende Rollen sind vorzusehen:

- Key-Manager (KM)
- System-Administrator (Sys-Admin)
- CA-Administrator (CA-Admin)
- System-Security Officer (SSO)

Jede dieser Rollen ist mit mindestens einer Person mit ausreichender Verfügbarkeit zu besetzen; mindestens ein Vertreter ist zu benennen. Innerhalb eines Prozesses darf eine Person nicht mehr als eine dieser Rollen wahrnehmen.

Zusätzlich zu diesen projekt-spezifischen Rollen ist in jeder Organisation ein organisationsweiter Sicherheitsbeauftragter festzulegen. Dieser ist auch die erste Ansprechstelle für organisationsübergreifende Sicherheitsvorfälle.

Die KM-Rolle umfasst:

- die sichere Durchführung der Key-Management-Prozesse,
- die Erzeugung, Zertifizierung, Verwaltung und Löschung der asymmetrischen Schlüssel der A-MSCA, sowie der symmetrischen Schlüssel, die zur Verschlüsselung von Daten der Kontroll- und Werkstattkarten verwendet werden.

Die Aufgaben des Key-Managers können nur gemeinsam mit einer weiteren autorisierten Person durchgeführt werden.

Die Sys-Admin-Rolle umfasst:

- die Verantwortlichkeit für den reibungslosen Betrieb der IT-Systeme,
- die Verantwortlichkeit für den reibungslosen Betrieb der technischen Netzwerkkomponenten. Dies betrifft beispielsweise die Firewall-Komponenten, die VPN-Komponenten und die Verkabelung.

Die CA-Admin-Rolle umfasst:

- die Verantwortlichkeit für die Konfiguration und den Betrieb der MSCA Software.

Die SSO-Rolle umfasst:

- die Überwachung der Sicherheit aller Geschäftsprozesse im Detail und Auswertung des Standes der Sicherheitsmaßnahmen,
- die Überwachung aller anderen Rollen, die Umsetzung der Security Policy, das Change-Management und die Realisierung der Geschäftsprozesse und Anweisungen innerhalb seiner Organisation,
- die Verantwortung zur Durchführung der Audits, die regelmäßig innerhalb seiner Organisation vorgenommen werden müssen.

Identifikation und Authentifizierung der einzelnen Rollen sollen entsprechend dieser A-MSA Policy im [A-MSCA PS] festgeschriebenen werden.

5.2.3 Personelle Sicherheitsmaßnahmen A-MSCA

Die A-MSCA stellt sicher, dass nur zuverlässiges und ausreichend qualifiziertes Personal mit den erforderlichen Tätigkeiten betraut wird. Die A-MSCA kann darüber hinausgehende Anforderungen festlegen. Diese müssen im [A-MSCA PS] festgehalten werden.

Personen die im Umfeld des Digital Tachograph Systems arbeiten und Zutritt zu Systemräumen benötigen, müssen entweder mindestens 1 Jahr im Unternehmen der A-MSCA beschäftigt sein, oder eine §55 Überprüfung (der Stufe geheim) nach dem Sicherheitspolizeigesetz (SPG) vorweisen.

5.2.4 Überwachung/Protokollierung A-MSCA

Alle sicherheitsrelevanten Aktionen und Prozesse auf den für die Tätigkeit relevanten IT-Systemen sind so zu protokollieren, dass sich der zugehörige Zeitpunkt und die entsprechenden Personen mit hinreichender Sicherheit nachvollziehen lassen. Dazu gehören zumindest (siehe [ERCA Policy Gen 2], Kapitel 5.4):

- jeder Versuch der Einrichtung von Benutzerbereichen (Accounts) und Authentifizierungsmethoden
- jeder Versuch der An- und Abmeldung

- Software-Installationen und –Updates
- Hardware-Modifikationen
- jeder Versuch der Konfigurationsänderungen an der Software
- Herunterfahren und Neustarts des IT-Systems und der Software
- jeder Versuch der Erstellung von Zertifikatsrequests
- jeder Versuch des HSM Zugriffs (Authentisierung, Schlüsselerzeugung und –löschung, Schlüsselimport und –export, Schlüsselverwendung)
- Protokolle aller Audits

Die Protokolle sind gegen Veränderung und unberechtigten Zugriff zu schützen. Sie müssen regelmäßig und anlassbezogen ausgewertet und analysiert werden können.

Alle Einträge sind mit Datums- und Zeitangabe zu versehen.

Zwei Exemplare der Protokolldaten sind in zwei getrennten, physisch gesicherten Umgebungen aufzubewahren.

5.2.5 Archivierung A-MSCA

Siehe Abschnitt 5.1.5 Archivierung.

5.2.6 Schlüsselwechsel A-MSCA

MSCA Schlüsselpaare werden regelmäßig und nach Bedarf generiert. Die A-MSCA achtet dabei darauf, dass die Gültigkeitsdauer des aktuell im Einsatz befindlichen MSCA Schlüsselpaares nicht überschritten wird.

5.2.7 Kompromittierung und Notfallwiederherstellung A-MSCA

Das [A-MSCA PS] muss eine explizite Vorgehensweise für den Fall enthalten, dass eine Kompromittierung eines oder mehrerer MSCA Schlüssel (MS.SK, MSCA_Card.SK) oder Master Keys (Km_{WC}, $K_{M\text{-}WC}$, $K_{M\text{-}DSRC}$) stattgefunden hat oder der begründete Verdacht dazu besteht. Diese Vorgehensweise soll auch Anweisungen an externe Dienstleister und Informationen an Kartenbesitzer und Gerätehersteller enthalten. Im Falle einer Schlüsselkompromittierung oder des begründeten Verdachts ist die A-MSA und von dieser die ERCA unverzüglich zu informieren.

Die A-MSCA hat einen Notfallplan zu erstellen, in dem das Verhalten bei schwerwiegenden Notfällen wie einer Schlüsselkompromittierung oder beim Verlust oder Ausfall von relevanten Daten und/oder IT-Systemen festgelegt ist.

5.2.8 Einstellung des Betriebs A-MSCA

Siehe Abschnitt 9.10 Inkrafttreten und Beendigung der Gültigkeit.

5.3 Sicherheitsmaßnahmen betreffend Infrastruktur, Verwaltung und Betrieb A-CP

5.3.1 Physische Sicherheitsmaßnahmen A-CP

Die Vertraulichkeit der spezifischen Daten des Kartenhalters und der kartenspezifischen Daten muss gewährleistet sein. Aufgrund der gehobenen Sicherheitsanforderungen an die Produktion und Personalisierung der Kontrollgerätekarten/Fahrtenschreiberkarten ist eine gesicherte Umgebung gefordert.

Der Betrieb der Kartenpersonalisierung ist durch geeignete bauliche und technische Maßnahmen gegen äußere Einflüsse abzusichern (Details siehe [A-CP PS]). Hierzu gehören zumindest:

- Hochsicherheitszugangskontrolle für den Zugang zum Hochsicherheitsbereich der Kartenpersonalisierung und zur PIN Brief Druckstation
- 24 h Überwachung der gegen externe Eingriffe zu schützenden Anlagenteile (z.B. Gebäude, Personalisierungsanlagen, etc.)
- Absicherung des Produktionsgeländes und der Gebäude
- Computerüberwachte Alarmanlagen
- „Man-Trap" - gesicherte Eingänge
- Besucherregelung
- Direkte Verbindung zur Exekutive oder 24 Stunden/Tag * 7 Tage/Woche anwesender Sicherheitsdienst

Die Sicherheitsinfrastruktur und die Sicherheit innerhalb des A-CP muss jederzeit gewährleistet und aufrechterhalten werden. Jede Änderung, die sich auf die Sicherheit auswirkt, muss von der A-MSA genehmigt werden.

5.3.2 Organisatorische Sicherheitsmaßnahmen A-CP

Der A-CP wendet ein geeignetes Information Security Management System (ISMS) an, durch das die informationstechnische Sicherheit aller für ihre Aufgaben relevanten Tätigkeiten dauerhaft gewährleistet ist. Die Vorgehensweisen sollen den Anforderungen von [ISO 27001] genügen.

Der A-CP stellt sicher, dass für alle im Zusammenhang mit dem A-CP relevanten IT-Systeme und Informationen eine Schutzbedarfsfeststellung durchgeführt wird.

Für die Tätigkeit des A-CP ist ein Sicherheitskonzept zu erstellen. Dieses Konzept ist mit dem Betriebskonzept abzustimmen.

Eine Aufteilung der Funktionen ist entsprechend der nachfolgenden Rollen vorzunehmen:

- System-Security Officer (SSO)
- Key Manager (KM)
- Auditor
- Administrator
- Qualitätskontrolle
- Operator
- Service

Jede dieser Rollen ist mit mindestens einer Person mit ausreichender Verfügbarkeit zu besetzen; mindestens ein Vertreter ist zu benennen. Innerhalb eines Prozesses darf eine Person nicht mehr als eine dieser Rollen wahrnehmen.

Bei internen Audits können die Rollen Qualitätskontrolle und Auditor von einer Person wahrgenommen werden.

Die SSO-Rolle umfasst:

- die Überwachung der Sicherheit aller Geschäftsprozesse im Detail und Auswertung des Standes der Sicherheitsmaßnahmen,
- die Überwachung aller anderen Rollen, die Umsetzung der Security Policy, das Change-Management und die Realisierung der Geschäftsprozesse und Anweisungen innerhalb der Organisation.

Die KM-Rolle umfasst:

- die sichere Durchführung der Key-Management-Prozesse,

- die Erzeugung, Zertifizierung, Verwaltung und Löschung der asymmetrischen Schlüssel der A-MSCA, sowie der symmetrischen Schlüssel, die zur Verschlüsselung von Daten der Kontroll- und Werkstattkarten verwendet werden,
- die Aufgaben des Key-Managers können nur gemeinsam mit einer weiteren autorisierten Person durchgeführt werden.

Die Auditor-Rolle umfasst:

- die Verantwortung zur Durchführung aller Audits, die regelmäßig innerhalb der Organisation vorgenommen werden müssen.

Die Administrator-Rolle umfasst:

- die Verantwortlichkeit für die Verwaltung und den reibungslosen Betrieb der technischen Komponenten.

Die Qualitätskontrolle-Rolle umfasst:

- die Verantwortung über die gesamte Qualitätskontrolle.

Die Operator-Rolle umfasst:

- unter anderem die Verantwortung für die Erzeugung von Backup- und Recovery-Prozeduren.

Die Service-Rolle umfasst:

- die Verantwortung für das Service der technischen Komponenten.

Der A-CP muss die Aufgaben der einzelnen Rollen im [A-CP PS] beschreiben.

Identifikation und Authentifizierung der einzelnen Rollen sollen entsprechend dieser A-MSA Policy im [A-CP PS] festgeschriebenen werden.

Um die interne Sicherheit der Kartenproduktion zu gewährleisten, sind mindestens folgende Anforderungen zu erfüllen:

- "Vier-Augen Prinzip" in allen sicherheitsrelevanten Bereichen im Rahmen des Projekts Digital Tachograph System
- Persönliche Identifikation der am Produktionsprozess beteiligten Mitarbeiter
- Genaue Dokumentation der verwendeten Kartenrohlinge (Volume Check)
- Aufbewahrung der Kartenrohlinge im Tresor

5.3.3 Personelle Sicherheitsmaßnahmen A-CP

Der A-CP stellt sicher, dass nur zuverlässiges und ausreichend qualifiziertes Personal mit den erforderlichen Tätigkeiten betraut wird. Durch alle im Bereich der Kartenpersonalisierung beschäftigten Personen ist die Einhaltung der personenbezogenen Sicherheitsmaßnahmen zu gewährleisten.

5.3.4 Überwachung/Protokollierung A-CP

Diebstahl oder Verlust von Karten und Schlüsselmaterial, sowie andere Verstöße gegen die Sicherheitsvorschriften müssen in adäquater Zeit erkannt und behandelt werden.

Um die interne Sicherheit der Kartenproduktion zu gewährleisten, sind mindestens folgende Anforderungen bzgl. der Überwachung zu erfüllen:

- Überwachung der Kartenproduktion und PIN Letter Produktion
- Überwachung des Tresors

Die bei der Personalisierung von Kontrollgerätekarten/Fahrtenschreiberkarten aufgenommenen Protokollierungen müssen eine Zuordnung der jeweiligen Aktion zur zugehörigen Kontrollgerätekarten-/Fahrtenschreiberkartennummer und zum zugehörigen Zertifikat erlauben.

Alle sicherheitsrelevanten Aktionen und Prozesse auf den für die Tätigkeit relevanten IT-Systemen sind so zu protokollieren, dass sich der zugehörige Zeitpunkt und die entsprechenden Personen mit hinreichender Sicherheit nachvollziehen lassen. Dazu gehören zumindest:

- das Einrichten von Benutzerbereichen (Accounts)
- Software-Installationen und –Updates
- Hardware-Modifikationen
- Herunterfahren und Neustarts des IT-Systems
- Zugriff auf Logs und Archive
- aufgebrachte Zertifikate
- jeder Versuch der Erstellung von Key Distribution Requests
- Protokolle aller Audits
- nachweisliche Einarbeitung der relevanten Dokumente in das Sicherheitskonzept

Die Protokolle sind gegen Veränderung und unberechtigten Zugriff zu schützen. Sie sollen regelmäßig und anlassbezogen ausgewertet und analysiert werden.

Alle Einträge sind mit Datums- und Zeitangabe zu versehen.

Zwei Exemplare der Protokolldaten sind in zwei getrennten, physisch gesicherten Umgebungen aufzubewahren.

Die Protokolldaten sind so zu speichern, dass ein Zugriff während der Aufbewahrungszeit möglich ist.

Die Protokolldaten sind vor unautorisiertem Zugriff zu schützen.

5.3.5 Archivierung A-CP

Siehe Abschnitt 5.1.5 Archivierung.

5.3.6 Schlüsselwechsel A-CP

Siehe Abschnitt 5.1.6 Schlüsselwechsel.

5.3.7 Kompromittierung und Notfallwiederherstellung A-CP

Der A-CP hat einen Notfallplan zu erstellen, in dem das Verhalten bei schwerwiegenden Notfällen wie einer Schlüsselkompromittierung oder beim Verlust oder Ausfall von relevanten Daten und/oder IT-Systemen festgelegt ist.

5.3.8 Einstellung des Betriebs A-CP

Siehe Abschnitt 9.10 Inkrafttreten und Beendigung der Gültigkeit.

5.4 Sicherheitsmaßnahmen betreffend Infrastruktur, Verwaltung und Betrieb A-CIA

5.4.1 Physische Sicherheitsmaßnahmen A-CIA

Die A-CIA gewährleistet einen ausreichenden infrastrukturellen und physischen Schutz ihrer Daten und IT-Systeme. Dieser umfasst insbesondere einen ausreichenden Zutrittsschutz für sicherheitsrelevante Bereiche (Details siehe [A-CIA PS]).

Die Sicherheitsinfrastruktur um die Sicherheit innerhalb der A-CIA zu gewährleisten, muss jederzeit aufrechterhalten werden.

5.4.2 Organisatorische Sicherheitsmaßnahmen A-CIA

Die A-CIA wendet ein geeignetes Information Security Management System (ISMS) an, durch das die informationstechnische Sicherheit aller für ihre Aufgaben relevanten Tätigkeiten dauerhaft gewährleistet ist. Die Vorgehensweisen sollen den Anforderungen von [ISO 27001] genügen.

Durch die Einrichtung von Rollenkonzepten soll verhindert werden, dass einzelne Personen die Sicherheitsvorkehrungen der A-CIA umgehen. Hierzu werden den einzelnen Rollen jeweils beschränkte Rechte und Pflichten zugewiesen. Die genaue Ausgestaltung und mögliche Aufgliederung einzelner Rollen hängt von den konkreten Abläufen bei der A-CIA ab.

Zumindest folgende Rollen sind vorzusehen:

- System-Administrator (Sys-Admin)
- Administrator des ZKR (ZKR-Admin)
- Sachbearbeiter der Antragsstelle

Jede dieser Rollen ist mit mindestens einer Person mit ausreichender Verfügbarkeit zu besetzen.

Die Sys-Admin-Rolle umfasst:

- die Verantwortlichkeit für den reibungslosen Betrieb der IT-Systeme,
- die Verantwortlichkeit für den reibungslosen Betrieb der technischen Netzwerkkomponenten. Dies betrifft beispielsweise die Firewall-Komponenten, die VPN-Komponenten und die Verkabelung.

Die ZKR-Admin-Rolle umfasst:

- die Verantwortlichkeit für die Konfiguration und den Betrieb der ZKR-Software.

Die Rolle des Sachbearbeiters der Antragsstelle umfasst:

- die Verantwortlichkeit für die Antragsbearbeitung für eine Karte gemäß den gesetzlichen Vorgaben und die Erfassung der dafür notwendigen Antragsdaten.

Identifikation und Authentifizierung der einzelnen Rollen sollen entsprechend dieser A-MSA Policy im [A-CIA PS] festgeschrieben werden.

5.4.3 Personelle Sicherheitsmaßnahmen A-CIA

Die A-CIA stellt sicher, dass nur zuverlässiges und ausreichend qualifiziertes Personal mit den erforderlichen Tätigkeiten betraut wird.

Die A-CIA kann darüber hinausgehende Anforderungen festlegen. Diese müssen im [A-CIA PS] festgehalten werden.

5.4.4 Überwachung/Protokollierung A-CIA

Sicherheitsrelevante Aktionen und Prozesse auf den für die Tätigkeit relevanten IT-Systemen sind so zu protokollieren, dass sich der zugehörige Zeitpunkt und die entsprechenden Personen oder Personengruppen mit hinreichender Sicherheit nachvollziehen lassen.

Die Protokolldaten sind vor unautorisiertem Zugriff zu schützen.

Alle Einträge sind mit Datums- und Zeitangabe zu versehen.

5.4.5 Archivierung A-CIA

Siehe Abschnitt 5.1.5 Archivierung.

5.4.6 Schlüsselwechsel A-CIA

Siehe Abschnitt 5.1.6 Schlüsselwechsel.

5.4.7 Kompromittierung und Notfallwiederherstellung A-CIA

Kompromittierung ist für die A-CIA nicht anwendbar, da sie keine privaten oder geheimen Schlüssel speichert.

Die A-CIA hat einen Notfallplan zu erstellen, in dem das Verhalten bei schwerwiegenden Notfällen, wie beim Verlust oder Ausfall von relevanten Daten und/oder IT-Systemen, festgelegt ist.

5.4.8 Einstellung des Betriebs A-CIA

Siehe Abschnitt 9.10 Inkrafttreten und Beendigung der Gültigkeit.

6 Technische Sicherheitsmaßnahmen

Dieses Kapitel enthält Anforderungen für den Umgang mit folgendem Schlüsselmaterial:

- der öffentliche Schlüssel der ERCA (EUR.PK)
- die öffentlichen Zertifikate der ERCA (EUR.C, EUR.LC)
- die Schlüsselpaare der A-MSCA (MS.SK, MS.PK, MSCA_Card.SK, MSCA_Card.PK)
- die symmetrischen Schlüssel für Werkstattkarten (Km_{WC}, $K_{M\text{-}WC}$)
- der symmetrische Schlüssel für Kontroll- und Werkstattkarten ($K_{M\text{-}DSRC}$)
- der Transportschlüssel (MSCA.KT) für A-MSCA und A-CP

A-MSCA und A-CP stellen die Vertraulichkeit und Integrität aller bei ihnen erzeugten, verwendeten und/oder gespeicherten nicht-öffentlichen Schlüssel sicher und verhindern wirksam jeglichen Missbrauch dieser Schlüssel.

6.1 Schlüsselerzeugung und Installation

6.1.1 MSCA Schlüsselpaar

Die ERCA besitzt die Root-Schlüsselpaare der Digital Tachograph PKIs. Mit diesen Schlüsselpaaren werden die Zertifikate MS.C und MSCA_Card.C ausgestellt und signiert.

Die Erzeugung der MSCA-Schlüsselpaare MS.KP und MSCA_Card.KP darf nur bei aktiver Mitwirkung von mindestens drei unterschiedlichen Personen erfolgen. Eine dieser Personen muss die Rolle des A-MSCA Key-Managers übernehmen, die beiden anderen müssen jeweils eine andere der in dieser A-MSA Policy beschriebenen Rollen wahrnehmen.

Das für die Schlüsselerzeugung verwendete Gerät wird im [A-MSCA PS] genannt.

Die Schlüssel MS.SK und MS.PK müssen für einen RSA-Algorithmus mit einer Länge gemäß der unter Abschnitt 1 Einleitung genannten Bestimmungen erzeugt werden.

Die Schlüssel MSCA_Card.SK und MSCA_Card.PK müssen für den ECDSA-Algorithmus mit einer Länge gemäß der unter 1 Einleitung genannten Bestimmungen erzeugt werden.

Die A-MSCA stellt sicher, dass der MS.SK ausschließlich zur Generierung des MSCA Zertifikatsrequests MS.KCR laut [ERCA Policy Gen 1] Annex A sowie zur Signierung von Zertifikaten für Kontrollgerätekarten/Fahrtenschreiberkarten verwendet wird.

Die A-MSCA stellt sicher, dass der Key Identifier (KID) und der Modulus (n) für das MS.KP, das an die ERCA zur Erzeugung des MS.C gesendet wird, innerhalb der A-MSA einzigartig sind.

Die A-MSCA stellt sicher, dass der MSCA_Card.SK ausschließlich zur Generierung des MSCA Zertifikatsrequests MSCA_Card.KCR laut [ERCA Policy Gen 2] sowie zur Signierung von Zertifikaten für Kontrollgerätekarten/Fahrtenschreiberkarten verwendet wird.

Die A-MSCA stellt sicher, dass der Key Identifier (KID) und der öffentliche Schlüssel des MSCA_Card.KP, das an die ERCA zur Erzeugung des MSCA_Card.C gesendet wird, innerhalb der A-MSA einzigartig ist.

Die ERCA erzeugt aufgrund des MS.KCR und des MSCA_Card.KCR die MSCA Zertifikate MS.C und MSCA_Card.C.

Die MSCA Zertifikate MS.C und MSCA_Card.C sowie der öffentliche Schlüssel der ERCA EUR.PK und die Zertifikate der ERCA EUR.C und EUR.LC werden von der ERCA an die A-MSCA übergeben.

Die A-MSCA sollte - im Rahmen der Vorgaben der [ERCA Policy Gen 1] und [ERCA Policy Gen 2] - eine angemessene Anzahl von Ersatz-Schlüsselpaaren mit den zugehörigen Zertifikaten vorhalten, um bei Nichtverfügbarkeit des aktuellen Schlüssels einen schnellen Schlüsselwechsel auch ohne aktive Mitwirkung der ERCA durchführen zu können. Sollten mehrere aktuelle Ersatz-Schlüsselpaare vorliegen, stellt die A-MSCA sicher, dass stets der richtige Schlüssel verwendet wird.

Schlüsselerneuerung der MSCA bedeutet, dass ein neues Schlüsselpaar angelegt und ein neues MSCA Zertifikat signiert werden, welche das bereits existierende MSCA Schlüsselpaar und MSCA Zertifikat ersetzen. Eine Schlüsselerneuerung findet statt:

- falls sich der Nutzungszeitraum eines privaten MSCA Schlüssels dem Ende nähert. Bei der Erzeugung der nächsten Schlüsselgeneration von MS.KP und MSCA_Card.KP ist eine Vorlaufzeit von einem Monat, den die ERCA für die Erstellung der Zertifikate benötigt, zu berücksichtigen.
- bei anschließendem Widerruf eines MSCA Zertifikats.

Jeder MS.SK und MSCA_Card.SK soll höchstens zwei Jahre eingesetzt werden.

Die A-MSCA hat den MS.SK und MSCA_Card.SK und alle Ersatz-Schlüssel durch technisch-organisatorische Maßnahmen wirksam vor Missbrauch, Veränderung und unbefugter Kenntnisnahme zu schützen.

Es darf nur eine Sicherheitskopie des MS.SK und MSCA_Card.SK angelegt werden, wenn zum Abrufen des Schlüssels zumindest ein 4-Augen-Prinzip garantiert ist. Die durchzuführenden Vorgänge sind im [A-MSCA PS] darzustellen.

Die A-MSCA verhindert durch technisch-organisatorische Maßnahmen wirkungsvoll, dass ein Zugriff auf den MS.SK und MSCA_Card.SK durch eine einzelne Person erfolgen kann (,,4-Augen-Prinzip").

Eine Schlüsselhinterlegung ist verboten, das Backup des MS.SK und MSCA_Card.SK wird intern von der MSCA verwaltet.

Die A-MSCA stellt in Kooperation mit der ERCA sicher, dass sie zu jedem Zeitpunkt über gültige Schlüsselpaare (MS.KP und MSCA_Card.KP) mit zugehörigem Zertifikat verfügt.

Wird ein Signatur-Schlüsselpaar nicht mehr verwendet, so wird der öffentliche Schlüssel archiviert und der private Schlüssel zerstört, dass eine Wiederherstellung unmöglich ist oder in einer Art gespeichert, dass eine Weiterverwendung unmöglich ist.

6.1.2 Master Keys

Die A-MSCA fordert bei Bedarf von der ERCA die Motion Sensor Master Keys für Werkstattkarten Km_{WC} und K_{M-WC}, sowie den DSRC Master Key K_{M-DSRC} an. Für Anforderung und Auslieferung dieses Schlüssels zwischen ERCA und A-MSCA sind die Bestimmungen der ERCA einzuhalten. Details dazu sind im [A-MSCA PS], [ERCA Policy Gen 1] und [ERCA Policy Gen 2] angegeben. Die Verteilung des Motion Sensor Master Key Km_{WC} ist mit Hilfe einer RSA-Verschlüsselung geschützt. Das dazu erforderliche RSA-Schlüsselpaar wird vom A-CP erzeugt. Die Verteilung des Motion Sensor Master Key K_{M-WC} und des DSRC Master Key K_{M-DSRC} ist mit Hilfe einer EC-Verschlüsselung geschützt. Die dazu erforderlichen EC-Schlüsselpaare werden vom A-CP erzeugt.

Der A-CP generiert die Key Distribution Requests (KDRs) für die Motion Sensor Master Keys Km_{WC} und K_{M-WC} sowie den DSRC Master Key K_{M-DSRC}. Diese werden über die A-MSCA an die ERCA weitergeleitet. Die ERCA erzeugt aufgrund der KDRs für jeden Master Key eine Key Distribution Message (KDM) laut [ERCA Policy Gen 1], Kapitel D3 und [ERCA Policy Gen 2], Kapitel 4.2.4. Die KDMs mit den Master Keys Km_{WC}, K_{M-WC} und K_{M-DSRC}, der öffentliche Schlüssel der ERCA EUR.PK und die Zertifikate der ERCA EUR.C und EUR.LC werden über die A-MSCA an den A-CP weitergeleitet.

Der A-CP stellt sicher, dass:

- innerhalb seines Verantwortungsbereiches das Auftreten von Schlüsselduplikaten für die Verteilung der Motion Sensor Master Keys und des DSRC Master Key ausgeschlossen ist;
- das RSA-Schlüsselpaar nur zur Anforderung des Km_{WC} verwendet wird und nach Abschluss der Anforderungsprozedur gesichert zerstört wird;
- die EC-Schlüsselpaare nur zur Anforderung des K_{M-WC} und K_{M-DSRC} verwendet werden und nach Abschluss der Anforderungsprozedur gesichert zerstört werden;
- der Key Distribution Request für den Km_{WC} entsprechend den Anforderungen der [ERCA Policy Gen 1] Annex D erstellt wird;
- die Key Distribution Requests für den K_{M-WC} und den K_{M-DSRC} entsprechend der [ERCA Policy Gen 2] Kapitel, 4.2 erstellt wird;
- der Km_{WC} entsprechend der Definition unter [ERCA Policy Gen 1] Annex D übernommen wird;
- der K_{M-WC} und K_{M-DSRC} entsprechend der Definition unter [ERCA Policy Gen 2] Kapitel 4.2 übernommen wird;
- das Gerät, welches für die Erzeugung dieses Schlüssels verwendet wird, im [A-CP PS] genannt wird;
- dass Km_{WC}, K_{M-WC} und K_{M-DSRC} ausreichend verfügbar sind;
- die Motion Sensor Master Keys Km_{WC} und K_{M-WC} gemäß den unter Abschnitt 1 Einleitung genannten Bestimmungen in alle Werkstattkarten eingebracht wird;
- der DSRC Master Key K_{M-DSRC} gemäß den unter Abschnitt 1 Einleitung genannten Bestimmungen in alle Kontroll- und Werkstattkarten eingebracht wird;
- die Schlüssel Km_{WC}, K_{M-WC} und K_{M-DSRC} die gesicherte Umgebung nie verlassen.

Die A-MSA verhindert den unautorisierten Gebrauch der Master Keys.

Die A-MSCA stellt sicher, dass der Key Identifier (KID) und der Modulus (n), welche an die ERCA zur Übergabe des Km_{WC} gesendet werden einzigartig sind.

Die A-MSCA stellt sicher, dass die Key Identifier (KID), welche an die ERCA zur Übergabe des $K_{M\text{-}WC}$ und $K_{M\text{-}DSRC}$ gesendet werden, einzigartig sind.

Die A-MSCA und der A-CP stellen durch geeignete Maßnahmen sicher, dass die Schlüssel Km_{WC}, $K_{M\text{-}WC}$ und $K_{M\text{-}DSRC}$ nur an die hierfür vorgesehenen Empfänger weitergegeben wird und sichern diese Weitergabe durch geeignete Maßnahmen in ihrem jeweiligen Einflussbereich (Details siehe [A-MSCA PS] und [A-CP PS]). Die A-MSA überwacht die Sicherheitsmaßnahmen der A-MSCA und des A-CP.

Eine Schlüsselhinterlegung ist verboten, das Backup der Master Keys wird intern verwaltet.

Bei der Beantragung der Master Keys bei der ERCA ist eine Vorlaufzeit von bis zu einem Monat zu berücksichtigen.

6.1.3 Transportschlüssel

Für den Fall, dass die A-MSCA ihren Kommunikationspartnern (z.B. A-CP) zur Absicherung der gegenseitigen Kommunikation kryptographische Schlüssel zur Verfügung stellt, so ist deren Vertraulichkeit und Integrität von der A-MSCA wirksam zu schützen sowie jeglicher Missbrauch wirksam zu verhindern. Die A-MSA verpflichtet die Kommunikationspartner der A-MSCA dazu, in deren Einflussbereich gleichwertige Sicherheitsvorkehrungen zum Schutz der Schlüssel zu treffen (Details siehe [A-MSCA PS] und [A-CP PS]).

6.1.4 Test-Umgebung

Die A-MSCA betreibt ein Testsystem, welches für Interoperabilitätstests verwendet wird. Das Testsystem ist vom produktiven IT-System separiert und verwendet eigene MSCA Schlüsselpaare und Master Keys. Die MSCA Zertifikate und Master Keys werden vom Testsystem der ERCA bezogen.

Der A-CP betreibt ein physisches Testsystem, welches vom produktiven System parallel und separiert betrieben wird. Dieses Testsystem wird für Interoperabilitätstests verwendet. Der Personalisierungsprozess von Tests und produktiven Daten ist logisch und physisch getrennt.

6.2 Anforderung zum Schutz privater und geheimer Schlüssel und für den Einsatz kryptographischer Module

A-MSCA und A-CP stellen innerhalb ihres jeweiligen Einflussbereiches sicher, dass private und geheime Schlüssel (z.B. Master Keys) hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit in einer gesicherten Umgebung aufbewahrt und eingesetzt werden. Sofern nach den Vorgaben der unter Abschnitt 1 Einleitung genannten Bestimmungen Schlüssel übertragen werden müssen, ist die Vertraulichkeit zu sichern.

Für die Erzeugung und Speicherung der A-MSCA Schlüssel, der Kontrollgerätekarten-/Fahrtenschreiberkartenschlüssel und für die Verteilung der Motion Sensor Master Keys und des DSRC Master Key sind besonders geeignete technische IT-Systeme einzusetzen, die eine der folgenden Anforderungen erfüllen (Zertifizierungen zumindest bei der Inbetriebnahme):

- Zertifizierung nach EAL 4 oder höher in Übereinstimmung mit [ISO/IEC 15408] unter Verwendung eines geeigneten Protection Profile
- Erfüllung der Anforderungen nach [ISO/IEC 19790]
- Erfüllung der Anforderungen nach [FIPS 140-2], Level 3
- äquivalente Sicherheitskriterien, die eine gleichwertige Sicherheit gewährleisten

Die obig genannten Anforderungen gelten immer dann, wenn auf die genannten Schlüssel im Klartext zugegriffen werden kann. Werden die Schlüssel mit Hilfe eines anerkannten starken Verschlüsselungsverfahrens mit einer Schlüssellänge von mindestens 100 Bit geschützt

(Transportschlüssel MSCA.KT), werden keine speziellen Anforderungen an die Geräte zur Datenspeicherung gestellt.

Operationen mit privaten Schlüsseln und geheimen Schlüsseln müssen im HSM erfolgen, wo die verwendeten Schlüssel gespeichert werden.

Private MSCA Schlüssel und Master Keys dürfen nur in einer physisch sicheren Umgebung von Mitarbeitern in vertrauenswürdigen Rollen unter Einhaltung des 4-Augen-Prinzips verwendet, gesichert, gespeichert und wiederhergestellt werden. Alle Ereignisse der Verwendung privater Schlüssel und Master Keys werden protokolliert.

Alle Kopien der privaten MSCA Schlüssel und der Master Keys unterliegen denselben Sicherheitsstufen wie die produktiv verwendeten Schlüssel.

Import und Export von privaten Schlüsseln erfolgt nur zu Sicherungs- und Wiederherstellungszwecken.

Der Import und Export von Master Keys ist zu Sicherungs- und Wiederherstellungszwecken zulässig.

Der Import und Export von Master Keys aus anderen Gründen ist verboten.

Am Ende des Nutzungszeitraums des privaten MSCA Schlüssels muss die A-MSCA alle Kopien des Schlüssels so zerstören, dass er nicht wiederhergestellt werden kann. Ebenso werden am Ende des Lebenszyklus eines Master Keys alle Kopien des Schlüssels zerstört, so dass er nicht wiederhergestellt werden kann.

Ebenso ist zu dokumentieren, wie diese IT-Systeme in einer sicheren Betriebsumgebung eingesetzt werden.

6.3 Weitere Aspekte des Schlüsselmanagements

Der Datenaustausch zwischen A-MSCA und ERCA findet grundsätzlich auf der Basis von [ERCA Policy Gen 1] Annex C und [ERCA Policy Gen 2] Kapitel 4.1 und 4.2 statt.

Die MSCA Zertifikate (MS.C und MSCA_Card.C) werden von der A-MSCA für unbegrenzte Zeit archiviert.

Die Gültigkeitsdauer der Zertifikate der Kontrollgerätekarten/Fahrtenschreiberkarten wird den Vorgaben von [Annex 1C] entsprechend gesetzt (siehe auch Abschnitt 1.4.1 Zulässige Verwendung).

Die Verwendungsdauer des privaten MSCA Schlüssel beträgt zwei Jahre. Die Verwendungsdauer für private Schlüssel beginnt mit dem Gültigkeitsdatum im entsprechenden Zertifikat. Die A-MSCA darf nach Ablauf der Nutzungsdauer diesen privaten Schlüssel nicht mehr verwenden.

6.4 Aktivierungsdaten

Für die Verwendung der privaten und geheimen Schlüssel der A-MSCA ist eine Aktivierung gemäß [ERCA Policy Gen 2] Kapitel 6.4 vorzusehen.

Das Generieren, Importieren, Verwenden oder Löschen von privaten MSCA Schlüsseln und/oder Master Keys, welche in einem HSM gespeicherten sind, ist nur nach Authentifizierung von Mitarbeitern in vertrauenswürdigen Rollen unter Einhaltung des 4-Augen-Prinzips möglich. Die Authentifizierung erfolgt mit geeigneten Mitteln (z.B. Passwörter, Authentifizierungs-Token). Die Dauer einer Authentifizierungssitzung darf nicht unbegrenzt sein.

Zur Aktivierung der MSCA Software und des Systems, auf dem diese Software läuft, muss die Benutzerauthentifizierung mit geeigneten Mitteln (z.B. durch ein Passwort) erfolgen.

Details zu der Handhabung der Aktivierungsdaten sind im [A-MSCA PS] beschrieben.

6.5 Sicherheitsmaßnahmen für Computer

6.5.1 Sicherheitsmaßnahmen für Computer A-MSCA

Die für die Tätigkeit der A-MSCA eingesetzten IT-Systeme müssen so betrieben werden, dass mögliche Schädigungen durch Viren u. ä. weitestgehend verhindert sowie die möglichen Folgen von Schäden und Störungen minimiert werden.

Die IT-Systeme müssen über wirksame Zugangskontrollen verfügen und insbesondere die in dieser A-MSA Policy, dem Sicherheitskonzept und Betriebshandbuch beschriebenen Rollenkonzepte wirksam implementieren.

Die Initialisierung von HSMs, die die privaten Signaturschlüssel der A-MSCA (MS.SK und MSCA_Card.SK) oder den geheimen symmetrischen Transportschlüssel (MSCA.KT) enthalten, darf nur in Kooperation von zwei Personen entsprechend dem Rollenkonzept erfolgen.

IT-Systeme brauchen keine formale Sicherheitseinstufung, wenn sie die in dieser A-MSA Policy festgelegten Anforderungen erfüllen.

6.5.2 Sicherheitsmaßnahmen für Computer A-CP

Die für die Tätigkeit des A-CP eingesetzten IT-Systeme müssen so betrieben werden, dass mögliche Schädigungen durch Viren u. ä. weitestgehend verhindert sowie die möglichen Folgen von Schäden und Störungen minimiert werden.

Die IT-Systeme müssen über wirksame Zugangskontrollen verfügen und insbesondere die in dieser A-MSA Policy, dem Sicherheitskonzept und Betriebshandbuch beschriebenen Rollenkonzepte wirksam implementieren.

6.5.3 Sicherheitsmaßnahmen für Computer A-CIA

Die für die Tätigkeit der A-CIA eingesetzten IT-Systeme müssen so betrieben werden, dass mögliche Schädigungen durch Viren u. ä. weitestgehend verhindert sowie die möglichen Folgen von Schäden und Störungen minimiert werden.

Die IT-Systeme müssen über wirksame Zugangskontrollen verfügen und insbesondere die in dieser A-MSA Policy beschriebenen Rollenkonzepte wirksam implementieren.

IT-Systeme brauchen keine formale Sicherheitseinstufung, wenn sie die in dieser A-MSA Policy festgelegten Anforderungen erfüllen.

6.6 Technische Maßnahmen im Lebenszyklus

6.6.1 Technische Maßnahmen im Lebenszyklus A-MSCA

Die A-MSCA soll für ihre Aufgaben vertrauenswürdige IT-Systeme und Software einsetzen, die durch geeignete Maßnahmen wirksam gegen unautorisierte Veränderungen geschützt sind (Details siehe [A-MSCA PS]).

Bei allen Veränderungen der eingesetzten Soft- und Hardware werden Kontrollmechanismen dokumentiert eingesetzt.

Die Produktivsysteme werden von anderen IT-Systemen separiert betrieben. Dies gilt entsprechend Vorgabe aus [ERCA Policy Gen 2] insbesondere für das Testsystem, welches für Interoperabilitätstests verwendet wird.

6.6.2 Technische Maßnahmen im Lebenszyklus A-CP

Der A-CP soll für ihre Aufgaben vertrauenswürdige IT-Systeme und Software einsetzen, die durch geeignete Maßnahmen wirksam gegen unautorisierte Veränderungen geschützt sind (Details siehe [A-CP PS]).

6.6.3 Technische Maßnahmen im Lebenszyklus A-CIA

Die A-CIA soll für ihre Aufgaben im Rahmen der Kartenausgabe vertrauenswürdige IT-Systeme und Software einsetzen, die durch geeignete Maßnahmen wirksam gegen unautorisierte Veränderungen geschützt sind (Details siehe [A-CIA PS]).

6.7 Maßnahmen für Netzwerksicherheit

Die von der A-MSCA, dem A-CP und der A-CIA eingesetzten Netzwerke und die dort gespeicherten und verarbeiteten Daten sind durch besondere Schutzmechanismen (wie z. B. Firewalls) gegen externe Zugriffe (insbesondere Zugriffe aus dem Internet) zu schützen.

Werden sensible Daten über ungesicherte Netzwerke übertragen, müssen diese bei der Übertragung geschützt werden.

6.8 Zeitstempel

Logdaten, welche für das Audit relevant sind, werden mit Datum und Zeitangabe versehen.

7 Profile von Zertifikaten, Widerrufslisten und OCSP-Signer-Zertifikaten

7.1 Zertifikatsprofil

Inhalte und Formate der von der A-MSCA erstellten Zertifikate entsprechen den Anforderungen aus [Annex 1B] und [Annex 1C]. Die A-MSCA signiert die von ihr erstellten Zertifikate

- EQT.C mit ihrem privaten Signaturschlüssel MS.SK und
- Card_MA.C und Card_Sign.C mit ihrem privaten Signaturschlüssel MSCA_Card.SK.

7.2 CRL Profile

Es werden keine CRLs verwendet. Zertifikatsinformationen (und Statusinformationen über Kontrollgerätekarten/Fahrtenschreiberkarten) können über das ZKR abgefragt werden.

7.3 OCSP Profile

Es wird kein OCSP Service verwendet.

8 Konformitätsprüfungen

8.1 Konformitätsprüfungen A-MSCA

Die A-MSA stellt die Durchführung von regelmäßigen und anlassbezogenen unabhängigen Überprüfungen des Betriebs der A-MSCA sicher. Jede dieser Überprüfungen hat entsprechend [ERCA Policy Gen 1] und [ERCA Policy Gen 2] zu erfolgen.

8.1.1 Häufigkeit und Umstände der Prüfungen A-MSCA

Die Einhaltung der Sicherheitsvorschriften, insbesondere dieser A-MSA Policy sind durch zumindest zweijährliche Audits durch die A-MSA nachzuweisen.

Anlassbezogene Audits im Zusammenhang mit den unter Abschnitt 1 Einleitung genannten Bestimmungen können jederzeit von der A-MSA verlangt werden.

Vor der Betriebsaufnahme und innerhalb von 12 Monaten nach der Betriebsaufnahme der A-MSCA wird ein Audit durchgeführt, um die Übereinstimmung des Betriebs mit den Vorgaben dieser A-MSA Policy zu prüfen.

Stellt ein Audit keine Anhaltspunkte für eine Nichtkonformität fest, ist das nächste Audit innerhalb von 24 Monaten durchzuführen. Wenn ein Audit Nichtkonformität aufzeigt, muss innerhalb von 12 Monaten ein Folgeaudit durchgeführt werden, um zu überprüfen, ob die Nichtkonformitäten behoben wurden.

8.1.2 Identität und Qualifikation der Prüfstelle A-MSCA

Die A-MSA kann die Audits selbst durchführen oder externe Dienstleister mit der Aufgabe als externe Prüfstelle betrauen.

8.1.3 Verhältnis von Prüfer zu Überprüftem A-MSCA

Der Prüfer muss unabhängig und nicht mit der Organisation verbunden sein, die Gegenstand der Prüfung ist.

8.1.4 Inhalt der Prüfungen A-MSCA

Bei Überprüfungen des A-MSCA-Betriebs muss insbesondere die Übereinstimmung des laufenden Betriebs mit den relevanten Rechtsvorschriften, mit dieser A-MSA Policy sowie mit dem aktuellen IT-Sicherheitskonzept verifiziert werden.

Die A-MSA stellt sicher, dass die Sicherheit des Betriebs der A-MSCA durch die Überprüfungen nicht beeinträchtigt wird. Insbesondere stellt sie sicher, dass die Ergebnisse der Überprüfungen Unbefugten nicht zugänglich gemacht werden.

Das Sicherheitsaudit beinhaltet insbesondere die folgenden Punkte:

- Sicherheitsmanagement
- Externe/bauliche Sicherheit
- Zugangsregelungen
- Produktionsprozesse, Infrastruktur, Tresor
- Prüfung der sicherheitsrelevanten Dokumentationen und Protokolle

8.1.5 Beseitigung von Mängeln A-MSCA

Sofern Überprüfungen der A-MSCA Schwachstellen oder Abweichungen offen gelegt haben, veranlasst die A-MSA die A-MSCA, diese zu beseitigen. Der Audit-Bericht muss dabei die nötigen Maßnahmen zur Korrektur der Abweichungen und einen Zeitplan zu deren

Umsetzung enthalten. Die A-MSCA berichtet der A-MSA unverzüglich über Einleitung und Abschluss dieser Maßnahmen. Die A-MSA kann eine unabhängige Überprüfung des Erfolgs dieser Maßnahmen anordnen.

8.1.6 Veröffentlichung der Prüfergebnisse A-MSCA

Eine Veröffentlichung der Prüfergebnisse außerhalb des Digital Tachograph Systems ist nicht vorgesehen.

Eine Zusammenfassung des Audit-Berichts wird von der A-MSA der ERCA in Englisch zur Verfügung gestellt.

8.2 Konformitätsprüfungen A-CP

Der A-CP gestattet Sicherheitsaudits hinsichtlich seines Sicherheitskonzeptes durch die A-MSA oder durch eine dritte Partei im Auftrag der A-MSA. Eine Überprüfung hat entsprechend [ERCA Policy Gen 1] und [ERCA Policy Gen 2] zu erfolgen.

8.2.1 Häufigkeit und Umstände der Prüfungen A-CP

Sicherheitsaudits des A-CP erfolgen auf Anfrage der A-MSA mit einer Ankündigungsfrist von 5 Werktagen. Der A-CP hat im Rahmen der Sicherheitsaudits den mit dem Audit beauftragten Personen sämtliche Dokumente, insbesondere Protokolle gemäß Abschnitt 5.3.4 Überwachung/Protokollierung A-CP, vorzulegen und sämtliche für das Audit notwendige oder nützliche Auskünfte zu erteilen.

Vor der Betriebsaufnahme des A-CP wird ein Audit durchgeführt, um die Übereinstimmung des Betriebs mit den Vorgaben dieser A-MSA Policy zu prüfen. Nach der Inbetriebnahme haben regelmäßige Audits stattzufinden, jedoch maximal ein geplanter Audit pro Jahr.

8.2.2 Identität und Qualifikation der Prüfstelle A-CP

Die A-MSA kann die Audits selbst durchführen oder geeignete externe Dienstleister mit der Aufgabe als externe Prüfstelle betrauen. Es können auch Audits, Nachweise und Zertifikate anderer Prüfstellen anerkannt werden. Dies liegt im Ermessen der A-MSA.

8.2.3 Verhältnis von Prüfer zu Überprüftem A-CP

Der Prüfer muss unabhängig und nicht mit der Organisation verbunden sein, die Gegenstand der Prüfung ist.

8.2.4 Inhalt der Prüfungen A-CP

Bei Überprüfungen des A-CP-Betriebs muss insbesondere die Übereinstimmung des laufenden Betriebs mit den relevanten Rechtsvorschriften, mit dieser A-MSA Policy sowie mit dem aktuellen IT-Sicherheitskonzept verifiziert werden.

Die A-MSA stellt sicher, dass die logische und physische Sicherheit, sowie A-CP interne Sicherheitsrichtlinien (z.B. sichere Produktionsumgebung, Datenschutz, etc.) durch die Überprüfungen nicht beeinträchtigt werden. Insbesondere stellt sie sicher, dass die Ergebnisse der Überprüfungen Unbefugten nicht zugänglich gemacht werden.

Die einzelnen zu überprüfenden Punkte (Zugangsregelungen, etc.) ergeben sich aus der entsprechenden Norm [ISO 27001] sowie den bestehenden PCI Richtlinien für Kartenproduktion und Personalisierung dessen.

8.2.5 Beseitigung von Mängeln A-CP

Werden Sicherheitslücken im Zuge des Audits des A-CP identifiziert, so ist das weitere Vorgehen mit der A-MSA zu beschließen. Erkannte Sicherheitslücken sind innerhalb einer gemeinsam vereinbarten Zeit zu schließen. Dies beinhaltet die durchzuführenden Modifikationen und den Zeitrahmen, in dem die Änderungen eingebracht werden sollen. Die Änderungen sind durch den A-CP zu dokumentieren.

8.2.6 Veröffentlichung der Prüfergebnisse A-CP

Eine Veröffentlichung der Prüfergebnisse außerhalb des Digital Tachograph Systems ist nicht vorgesehen.

Eine Zusammenfassung des Audit-Berichts wird von der A-MSA der ERCA in Englisch zur Verfügung gestellt.

8.3 Konformitätsprüfungen A-CIA

8.3.1 Häufigkeit und Umstände der Prüfungen A-CIA

Es sind regelmäßige Audits der A-CIA gemäß eines definierten und von der A-MSA genehmigten Auditplanes durchzuführen. Ein Audit gemäß [ISO 27001] entspricht den vorgenannten Anforderungen. Eine Überprüfung hat entsprechend [ERCA Policy Gen 1] und [ERCA Policy Gen 2] in der jeweils aktuell geltenden Fassung zu erfolgen.

8.3.2 Identität und Qualifikation der Prüfstelle A-CIA

Die A-MSA kann die Audits selbst durchführen oder externe Dienstleister mit der Aufgabe als externe Prüfstelle betrauen.

8.3.3 Verhältnis von Prüfer zu Überprüftem A-CIA

Die Prüfer/Auditoren dürfen nicht in die Entwicklung, Implementierung oder das operative Management der A-CIA involviert sein.

8.3.4 Inhalt der Prüfungen A-CIA

Bei Überprüfungen des A-CIA-Betriebs muss insbesondere die Übereinstimmung des laufenden Betriebs mit den relevanten Rechtsvorschriften, mit dieser A-MSA Policy sowie mit dem aktuellen IT-Sicherheitskonzept verifiziert werden.

Die A-MSA stellt sicher, dass die Sicherheit des Betriebs der A-CIA durch die Überprüfungen nicht beeinträchtigt wird. Insbesondere stellt sie sicher, dass die Ergebnisse der Überprüfungen Unbefugten nicht zugänglich gemacht werden.

8.3.5 Beseitigung von Mängeln A-CIA

Sofern Überprüfungen der A-CIA Schwachstellen oder Abweichungen offen gelegt haben, veranlasst die A-MSA die A-CIA, diese zu beseitigen. Der Audit-Bericht muss dabei die nötigen Maßnahmen zur Korrektur der Abweichungen und einen Zeitplan zu deren Umsetzung enthalten. Der A-CIA berichtet der A-MSA unverzüglich über Einleitung und Abschluss dieser Maßnahmen. Die A-MSA kann eine unabhängige Überprüfung des Erfolgs dieser Maßnahmen anordnen.

8.3.6 Veröffentlichung der Prüfergebnisse A-CIA

Eine Veröffentlichung der Prüfergebnisse außerhalb des Digital Tachograph Systems ist nicht vorgesehen.

Eine Zusammenfassung des Audit-Berichts wird von der A-MSA der ERCA in Englisch zur Verfügung gestellt.

9 Sonstige geschäftliche und rechtliche Regelungen

9.1 Gebühren

Keine Angaben.

9.2 Finanzielle Verantwortung

Keine Angaben.

9.3 Vertraulichkeit von Geschäftsinformationen

Die Rechtsgrundlage für die Vertraulichkeit der Daten ist

- die Verordnung [VO (EU) Nr. 2016/679] und
- das [DSG] idgF

zum Schutz von Einzelpersonen bezüglich der Verarbeitung von personenbezogenen Daten und deren Weiterleitung.

Alle Informationen sind vertraulich zu behandeln, ausgenommen

- Zertifikate
- Informationen zur Identifizierung des Kartenantragstellers und andere persönliche oder firmenspezifische Informationen auf Kontrollgerätekarten/Fahrtenschreiberkarten und Zertifikaten, außer andere Gesetze oder Vereinbarungen entbinden davon.

Mitprotokollierte Daten dürfen nur dann als Ganzes zur Verfügung gestellt werden, wenn dies vom Gesetz gefordert ist.

9.4 Schutz personenbezogener Daten

Die Verwendung von personenbezogenen Daten erfolgt unter Einhaltung der datenschutzrechtlichen Rahmenbedingungen (siehe Abschnitt 9.3 Vertraulichkeit von Geschäftsinformationen).

9.5 Schutz- und Urheberrechte

Keine Angaben.

9.6 Zusicherungen und Verpflichtungen

Die A-MSA, die A-MSCA, der A-CP und die A-CIA operieren nach [ERCA Policy Gen 1], [ERCA Policy Gen 2], dieser A-MSA Policy und den jeweils zutreffenden Practice Statements [A-MSCA PS], [A-CP PS] und [A-CIA PS].

9.7 Haftungsausschlüsse

Die A-MSA lehnt jegliche Gewährleistungen und Verpflichtungen jeder Art ab, einschließlich der Gewährleistung der Marktgängigkeit, der Gewährleistung der Eignung für einen bestimmten Zweck und der Gewährleistung der Richtigkeit der bereitgestellten

Informationen (ausgenommen, dass sie von einer autorisierten Quelle stammt) sowie Haftung für Fahrlässigkeit und Mangel an angemessener Sorgfalt der Kartenantragsteller und vertrauenden Parteien.

Im Rahmen dieser A-MSA Policy werden folgende Regelungen getroffen:

- Die A-MSCA, der A-CP und die A-CIA haften nicht gegenüber dem Kartenantragsteller, nur gegenüber der A-MSA.
- Kontrollgerätekarten/Fahrtenschreiberkarten, Schlüssel und Zertifikate sind nur zur Verwendung innerhalb des Digital Tachograph Systems zugelassen. Jede Veränderung der Kontrollgerätekarte/Fahrtenschreiberkarte (z.B. Aufbringen von zusätzlichen Schlüsseln, Zertifikaten oder anderen Daten) verletzt diese A-MSA Policy und keine beteiligte Organisation haftet für dadurch entstandene Schäden. Die Kontrollgerätekarte/Fahrtenschreiberkarte verliert in diesem Fall ihre Gültigkeit.

9.8 Haftungsbeschränkungen

Die A-MSA haftet nicht für Verluste

- der Services aufgrund von Krieg, Naturkatastrophen oder anderen unkontrollierbaren Kräften;
- aufgrund der unbefugten Verwendung von Zertifikaten, die von der A-MSCA ausgestellt wurden, und der Verwendung von Zertifikaten, die über die in dieser A-MSA Policy und des [A-MSCA PS] definierte Verwendung hinausgehen;
- durch betrügerische oder fahrlässige Verwendung von Zertifikaten und/oder Zertifikatsstatusinformationen, die von der A-MSCA ausgestellt wurden.

Die A-MSA übernimmt keinerlei Haftung für jegliche Art von Schadensersatz oder sonstige Ansprüche oder Verpflichtungen jeglicher Art, die sich aus unerlaubter Handlung, ungültigen Verträgen oder anderen Gründen in Bezug auf Dienstleistungen ergeben, die mit der Ausstellung, Verwendung oder Nutzung von von der A-MSCA ausgestellten Zertifikaten oder den zugehörigen Schlüsselpaaren, welche von einem Kartenantragsteller verwendet wird, ausgehen.

9.9 Schadenersatz

Keine Angaben.

9.10 Inkrafttreten und Beendigung der Gültigkeit

Diese Version dieser A-MSA Policy tritt abhängig vom jeweiligen Kartentyp mit dem Zeitpunkt der Umstellung auf Kontrollgerätekarten/Fahrtenschreiberkarten der zweiten Generation in Kraft.

Die Wahrnehmung der Rolle der A-MSCA durch das BRZ ist in §102c des [KFG] geregelt.

Die Gültigkeit dieser A-MSA Policy endet, wenn die A-MSA ihre Tätigkeit einstellt oder wenn die A-MSA ankündigt, dass diese A-MSA Policy nicht mehr gültig ist, z.B. weil eine neue Version dieser A-MSA Policy wirksam wird.

Bevor die Tätigkeit der A-MSCA, des A-CP und/oder der A-CIA beendet werden kann, muss von der A-MSA gewährleistet sein, dass:

- alle an der Umsetzung dieser A-MSA Policy beteiligten Organisationen über das Betriebsende informiert werden

- die A-MSCA, der A-CP und/oder die A-CIA sicherstellen, dass die im Betrieb notwendigen Daten an die A-MSA übergeben werden oder Vereinbarungen getroffen werden, dass der Zugriff auf die Daten auch weiterhin möglich ist

Die A-MSA entscheidet über eine Verlegung der Verantwortlichkeit der A-MSCA, des A-CP und/oder der A-CIA. Dafür muss die A-MSA eine neue A-MSCA, einen neuen A-CP und/oder eine neue A-CIA benennen. Um diese Verlegung durchzuführen, müssen die folgenden Punkte erfüllt werden:

1. Die A-MSA stellt sicher, dass die Übertragung der Aufgaben und Pflichten an die neue A-MSCA, den neuen A-CP und/oder die neue A-CIA in geeigneter Art und Weise erfolgt.
2. Die alte A-MSCA und/oder der alte A-CP müssen alle vorhandenen Schlüssel der A-MSCA an die neue A-MSCA und/oder den neuen A-CP übertragen. Die Art und Weise wird durch die A-MSA bestimmt.
3. Kopien von Schlüsseln jeglicher Art, die in Zusammenhang mit der alten A-MSCA und/oder dem alten A-CP gebracht werden können oder nicht transferiert werden konnten, müssen vernichtet werden.

Bei Einstellung des Betriebs vernichten die A-MSCA und der A-CP auf sichere Weise alle Kopien eines in ihrem Besitz befindlichen Master Keys.

9.11 Individuelle Benachrichtigungen und Kommunikation

Keine Angaben.

9.12 Änderungen der A-MSA Policy

Aktuelle und früher gültige A-MSA Policies und die dazugehörigen Practice Statements sind aufzubewahren.

Änderungen mit signifikanten Auswirkungen müssen mindestens 60 Tage vor Inkrafttreten bekannt gemacht werden.

Änderungen ohne signifikante Auswirkungen müssen mindestens 30 Tage vor Inkrafttreten bekannt gemacht werden.

Betroffene Kartenantragsteller können innerhalb von 15 Tagen Kommentare zu den Änderungen abgeben.

Wird die Änderung durch einen abgegebenen Kommentar abgeändert, so ist dies 30 Tage vor Inkrafttreten der Änderung anzukünden.

Informationen über Änderungen dieser Politik sind an die ERCA, die A-MSCA, den A-CP und die A-CIA weiterzuleiten.

Hat eine Änderung der A-MSA Policy signifikante Auswirkungen auf einen großen Teil der Benutzer, hat die A-MSA die geänderte A-MSA Policy der Kommission zur Bestätigung vorzulegen.

Die einzigen Änderungen die nicht bekannt zu machen sind, sind:

- textliche Änderungen ohne Auswirkung auf den Inhalt
- Änderungen der Kontaktinformationen

9.13 Regelungen zur Schlichtung von Streitfällen

Beschwerden, die sich auf die Einhaltung oder Umsetzung von Bestimmungen dieser A-MSA Policy beziehen, können schriftlich an die A-MSA gerichtet werden (siehe Abschnitt 1.5 Verwaltung der A-MSA Policy).

Die A-MSA wird eine solche Beschwerde innerhalb angemessener Zeit prüfen und versuchen, eine für beide Seiten zufriedenstellende Lösung zu finden.

9.14 Gerichtsstand

Es gilt ausschließlich österreichisches Recht, ausgenommen Verweisungsnormen des IPRG. Die Anwendung des UN-Kaufrechts ist ausgeschlossen. Für Streitigkeiten zwischen A-MSA, A-MSCA, A-CP, A-CIA und einem Unternehmer wird das dem Streitwert nach zuständige Gericht für Handelssachen in Wien ausschließlich für zuständig erklärt.

9.15 Einhaltung geltenden Rechts

Es gelten die relevanten europäischen und nationalen Gesetze und Vorschriften in der aktuellen Fassung; insbesondere das [KFG].

Die Fassung dieses Dokuments in deutscher Sprache ist die einzig Rechtsverbindliche.

Die A-MSCA und die gegebenenfalls von ihr beauftragten externen Dienstleister erfüllen ihre Aufgaben im Einklang mit geltendem Recht (siehe [KFG]). Die in diesem Abschnitt genannten Rechtsvorschriften erheben keinen Anspruch auf Vollständigkeit.

Alle während des Betriebs der A-MSA anfallenden personenbezogenen Daten werden im Sinne der Verordnung [VO (EU) Nr. 2016/679] und des [DSG] idgF behandelt.

Bezüglich der zu beachtenden Vorgaben und Regelungen ist im Fall von Widersprüchen folgende Reihenfolge einzuhalten:

1. gesetzliche Vorgaben und anwendbare Rechtsvorschriften sind
    a. die Verordnungen [VO (EU) Nr. 165/2014] idgF und [VO (EG) Nr. 561/2006]
    b. die [Richtlinie 2006/22 (EG)]
    c. das [KFG] und die auf Basis des [KFG] erlassenen Verordnungen
2. die jeweils aktuell gültige A-MSA Policy
3. das jeweils aktuell gültige Practice Statement der betroffenen Organisation

9.16 Sonstige Bestimmungen

Keine Angaben.