VOLKSWAGEN

AKTIENGESELLSCHAFT

Volkswagen Public Key Infrastructure

- Certificate Policy für die Volkswagen PKI -

Version 1.0.2

Document Properties	
Project	Volkswagen Public Key Infrastructure
Sub-Project	Documentation
Document	Certificate Policy für die Volkswagen PKI
Chapter	
Document-ID	1.3.6.1.4.1.3210.1883.20.1.1.2.1.1.1.0
Author	Uwe-Jens Hofmann (VW), Jan-Patrick Feige (VW), Henning Boost (Computacenter), Matthias Aevermann (Computacenter)
OrgUnit	K-SIS-O
Version	1.0.2
Status	Publiziert
Date	2014-12-12
Classification	Öffentlich

Document – Distribution		
Name	Company	Department
Hofmann, Uwe-Jens	Volkswagen AG	K-SIS-O
Jan-Patrick Feige	Volkswagen AG	K-SIS-O

Change – History			
	Date	Author	Remarks
0.9.7	01.12.2010	Henning Boost	First Draft
0.9.8	16.11.2011	Matthias Aevermann	Überarbeitung
0.9.9	24.02.2012	Uwe-Jens Hofmann Jan-Patrick Feige	Überprüfung / Qualitätssicherung / Anpassungen
1.0.0	29.10.2013	Uwe-Jens Hofmann	Aktualisierung OE-Bezeichnungen
1.0.1	28.11.2013	Uwe-Jens Hofmann	diverse Überarbeitungen
1.0.2	02.12.2013	Uwe-Jens Hofmann	**TYP_INTERN** eingeführt
1.0.2	02.12.2013	Michael Liebe	Review
1.0.2	31.01.2014	Uwe-Jens Hofmann	Ergänzung unter 6.1.5 und Fehlerkorrekturen

Inhalt

Vorbemerkungen:

Wenn diese CP in einer Sprache geschrieben ist, in der Funktionsbezeichnungen für männliche und weibliche Personen unterschiedlich sind, dann schließen die verwendeten Bezeichnungen für das eine Geschlecht Personen des anderen Geschlechts mit ein.

1 EINLEITUNG

1.1 Überblick

Die Volkswagen AG betreibt eine eigene Public Key Infrastructure (PKI), die für Personen und IT-Komponenten Zertifikate erstellen kann („Volkswagen PKI“). Innerhalb dieser PKI gibt es verschiedene Zertifizierungsstellen (engl.: Certificate Authorities, CAs).

Die hier vorliegende Zertifikatsrichtlinie (engl. Certificate Policy, CP) richtet sich an alle Teilnehmer der Public Key Infrastruktur (PKI) der Volkswagen AG und an die Betreiber einzelner CAs dieser PKI. Sie enthält Vorgaben und Anforderungen an die PKI sowie an die zum Einsatz kommenden Zertifikate.

Eine Spezifikation der Umsetzung der hier vorliegenden CP muss im Rahmen eines separaten, CA-spezifischen Certification Practice Statements (CPS) erfolgen.

1.1.1 Ziel der Richtlinie

Die in diesem Dokument aufgeführten Regelungen unterstützen das Ziel der Volkswagen AG, mit Hilfe der Volkswagen PKI sichere, organisationsübergreifende, elektronische Geschäftsprozesse zu realisieren. Diese Richtlinie kann zudem der Darstellung des Sicherheitsstandards der Volkswagen PKI gegenüber Dritten (i.d.R. Partner) dienen.

1.1.2 Zertifikatstypen

Innerhalb dieser CP werden 5 Zertifikatstypen unterschieden: **TYP_CA**, **TYP_INTERN**, **TYP_PERSON**, **TYP_MASCHINE** und **TYP_PROZESS**.

- Unter **TYP_CA** fallen alle Zertifikate, mit denen weitere Zertifikate oder Sperrlisten signiert werden.
- Unter **TYP_INTERN** fallen alle Zertifikate, die für das sichere Zusammenspiel der zentralen Software- und Hardware-Komponenten und für den Betrieb der Volkswagen PKI benötigt werden.
- Unter **TYP_PERSON** fallen alle Zertifikate, denen eine natürliche Person als Zertifikatsnehmer eindeutig zuzuordnen ist.
- Unter **TYP_MASCHINE** fallen alle Zertifikate, die einem technischen Gerät eindeutig zuzuordnen sind.

- Unter **TYP_PROZESS** fallen alle Zertifikate, die technischen Accounts, Org.-Einheiten, technischen Verfahren oder IT-Anwendungen zuzuordnen sind.

Alle Regelungen in dieser Zertifizierungsrichtlinie (CP) gelten gleichermaßen für alle genannten Zertifikatstypen, soweit eine Regelung für diese relevant ist. Gilt eine Regelung nur für einen bestimmten Zertifikatstyp, wird dieses zu Beginn der Regelung entsprechend gekennzeichnet.

1.1.3 Struktur des Dokuments

Die Struktur dieses Dokuments orientiert sich an der Struktur des RFC 3647 und enthält u.a. die darin aufgeführten Gliederungspunkte.

1.1.4 Konventionen / Nomenklatur

Bei der Formulierung einzelnen Regelungen dieser Richtlinie werden bei Bedarf die Begriffe „**MUSS**“, „**DARF NUR**“**,** „**DARF NICHT**“, „**SOLL**“, „**SOLL NICHT**“, „**KANN**“ und „**BRAUCHT NICHT**“ in vollständiger Großschreibung verwendet. Deren Bedeutung ist wie folgt geregelt:

- „MUSS“ / „DARF NUR“ / „DARF NICHT“: verbindliche Vorgabe
- „SOLL“ / „SOLL NICHT“: Vorgabe, Nichteinhaltung nur in begründeten Ausnahmefällen
- „KANN“ / „BRAUCHT NICHT“: optional

1.1.5 Gültigkeit

Diese Richtlinie besitzt Gültigkeit für die Root-CA (VW-CA-ROOT-*nn*) der Volkswagen PKI und aller Zertifizierungsstellen, die mittel- oder unmittelbar der Root-CA untergeordnet sind.

Sie ist somit gültig für die Volkswagen AG und alle Tochterunternehmen und Beteiligungsgesellschaften, sobald diese eine entsprechende CA oder eine Registrierungsstelle (engl.: Registration Authority, RA) für eine dieser CAs betreiben.

Diese Richtlinie gilt nicht für Test- und Entwicklungsumgebungen der Volkswagen PKI, wenn diese vollständig vom Produktivsystem isoliert sind.

1.2 Dokumentenname und Identifikation

Diese Richtlinie ist folgendermaßen identifiziert:

- Dokumentenname: Certificate Policy für die Volkswagen PKI

- Object Identifier (OID): 1.3.6.1.4.1.3210.1883.20.1.1.2.1.1.1.0
- Version: 1.0.2

1.3 PKI Teilnehmer

1.3.1 Zertifizierungsstellen (CA)

Zertifizierungsstellen der Volkswagen PKI stellen Zertifikate sowie Sperrlisten aus. Übergangsweise kann es auch CAs geben, die noch keine Zertifikate oder Sperrlisten ausgestellt haben.

Die Volkswagen Public Key Infrastruktur (PKI) besteht aus einer zentralen Wurzelzertifizierungsstelle (VW-CA-ROOT-nn) und verschiedenen weiteren CAs, die unterschiedliche Sicherheitsniveaus und Zertifikatstypen bedienen.

Die Wurzelzertifizierungsstelle (VW-CA-ROOT-nn) stellt ausschließlich Zertifikate für unmittelbar nachgeordneten CAs sowie Zertifikate des Typs **TYP_INTERN** entsprechend dieser Certificate Policy (CP) und ihrem Certification Practice Statement (CPS) aus. Nähere Informationen zu einer einzelnen CA sind ihrem jeweiligen CPS zu entnehmen.

Die jeweils gültige Abbildung der CA-Hierarchie findet sich in der Anlage 1 [A1].

1.3.2 Registrierungsstellen (RA)

Registrierungsstellen führen die Prüfung von Zertifikatsanträgen eines Zertifikatsnehmers einer CA durch. RAs der Volkswagen PKI werden durch eine Gesellschaft der Volkswagen AG betrieben und **SOLLEN** nur Personal einer Gesellschaft der Volkswagen AG einsetzen. RAs **KÖNNEN** auf unterschiedliche Zertifikatstypen und auf unterschiedliche Aufgaben bei der Zertifikatserstellung spezialisiert sein.
Es **KANN** auch automatisierte RAs ohne Personal geben. Für solche automatisierten RAs **MUSS** dokumentiert sein, unter welchen Rahmenbedingungen welche Zertifikatstypen erstellt werden.

1.3.3 Zertifikatsnehmer (Zertifikatsinhaber)

Zertifikatsnehmer der Volkswagen PKI sind CAs (**TYP_CA**), interne Komponenten der Volkswagen-PKI (**TYP_INTERN**), natürliche Personen (**TYP_PERSON**), Geräte (**TYP_MASCHINE**) oder technische Accounts und Prozesse (**TYP_PROZESS**) für die ein Zertifikat durch die Volkswagen PKI ausgestellt wird (siehe dazu auch Abschnitt 1.1.2).

[**TYP_INTERN**]: Die Software-Produkte der PKI-Anwendung geben vor, für welche internen Zertifikatsnehmer und mit welchen Parametern die Zertifikate zu erstellen sind. Diese Zertifikate werden im Rahmen der Software-Betreuung eingerichtet.

[**TYP_PERSON**]: Es **SOLLEN** nur solche Personen ein Zertifikat der Volkswagen PKI erhalten, deren dafür benötigte Informationen vollständig im Volkswagen Corporate Directory (VCD) enthalten sind.

[**TYP_MASCHINE**]: Zertifikatsnehmer **MÜSSEN** Geräte der Volkswagen AG sein oder in ihrem Sinne betrieben werden.

[**TYP_PROZESS**]: Zertifikatsnehmer **MÜSSEN** Instanzen der Volkswagen AG sein oder in ihrem Sinne agieren. Bei der Beantragung für Zertifikate vom **TYP_PROZESS MUSS** eine Person oder Funktion als Ansprechpartner angegeben werden.

1.3.4 Zertifikatsnutzer

Zertifikatsnutzer sind alle Personen und Organisationen, die Zertifikate von Zertifikatsnehmern (siehe Abschnitt 1.3.3) nutzen wollen.

1.3.5 Andere Teilnehmer

Zertifikatsnehmer, die keine Verpflichtungen im Rahmen dieser CP eingehen, sind nicht Bestandteil dieser Richtlinie und werden nicht betrachtet.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendung von Zertifikaten

Zertifikate der Volkswagen PKI **DÜRFEN NUR** im Sinne der im Attribut „**KeyUsage**“ gemäß RFC 5280 eingetragenen Schlüsselverwendungen genutzt werden. Soweit Angaben im Attribut „**ExtendedKeyUsage**“ gemacht werden, sind diese ebenfalls maßgeblich.

Mögliche Attribute eines Zertifikats sind im CPS der ausstellenden CA dokumentiert.

[**TYP_CA**]: CA-Zertifikate **DÜRFEN NUR** in Übereinstimmung mit ihren Erweiterungen „**BasicContraints**“ (Basiseinschränkungen) und „**PathLengthConstraint**“ (Einschränkung der Pfadlänge) genutzt werden.

1.4.2 Untersagte Verwendung von Zertifikaten

Ein Zertifikat **DARF NUR** mit Anwendungen des Volkswagen Konzerns oder im Auftrag des Volkswagen Konzerns entsprechend der im Zertifikat festgelegten Art verwendet werden (siehe dazu Abschnitt 1.4.1).

1.5 Verwaltung der Richtlinie

1.5.1 Änderungsmanagement

Änderungen an der CP oder einem CPS durchlaufen einen abgestimmten Änderungsabstimmungsprozess. Angaben zu CP oder CPS, deren Änderungen nicht abgestimmt werden müssen, werden in der jeweiligen Anlage 1 zur CP oder zum CPS aufgeführt; diese Anlagen durchlaufen nicht den genannten Änderungsabstimmungsprozess.

1.5.2 Ansprechpartner

Die vorliegende Richtlinie wird von der Volkswagen AG als Betreiber der Volkswagen PKI herausgegeben.

Die verantwortliche Stelle innerhalb der Volkswagen AG ist in Anlage 1 [A1] aufgeführt.

1.5.3 Eignungsprüfer zur Feststellung der Regelkonformität eines CPS

Der in Abschnitt 1.5.2 als Ansprechpartner genannte Kontakt **MUSS** sicherstellen, dass jedes CPS einer CA der Volkswagen PKI in regelmäßigen Abständen hinsichtlich seiner Regelkonformität überprüft wird.

1.5.4 Verfahren zur Freigabe eines CPS

Ein CPS für eine neue CA durchläuft das Änderungsmanagement (siehe Abschnitt 1.5.1).

1.6 Begriffe und Akronyme

BasicContraints	Attribut in einem Zertifikat, welches Einschränkungen innerhalb einer PKI festlegt. Beispielsweise die Länge des Zertifizierungspfades.
BSI	Bundesamt für Sicherheit in der Informationstechnik
CDP	CRL Distribution Point: Pfad zu einem Verzeichnis, in dem die CRL einer Zertifizierungsstelle enthalten ist.
Certificate Authority (CA)	Instanz, die Zertifikate an weitere Zertifikatsnehmer ausstellt.
CERT	Computer Emergency Response Team
Certificate Policy (CP)	Richtlinie, die Anforderungen an die Funktionsweise einer PKI oder CA formuliert.
Common Name (CN)	Komponente des Distinguished Name (DN).
CPS	Certification Practice Statement: Beschreibung der Maßnahmen, um einer CP zu genügen.
CRL	Certificate Revocation List: Liste der Nummern von Zertifikaten, die von der ausgebenden CA (inzwischen) gesperrt wurden.
Distinguished Name (DN)	Ein aus mehreren Bestandteilen bestehender Bezeichner, der in Zertifikaten die ausstellende CA und den Zertifikatsnehmer eindeutig beschreibt. Der DN wird im Standard X.501 definiert.
FIPS	Federal Information Processing Standard: Bezeichnung für öffentlich bekanntgegebene Standards der USA. FIPS-140: Sicherheitsanforderungen für kryptographische Module
Hardware Security Module	IT-System zur Erzeugung und ggf. Verwahrung kryptographischen Schlüsselmaterials.
http	hypertext transfer protocol: Übertragungsprotokoll für Daten über ein Netzwerk.
HSM	siehe „Hardware Security Module“

ldap	lightweight data access protocol: Übertragungsprotokoll für Anfragen an Verzeichnisdienste bzw. deren Antworten.
ISSO	Informationssysteme-Sicherheitsorganisation: Organisationseinheit innerhalb der Volkswagen AG.
KeyUsage	Eintrag in einem Zertifikat. Gibt an, für welchen Nutzungszweck ein Zertifikat ausgestellt wurde bzw. verwendet werden darf.
PathLengthConstraint	Attribut in CA-Zertifikaten, das die maximale Anzahl erlaubter CA-Hierarchie-Ebenen unterhalb einer CA definiert.
PIN	Persönliche Identifikationsnummer (PIN-Code)
PKI	Public Key Infrastructure: bezeichnet ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann.
Public Key Infrastructure	siehe „PKI"
PUK	Personal Unblocking Key: Code zum Entsperren der Karte, falls ein PIN-Code mehrfach falsch eingegeben wurde.
OCSP	Online Certificate Status Protocol: Ein alternatives Verfahren zur Sperrstatusprüfung von Zertifikaten. Hierbei handelt es sich um ein Client-Server-Protokoll, bei dem nur geringe Datenmengen ausgetauscht werden.
RA	siehe „Registration Authority"
Registrierungsstellen	siehe „Registration Authority"
Registration Authority	Ausgabestelle für Schlüsselträger.
RFC	Requests for Comments: Bitte um Kommentierung Folge von Dokumenten mit technischen Spezifikationen, einzelne RFCs bzw. deren Inhalte können sich durch allgemeine Akzeptanz zu Standards entwickeln.
Root-CA	Oberster Vertrauensknoten im CA-Baum einer PKI. Das Zertifikat der Root-CA ist durch den eigenen privaten Schlüssel signiert (self-signed).
Schlüsselträger	Komponente, auf dem ein Zertifikat und auch der zugehörige geheime Schlüssel gespeichert sind. Der Schlüsselträger wird

	dem Zertifikatsinhaber übergeben. Schlüsselträger können Dateien (Soft-Token, Soft-PSE) oder spezielle Hardware (z.B. Smart Cards) sein.
Schlüsselverantwortlicher	Person, die für die korrekte Nutzung und Unversehrtheit des privaten Schlüssels (eines Zertifikats) verantwortlich ist. Bei Zertifikaten TYP_PERSON ist dieses der Zertifikatsnehmer, bei allen anderen Zertifikaten der technische Verantwortliche oder Kostenstellenverantwortliche, für dessen Verantwortungsbereich ein Zertifikat erzeugt wird.
Security Officer	Verantwortliche Rolle zum Umsetzung von Sicherheitsmaßnahmen innerhalb einer IT-Infrastruktur z.B. einer PKI.
SO	siehe „Security Officer"
Soft-PSE	Software Personal Security Environment: Eine Datei, die einen privaten Schlüssel sowie das zugehörige Zertifikat und den öffentlichen Schlüssel enthält.
Soft-Token	siehe Soft-PSE
Sub-CA	CA, die einer anderen CA untergeordnet ist. Das Zertifikat einer Sub-CA ist von der übergeordneten CA signiert.
technische Zertifikate	Zertifikate der Typen (**TYP_CA**), (**TYP_INTERN**), (**TYP_GERÄT**) oder (**TYP_PROZESS**).
VCD	Volkswagen Corporate Directory: zentraler Verzeichnisdienst des Volkswagen Konzerns für definierte personenbezogene Daten.
Wurzelzertifizierungsstelle	siehe „Root-CA"
Zertifikatserneuerung	Neuerstellung eines bereits vorhandenen Zertifikats unter Nutzung des bereits zuvor verwendeten Schlüsselpaares.
Zertifikatsnehmer	Die Person oder die technische Entität, für die ein Zertifikat ausgestellt. Für jedes technische Zertifikat **MUSS** eine verantwortliche Person oder Funktionsstelle festgelegt werden,

	die die Rechte, die Pflichten und die Kommunikation des Zertifikatsnehmers übernimmt.
Zertifikatsnutzer	Die Stelle, der der Zertifikatsnehmer ein Zertifikat zur Verfügung stellt, damit es für eine kryptographische Verarbeitung verwendet werden kann (z.B. für Verschlüsselung oder Signaturprüfung).
Zertifizierungsstelle	siehe „CA“

2 VERANTWORTLICHKEITEN FÜR VERZEICHNISSE UND VERÖFFENTLICHUNGEN

2.1 Verzeichnisse

Verzeichnisse, die Zertifikatsinformationen (auch Sperrinformationen) vorhalten, **SOLLEN** 24 Stunden an 7 Wochentagen zur Verfügung stehen.

Die maximal zulässige Dauer einer Nichtverfügbarkeit eines Verzeichnisses ist im CPS einer CA spezifiziert.

Wird ein Zertifikat veröffentlicht, **SOLL** die Veröffentlichung mindestens bis zum Ende der zeitlichen Gültigkeit des Zertifikats erfolgen.

[**TYP_PERSON**]: Wenn sich Zertifikatsnutzer (siehe Abschnitt 1.3.4) außerhalb der Volkswagen AG befinden, **KANN** ein von außerhalb der Volkswagen AG zugreifbarer Verzeichnisdienst für personenbezogene Zertifikate bereitgestellt werden. Entsprechendes gilt für einen Zugriff auf die korrespondierenden Sperrlisten. Die entsprechenden Mechanismen sind dann im CPS der jeweiligen CA spezifiziert.

Zertifikate von Zertifikatsnehmern der Volkswagen PKI **DÜRFEN NUR** außerhalb der Volkswagen AG zugänglich gemacht werden, wenn dazu eine Einwilligung des Zertifikatsnehmers vorliegt.

[**TYP_MASCHINE, TYP_INTERN**]: Zertifikate dieser Typen **KÖNNEN** innerhalb der Volkswagen AG veröffentlicht werden, wenn der Antragsteller einer Veröffentlichung zustimmt. Die Zustimmung für eine Veröffentlichung **KANN** als Voraussetzung für eine Ausstellung definiert werden.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

Informationen zur Zertifikatserstellung in Form der hier vorliegenden CP sind innerhalb der Volkswagen AG veröffentlicht. Diese CP **KANN** auch für die Öffentlichkeit (insbesondere für Zertifikatsnutzer) zugänglich gemacht werden. Über die Art und Weise einer Veröffentlichung oder deren Unterbindung entscheidet der in Abschnitt 1.5.2 genannte Ansprechpartner.

Informationen zur Zertifikatserstellung in Form eines CPS **KÖNNEN** innerhalb der Volkswagen AG interessierten Personengruppen zugänglich gemacht werden. Eine Weitergabe eines CPS oder Teile dessen an Externe **DARF NUR** bei einem berechtigten

Interesse der Volkwagen AG erfolgen. Über die Art und Weise einer Weitergabe oder deren Unterbindung entscheidet der in Abschnitt 1.5.2 genannte Ansprechpartner.

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Zertifikatsinformationen, die Volkswagen AG-intern zugänglich sind, **SOLLEN** zeitnah nach Ausstellung eines Zertifikats aktualisiert werden.

Zertifikatsinformationen, die Volkswagen AG-extern zugänglich sind, **SOLLEN** mindestens täglich aktualisiert werden.

Sperrinformationen (unabhängig von internem oder externem Zugang) **SOLLEN** zeitnah nach Sperrung eines Zertifikats aktualisiert werden.

2.4 Zugriffskontrolle auf Verzeichnisse

Eine ausreichende Zugriffskontrolle auf Zertifikate und Sperrinformationen ist eingerichtet. Entsprechende Maßnahmen sind im CPS einer CA spezifiziert.

Werden Zertifikate und Sperrlisten für externe Zertifikatsnutzer veröffentlicht, **SOLL** eine Zugriffsbeschränkung für lesenden Zugriff erfolgen.

3 IDENTIFIKATION UND AUTHENTIFIZIERUNG

3.1 Namensregeln

3.1.1 Namensformen

Eine Namensgebung in Zertifikaten erfolgt entsprechend der Standards X.500 / RFC 822.

Die Namen für den „Subject Distinguished Name“ (Subject DN) und „Issuer Distinguished Name“ (Issuer DN) sind nach dem X.501 Standard definiert. In Subject DN und Issuer DN **MUSS** der jeweilige Common Name (CN) eingetragen sein.

3.1.2 Notwendigkeit aussagekräftiger Namen

Der verwendete Subject Distinguished Name (Subject DN) in einem Zertifikat ist eindeutig innerhalb der Volkswagen PKI.

[**TYP_PERSON, TYP_MASCHINE**]**:** Es ist erkenntlich, ob ein Zertifikat einer natürlichen Person bzw. einem Gerät zugeordnet ist.

[**TYP_CA, TYP_INTERN, TYP_MASCHINE, TYP_PROZESS**]**:** Der in den Zertifikaten benutzte Subject DN **SOLL** aussagekräftig sein.

[**TYP_CA**]: Namen von CAs der Volkswagen PKI **SOLLEN** die Form „VW-CA-<xxxx>-<nn>“ oder für CAs der Microsoft CA-Dienste „MS-CA-VWG“ für die Policy-CA und „MS-CA-<y>-01“ für CAs, deren Zertifikate von der Microsoft-Policy-CA signiert wurden, besitzen.

Dabei kennzeichnet <xxxx> den Hauptzweck der durch die CA ausgegebenen Zertifikate, <nn> eine zweistellige, fortlaufende Nummer (eventuell mit führender Null) und <y> eine Gesellschaft der Volkswagen. Namensabweichungen werden durch den in Abschnitt 1.5.2 genannten Ansprechpartner genehmigt.

3.1.3 Anonymität bzw. Pseudonymität von Zertifikatsnehmern

Ein als Pseudonym ausgestelltes Zertifikat **MUSS** als solches erkennbar sein.

Grund für die Verwendung von Pseudonymen **MUSS** die Zweckgebundenheit von Zertifikaten sein und **DARF NICHT** der Anonymisierung einzelner Personen dienen. Eine Nutzung von Pseudonymen **KANN** betreffen:

- Signatur (z. B. „Abteilung X“)
- Verschlüsselung (z. B. „info@volkswagen.de“)

- Authentisierung (z. B. „Webserver Administrator“)

Wenn Zertifikate für Pseudonyme erstellt werden, ist die reale Identität der Zertifikatsnehmer zu jedem Zeitpunkt feststellbar.

[**TYP_PROZESS**]: Solche Zertifikate **KÖNNEN** für Pseudonyme erstellt werden.

[**TYP_CA, TYP_INTERN, TYP_PERSON, TYP_MASCHINE**]**:** Solche Zertifikate **DÜRFEN NICHT** für Pseudonyme erstellt werden.

3.1.4 Regelungen zur Interpretation verschiedener Namensformen

[**TYP_PERSON**]: Ein Zertifikat, das zur sicheren E-Mail Kommunikation einsetzbar sein soll, **MUSS** die E-Mail Adresse des Zertifikatsnehmers im Attribut „**Subject Alternative Name**“ enthalten.

3.1.5 Eindeutigkeit von Namen

Es wird sichergestellt, dass ein Distinguished Name (DN), der von einer CA vergeben wird, durch diese CA eindeutig einem Zertifikatsnehmer zugeordnet ist. Die Zuordnung eines DN zu einem Zertifikatsnehmer wird auch über die Gültigkeitsdauer der Zertifikate hinaus eindeutig möglich sein.

[**TYP_CA**]: Es wird bei der Namensvergabe angestrebt werden, dass der Subject DN des CA-Zertifikats weltweit eindeutig ist.

3.1.6 Anerkennung, Authentifizierung und Funktion von Warenzeichen

Keine Vorgaben

3.2 Identitätsüberprüfung bei Erstantrag

3.2.1 Nachweis des Besitzes des privaten Schlüssels

Werden Schlüsselpaare im Verantwortungsbereich des Antragstellers produziert, **MUSS** dieser den Besitz des privaten Schlüssels nachweisen oder nachvollziehbar bestätigen.

3.2.2 Authentifizierung von Organisationen

Zertifikate, in denen Organisationen außerhalb der Volkswagen AG als Zertifikatsnehmer auftreten, **DÜRFEN NUR** dann ausgestellt werden, wenn das Zertifikat in einer Kommunikation mit dem Volkswagen Konzern oder in dessen Auftrag oder Sinn genutzt

wird. Die Authentifikation der Organisation **MUSS** durch den Kommunikationspartner oder Auftraggeber innerhalb des Volkswagen Konzerns erfolgen.

Werden Organisationen der Volkswagen AG, für die Zertifikate als Zertifikatsnehmer ausgestellt werden, aus der Volkswagen AG herausgelöst und außerhalb weiterbetrieben, werden für einen Übergangszeitraum separate Regelungen erarbeitet werden.

3.2.3 Authentifizierung natürlicher Personen

Antragssteller, die für sich oder andere Entitäten Zertifikate beantragen, **MÜSSEN** sich bei Zertifikatsbeantragung oder Zertifikatsauslieferung gegenüber der jeweiligen RA authentifizieren. Die Art und Weise der Authentifizierung ist im CPS der jeweiligen CA zu dokumentieren.

3.2.4 Nicht überprüfte Teilnehmerangaben natürlicher Personen

Keine Vorgaben

3.2.5 Überprüfung der Berechtigung

Der Prozess für die Prüfung der Berechtigung einer Antragsstellung ist dokumentiert.

[**TYP_CA**]: Sub-CAs **DÜRFEN NUR** in Abstimmung mit der für die Volkswagen PKI verantwortlichen Stelle (siehe dazu Abschnitte 1.5.2) implementiert werden. Antragsteller, die ein Zertifikat für eine Sub-CA beantragen, **MÜSSEN** nachweisen, dass der Betrieb der Sub-CA gemäß dieser CP gewährleistet ist.

[**TYP_INTERN**]: Zertifikate dieses Typs **DÜRFEN NUR** in Abstimmung mit der für die Volkswagen PKI verantwortlichen Stelle (siehe dazu Abschnitte 1.5.2) erstellt werden.

3.2.6 Kriterien zur Interoperabilität

Keine Vorgaben

3.3 Identifizierung und Authentifizierung bei Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Soweit eine Zertifikatserneuerung zulässig ist, erfolgt eine Identifizierung und Authentifizierung des Antragstellers. Dieses **KANN** auf den gleichen Verfahren wie bei einer Erstausstellung basieren oder **KANN** durch ein automatisiertes Verfahren erfolgen, welches

Informationen der Erstausstellung nutzt. Die Art und Weise ist im CPS der jeweiligen CA dokumentiert.

[**TYP_CA**]: Das Zertifikat einer Sub-CA **DARF NICHT** erneuert werden.

3.3.2 Zertifikatserneuerung nach einer Sperrung

Zertifikatserneuerungen gesperrter Zertifikate **DÜRFEN NICHT** erfolgen.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Eine zuverlässige Identifizierung und Authentifizierung des Antragstellers eines Sperrauftrags erfolgt vor einer Zertifikatssperrung. Die jeweiligen Verfahren sind im CPS einer CA definiert werden.

4 ABLAUFORGANISATION (Zertifikats-Lebenszyklus)

4.1 Zertifikatsantrag

4.1.1 Berechtigung zur Antragsstellung

[**TYP_PERSON**]: Alle natürlichen Personen, die Mitarbeiter der Volkswagen AG oder im Auftrag der Volkswagen AG tätig sind, **KÖNNEN** Zertifikate beantragen.

[**TYP_MASCHINE**]: Alle durch die Volkswagen AG oder in ihrem Sinne betriebenen Geräte **KÖNNEN** Zertifikate beantragen.

[**TYP_CA, TYP_PROZESS**]: Solche Zertifikate **KÖNNEN** beantragt werden, wenn es sich bei den Antragstellern um Instanzen der Volkswagen AG handelt oder diese in ihrem Sinne agieren.

Es gelten die in Abschnitt 3.2.5 gestellten Anforderungen.

Eine RA bzw. die dort für die Antragsgenehmigung verantwortlichen Personen **KÖNNEN** einen Antrag ablehnen. Eine Ablehnung **SOLL** begründet werden.

Siehe hierzu auch Abschnitt 4.2.2.

[TYP_INTERN]: Verantwortliche für CAs sind berechtigt, Zertifikate für die für den Betrieb ihrer jeweiligen CAs notwendigen Entitäten zu beantragen.

4.1.2 Registrierungsprozess und Zuständigkeiten

Der Registrierungsprozess ist dokumentiert. Es gelten die in Abschnitt 3.2 gestellten Anforderungen an eine Identifizierung. Der Nachweis einer korrekten Bearbeitung eines Antrags ist möglich.

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Eine Identifizierung und Authentifizierung eines Antragstellers erfolgt im Rahmen des jeweiligen Beantragungsprozesses. Dort ist auch die Art und Weise der Identifizierung und Authentifizierung dokumentiert.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Vorgaben zur Annahme eines Zertifikatsantrags sind im Rahmen der jeweiligen Beantragungsprozesse dokumentiert.

Voraussetzungen für eine Antragsannahme sind:

- Vollständige Antragsdaten
- Positives Ergebnis der Verifikation der Antragsdaten
- Positive Identitätsprüfung

Ist eine dieser Voraussetzungen nicht gegeben, **MUSS** ein Zertifikatsantrag abgelehnt werden.

Siehe hierzu auch Abschnitt 4.1.1.

[**TYP_MASCHINE, TYP_PROZESS**, **TYP_PERSON**]: Besteht die Möglichkeit eine zweifelsfreie Identifizierung des Antragstellers elektronisch vorzunehmen, **KANN** eine Zertifikatsausstellung im Rahmen eines sog. Self Service Prozesses bzw. automatisiert erfolgen.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Keine Vorgaben

4.3 Zertifikatsausstellung

4.3.1 Aktionen der Zertifizierungsstelle (CA) bei der Ausstellung von Zertifikaten

Eine Ausgabe von Zertifikaten **DARF NUR** für angenommene Zertifikatsanträge (siehe dazu Abschnitt 4.2.2) erfolgen. Die Aktionen bei der Zertifikatsausgabe erfolgen anhand eines beschriebenen Prozesses. Dabei wird sichergestellt, dass eine eindeutige Verbindung von Zertifikatsnehmer und dem zugehörigen Schlüsselpaar besteht.

4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausstellung des Zertifikats

[**TYP_PERSON**]: Soweit das Zertifikat nicht ausschließlich innerhalb gekapselter Anwendungen automatisiert genutzt wird, wird der Zertifikatsnehmer im Rahmen der Übergabe des Schlüsselträgers über die Ausstellung des Zertifikats informiert.

4.4 Zertifikatsübergabe

4.4.1 Verhalten bei der Annahme/Übergabe eines Zertifikats

Der Prozess für eine sichere Übergabe eines Zertifikates und die Bedingungen, die zu einer Annahme des Zertifikates durch den Zertifikatsnehmer führen, ist im Rahmen der jeweiligen Übergabeprozesse dokumentiert.

Der Antragsteller wird darauf hingewiesen, dass er Fehler in Zertifikaten, die für ihn ausgestellt wurden, an die für ihn zuständige RA melden **MUSS**.

4.4.2 Veröffentlichung eines Zertifikates durch die CA

Die Veröffentlichung von Zertifikaten erfolgt entsprechend dem im Abschnitt 2 dargelegten Anforderungen.

[**TYP_CA**]: Zertifikate diesen Typs werden innerhalb der Volkswagen AG veröffentlicht. Befinden sich Zertifikatsnutzer der von einer CA mittel- oder unmittelbar ausgestellten Zertifikate auch außerhalb der Volkswagen AG, erfolgt auch eine von extern zugängliche Veröffentlichung.

4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Zertifikats

Keine Vorgaben.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer (Zertifikatsinhaber)

Die Verantwortlichkeiten des Zertifikatsnehmers sind durch den Betreiber einer CA dokumentiert und werden dem Zertifikatsnehmer mitgeteilt.

Der im Zertifikat dokumentierte private Schlüssel **DARF NUR** für Anwendungen benutzt werden, die in Übereinstimmung mit den im Zertifikat angegebenen Nutzungsarten stehen.

[**TYP_PERSON, TYP_MASCHINE, TYP_PROZESS**]: Es **DÜRFEN NUR** folgende Nutzungsarten vorgesehen werden:

- Authentifizierung von Benutzer- oder Anwendungsdaten und technischen Systemen (Nutzungsart **digital signature**)

- Entschlüsselung von Benutzer- oder Anwendungsdaten oder von symmetrischen Schlüsseln, welche in dem so genannten Hybridverfahren für die Verschlüsselung solcher Daten dienen (Nutzungsarten **dataEncryption** bzw. **KeyEncryption**)
- Kennzeichnung der Verbindlichkeit (Nutzungsart **non-repudiation**/**content-commitment**) einer elektronischen Signatur durch den Zertifikatsnehmer.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch den Zertifikatsnutzer

Der Zertifikatsnutzer **MUSS** folgende Prüfungen vor Nutzung eines Zertifikates durchführen:

- Gültigkeit des genutzten Zertifikates und aller übergeordneten CAs.
- Entspricht die KeyUsage und Extended Key Usage (sofern vorhanden) des Zertifikats dem Anwendungsfall?
- Widersprechen Restriktionen im Zertifikat, in dieser CP oder in anderen vertraglichen Vereinbarungen nicht dem Anwendungsfall?
- Stammt das Zertifikat von einer CA, welche gültig ist und für diesen Verwendungszweck freigegeben ist?

4.6 Zertifikatserneuerung

4.6.1 Bedingungen für eine Zertifikatserneuerung

[**TYP_PERSON**]: Eine Zertifikatserneuerung unter Beibehaltung des asymmetrischen Schlüsselpaares **DARF NUR** erfolgen, wenn die bisher eindeutige Verbindung von Zertifikatsnehmer und privatem Schlüssel sichergestellt bleibt. Die Bedingungen für eine Zertifikatserneuerung sind dokumentiert. U.a. **MÜSSEN** die Schlüssel auf einem sicheren Träger (z.B. Smartcard) gespeichert sein und die Nutzungsberechtigung der Schlüssel nachgewiesen sein.

[**TYP_INTERN**, **TYP-MASCHINE, TYP_PROZESS**]: Solche Zertifikate **DÜRFEN NICHT** erneuert werden. Von der Volkswagen PKI wird nicht überprüft, ob mehrfach Zertifikate für dieselben Schlüssel beantragt werden.

[**TYP-CA**]: Von der Root-CA signierte CA-Zertifikate **DÜRFEN NICHT** erneuert werden. Ausgenommen von dieser Regel sind Cross-Zertifikate.

4.6.2 Berechtigung zur Beantragung einer Zertifikatserneuerung

[**TYP_PERSON**]: Eine Zertifikatserneuerung **DARF NUR** durch den Zertifikatsnehmer (Zertifikatsinhaber) der bisherigen Zertifikate beantragt werden. Die bisherigen Zertifikate **DÜRFEN NICHT** gesperrt sein.

4.6.3 Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung

[**TYP_PERSON**]: Die Bearbeitung eines Antrags auf Zertifikatserneuerung ist ein dokumentierter Prozess, der die Nutzungsberechtigung des bestehenden privaten Schlüssels voraussetzt.

4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Es gelten die Regelungen in Abschnitt 4.3.2.

4.6.5 Verhalten für die Annahme einer Zertifikatserneuerung

Es gelten die Regelungen in Abschnitt 4.4.1.

4.6.6 Veröffentlichung der Zertifikatserneuerung durch die CA

Es gelten die Regelungen in Abschnitt 4.4.2.

4.6.7 Benachrichtigung anderer PKI-Teilnehmer über die Erneuerung des Zertifikats

Es gelten die Regelungen in Abschnitt 4.4.3.

4.7 Zertifizierung nach Schlüsselerneuerung

4.7.1 Bedingungen für eine Zertifizierung nach Schlüsselerneuerung

Die Zertifizierungsstelle beschreibt Bedingungen, unter welchen Umständen ein neu erzeugtes Schlüsselpaar zusammen mit den bisherigen Zertifikatsdaten zertifiziert wird. Bedingungen sind zum Beispiel:

- Sperrung des bisherigen Zertifikats aufgrund einer Schlüsselkompromittierung
- Ablauf des bestehenden Zertifikates
- Ablauf der Schlüsselparameter (z. B. PIN, PUK)

4.7.2 Berechtigung zur Schlüsselerneuerung

Keine Regelung

4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Es gelten die Regelungen in Abschnitt 4.2.

4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Es gelten die Regelungen in Abschnitt 4.3.2.

4.7.5 Verhalten für die Annahme von Zertifikaten nach Schlüsselerneuerungen

Es gelten die Regelungen in Abschnitt 4.4.1.

Belehrungsmaßnahmen **KÖNNEN** entfallen, wenn sich seit der Erstausstellung keine neuen Sachverhalte ergeben haben.

4.7.6 Veröffentlichung von Zertifikaten nach Schlüsselerneuerungen durch die CA

Es gelten die Regelungen in Abschnitt 4.4.2.

4.7.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Es gelten die Regelungen in Abschnitt 4.4.3.

4.8 Zertifikatsänderung

4.8.1 Bedingungen für eine Zertifikatsänderung

Technisch bedeutet eine Zertifikatsänderung, dass ein neues Zertifikat zu Schlüsseln, für die bereits ein Zertifikat existiert, ausgestellt wird, weil im Zertifikat enthaltene Daten ihre Richtigkeit verloren haben. Sind diese Daten Zertifikatsnehmer-spezifisch, werden sie im Rahmen des Registrierungsprozesses berichtigt.

Es gelten die Regelungen in Abschnitt 4.6.1.

4.8.2 Wer darf eine Zertifikatsänderung beantragen?

Es gelten die Regelungen in Abschnitt 4.6.2.

4.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung

Es gelten die Regelungen in Abschnitt 4.6.3.

4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Es gelten die Regelungen in Abschnitt 4.6.4.

4.8.5 Verhalten für die Annahme einer Zertifikatsänderung

Es gelten die Regelungen in Abschnitt 4.6.5.

Belehrungsmaßnahmen **KÖNNEN** entfallen, wenn sich seit der Erstausstellung keine neuen Sachverhalte ergeben haben.

4.8.6 Veröffentlichung der Zertifikatsänderung durch die CA

Es gelten die Regelungen in Abschnitt 4.4.2.

4.8.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines neuen Zertifikats

Es gelten die Regelungen in Abschnitt 4.4.3.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Bedingungen für eine Sperrung

Eine CA beschreibt Bedingungen, unter welchen Umständen eine Zertifikatssperrung durchgeführt wird.

Bei folgenden Zuständen oder Ereignissen erfolgt eine Sperrung:

- Eine Kompromittierung des Schlüsselmaterials liegt vor.
- Die eindeutige Zuordnung des Schlüsselpaares zu seinem Zertifikatsnehmer ist nicht mehr gegeben.
- Die eindeutige Verbindung zwischen Zertifikat und Schlüssel ist nicht mehr gegeben.
- Ein Zertifikat wurde aufgrund von Angaben erwirkt, die nicht (mehr) gültig sind.
- Der Zertifikatsnehmer oder Schlüsselverantwortliche verlangt eine Sperrung.

- Die ausstellende CA beendet ihre Tätigkeit.
- Der Zertifikatsnehmer hat für denselben Verwendungszweck ein Nachfolgezertifikat erhalten (Sperrung **KANN** zeitversetzt erfolgen).

4.9.2 Berechtigte zur Beantragung einer Sperrung

Die CA dokumentiert, wer zur Beantragung einer Sperrung der durch sie ausgestellten Zertifikate berechtigt ist.

4.9.3 Verfahren für einen Sperrantrag

Sowohl die RA, als auch die CA dokumentieren das Verfahren für die Sperrung eines Zertifikates.

4.9.4 Fristen für einen Sperrantrag

Die CA **SOLL** Fristen für einen Sperrantrag gegenüber dem Zertifikatsnehmer dokumentieren.

Der Zertifikatsnehmer wird darauf hingewiesen, dass er dafür Sorge trägt, bei Vorliegen eines Sperrgrundes zeitnah eine Sperrung einzuleiten.

4.9.5 Fristen/Zeitspanne für die Bearbeitung des Sperrantrags durch die CA

Eine Zertifikatssperrung erfolgt zeitnah.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Sperrinformationen werden in Form von Sperrlisten (CRLs) bereitgestellt. Sperrinformationen **KÖNNEN** in Form eines OCSP-Dienstes bereitgestellt werden.

4.9.7 Frequenz der Veröffentlichung von Sperrlisten

Es gelten die auf Sperrlisten bezogenen Regelungen in Abschnitt 2.3.

Die Mindestfrequenz ist im jeweiligen CPS angegeben.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die maximale Latenzzeit für Sperrlisten ist von der CA dokumentiert.

Sperrlisten **SOLLEN** zeitnah nach ihrer Erstellung veröffentlicht werden.

4.9.9 Verfügbarkeit von Online-Sperrinformationen

Siehe Abschnitt 2.3.

Der Verweis auf die Adresse eines Online-Sperrinformationsdienstes (OCSP) **SOLL** im Zertifikatsattribut „Authority Information Access“ des Zertifikats enthalten sein. Der Dienst ist konzernintern erreichbar und **KANN** auch extern erreichbar sein.

4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen

Keine Vorgaben

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

[**TYP_CA**]: Eine Sperrung des Root-CA-Zertifikats der Volkswagen PKI wird auf andere Weise kommuniziert. Die Art und Weise wird zeitnah vor der Sperrung des Zertifikats festgelegt.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Keine Vorgaben

4.9.13 Bedingungen für eine Suspendierung

Eine Suspendierung von Zertifikaten **DARF NUR** bei unkritischen Vorgängen erfolgen. Dieses sind solche, bei denen keine Sperrung vorgesehen ist.

[**TYP_CA**]: Für die von der Root-CA ausgestellten Zertifikate **DARF** eine Suspendierung **NICHT** erfolgen.

4.9.14 Berechtigung zur Beantragung einer Suspendierung

Es gelten die Regelungen in Abschnitt 4.9.2.

4.9.15 Verfahren für Anträge auf Suspendierung

Es gelten die Regelungen in Abschnitt 4.9.3.

4.9.16 Begrenzungen für die Dauer von Suspendierungen

Keine Vorgaben

4.10 Statusabfragedienst für Zertifikate

4.10.1 Funktionsweise des Statusabfragedienstes

Eine CA **SOLL** Sperrinformationen wie unter 4.9.6 beschrieben zur Verfügung stellen.

Der Zugriff auf Sperrinformationen ist über eine im Zertifikat hinterlegte HTTP- oder LDAP-Adresse möglich. Für Zertifikatsnutzer innerhalb der Volkswagen AG **SOLLEN** beide Wege (HTTP und LDAP) zur Verfügung stehen, für externe Zertifikatsnutzer ist mindestens eine der beiden Möglichkeiten vorhanden. Ein Verweis auf verfügbare Sperrinformationen ist in den Zertifikatsattributen „**CRL Distribution Point**“ (CDP) enthalten.

Sperrinformationen **KÖNNEN** zusätzlich per Online Certificate Status Protocol (OCSP) zur Verfügung gestellt werden. Ein Verweis auf den OCSP-Dienst **SOLL** in den Zertifikatsattributen „**Authority Information Access**“ (AIA) enthalten sein.

4.10.2 Verfügbarkeit des Statusabfragedienstes

Aktuelle Sperrinformationen **SOLLEN** 24 Stunden an 7 Wochentagen zur Verfügung stehen.

4.10.3 Optionale Leistungen

Keine Vorgaben

4.11 Kündigung durch den Zertifikatsnehmer

Teilt der Zertifikatsnehmer mit, dass ein Zertifikat nicht mehr genutzt wird oder werden kann, wird das Zertifikat gesperrt.

4.12 Schlüsselhinterlegung und -wiederherstellung

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel

Ist eine Schlüsselhinterlegung möglich, dokumentiert die CA die Prozesse der Schlüsselhinterlegung. Die dabei angewendeten Verfahren entsprechen dem aktuellen Stand der Technik.

Eine Schlüsselhinterlegung **DARF NICHT** für Signaturschlüssel und **SOLL NICHT** für Authentisierungsschlüssel erfolgen.

Private Schlüssel **DÜRFEN NICHT** unverschlüsselt hinterlegt werden.

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln (session keys)

Keine Vorgaben

5 INFRASTRUKTURELLE, ORGANISATORISCHE UND PERSONELLE SICHERHEITSMASSNAHMEN

Dieser Abschnitt behandelt nicht-technische Sicherheitsmaßnahmen.

Nicht-technische Sicherheitsmaßnahmen sind anhand dokumentierter Vorgaben und Prozesse umgesetzt. Die Maßnahmen **MÜSSEN** ausreichen, um die in den Abschnitten 2 - 4 beschriebenen Anforderungen zu erfüllen.

5.1 Bauliche Sicherheitsmaßnahmen

Zentrale Komponenten der Volkswagen PKI sind im besonderen Maße gegen Ausfälle und Angriffe geschützt.

5.1.1 Lage und Gebäude

Unterbringung von Soft- und Hardware einer CA erfolgt in einem zutrittsgesicherten Bereich in den Räumlichkeiten eines gesicherten Rechenzentrums der Volkswagen AG.

5.1.2 Räumlicher Zugang

Die Server zentraler PKI-Funktionen sind in einem zutrittsgesicherten Bereich in den Räumlichkeiten eines gesicherten Rechenzentrums der Volkswagen AG untergebracht. Der Zugang zu dem Rechenzentrum **DARF NUR** über abgesicherte Zonen möglich sein.

5.1.3 Stromversorgung und Klimaanlage

Systeme zentraler PKI-Funktionen sind an eine unterbrechungsfreie Stromversorgung angeschlossen und **SOLLEN** über eine redundant ausgelegte Klimaanlage klimatisiert werden.

5.1.4 Gefährdungen durch Wasser

Keine Vorgaben

5.1.5 Brandschutz

Ein für Systeme zentraler PKI-Funktionen verwendeter Serverraum **SOLL** über ein System zur Brandfrühesterkennung mit einer Alarmaufschaltung zur Feuerwehr verfügen.

5.1.6 Aufbewahrung von Datenträgern

Keine Vorgaben

5.1.7 Müllbeseitigung

Es gelten die Brandschutzvorgaben der Volkswagen AG.

5.1.8 Externe Datensicherung

Soweit für die Server der CA-Dienste eine Datensicherung außerhalb des zutrittsbegrenzten Bereichs (siehe 5.1.2) abgelegt wird, **MUSS** sie verschlüsselt sein.

5.2 Verfahrensvorschriften

5.2.1 Rollenkonzept

Das Rollenkonzept ist unter der Prämisse erstellt, die Auswirkungen eines Missbrauchs durch einzelne Funktionsträger zu reduzieren bzw. die Möglichkeiten zum Missbrauch einzuschränken.

5.2.2 Mehraugenprinzip

Sicherheitsrelevante Vorgänge **SOLLEN** nach dem 4-Augen-Prinzip durchgeführt werden.

Arbeiten innerhalb eines gesicherten Bereichs, der zentrale Komponenten der Volkswagen PKI enthält, werden nach dem 4-Augen-Prinzip durchgeführt.

Nicht permanent berechtige Personen werden bei einem Zugang zu gesicherten Bereichen mit zentralen Komponenten der Volkswagen PKI von mindestens einer berechtigten Personen permanent begleitet.

5.2.3 Identifizierung und Authentifizierung einzelner Rollen

Funktionsträger der Volkswagen PKI einschließlich angeschlossener RAs **MÜSSEN** durch den Leiter des jeweiligen Bereichs namentlich benannt und den jeweiligen Rollen zugeordnet sein.

Eine Freischaltung als Security- oder Registration Authority Officer erfolgt nach dem Vier-Augen-Prinzip durch zwei Security Officer (SO).

5.2.4 Rollentrennung

Keine Vorgaben

5.3 Personalkontrolle

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

Für die Durchführung von Qualifikationsmaßnahmen ist der Leiter der jeweiligen Stelle der Volkswagen PKI verantwortlich.

Funktionsträger der Volkswagen PKI **MÜSSEN** Mitarbeiter der Volkswagen AG sein und **SOLLEN** zu der Gesellschaft gehören, für die sie eine CA/RA betreiben.

5.3.2 Sicherheitsüberprüfung von Mitarbeitern

Keine Vorgaben

5.3.3 Anforderungen an Schulungen

Funktionsträger der Volkswagen PKI **MÜSSEN** regelmäßig sowie im Bedarfsfall geschult werden. Die Verantwortung für diese Maßnahmen trägt der Leiter der jeweiligen PKI Stelle.

5.3.4 Häufigkeit von Schulungen und Belehrungen

Keine Vorgaben

5.3.5 Häufigkeit und Ablauf von Arbeitsplatzwechseln (Job Rotation)

Keine Vorgaben

5.3.6 Sanktionen für unerlaubte Handlungen

Keine Vorgaben

5.3.7 Anforderungen an freie Mitarbeiter

Keine Vorgaben

5.3.8 An Mitarbeiter auszuhändigende Dokumentation

Keine Vorgaben

5.4 Überwachungs- und Protokollierungsmaßnahmen

5.4.1 Arten aufgezeichneter Ereignisse

Alle Transaktionen zwischen CA, RA und Verzeichnissen, die zu einer Erzeugung von Schlüsselmaterial oder Zertifikaten führen oder zu einer Sperrung von Zertifikaten, **MÜSSEN** protokolliert werden.

Alle Administrationstätigkeiten auf Systemen der Volkswagen PKI **MÜSSEN** protokolliert werden.

5.4.2 Häufigkeit der Bearbeitung von Aufzeichnungen

Prozesse und Systeme der Volkswagen PKI sind in der (internen) Auditplanung der Volkswagen AG angemessen berücksichtigt.

5.4.3 Aufbewahrungszeit von Aufzeichnungen

Die Aufbewahrungszeit genügt den relevanten rechtlichen Anforderungen.

5.4.4 Schutz von Aufzeichnungen

Der Schutz der Aufzeichnungen genügt den relevanten rechtlichen Anforderungen.

Logging-Daten (Logfiles) von zentralen Systemen der Volkswagen PKI **SOLLEN** mittels elektronischer Signatur gegen unbemerkte Veränderungen geschützt werden.

Es galten auch die Anforderungen wie in Abschnitt 5.1.8.

5.4.5 Sicherung von Aufzeichnungen (Backup)

Die Sicherung genügt den relevanten rechtlichen Anforderungen.

5.4.6 Speicherung von Aufzeichnungen (intern / extern)

Die Speicherung genügt den relevanten rechtlichen Anforderungen.

5.4.7 Benachrichtigung der Ereignisauslöser

Keine Vorgaben

5.4.8 Schwachstellenanalyse

In die Schwachstellenanalyse von Systemen der Volkswagen PKI fließen Empfehlungen und Beobachtungen des CERTs und der jeweiligen Hersteller ein.

5.5 Archivierung von Aufzeichnungen

Die Archivierung genügt den relevanten rechtlichen Anforderungen.

5.5.1 Arten archivierter Aufzeichnungen

Folgende Daten werden archiviert:

- Beantragungsinformationen / Beantragungsformulare zu Zertifikaten
- Ausgabeprotokolle zu Zertifikaten
- Sperranträge zu Zertifikaten

5.5.2 Aufbewahrungsfristen für archivierte Daten

Keine Vorgaben

5.5.3 Schutz des Archivs

Keine Vorgaben

5.5.4 Datensicherung des Archivs (Backup)

Keine Vorgaben

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

Keine Vorgaben

5.5.6 Archivierung (intern / extern)

Keine Vorgaben

5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen

Keine Vorgaben

5.6 Schlüsselwechsel einer CA

Ein Schlüsselwechsel erfolgt anhand dokumentierter Verfahren.

[**TYP_CA**]: Information über einen bevorstehenden Schlüsselwechsel werden im Vorfeld allen Betroffenen kommuniziert.

[**TYP_CA:**]: Bei Schlüsselwechsel wird die laufende Nummer im CN einer CA (<nn>) erhöht (siehe Abschnitte 3.1.5 und 3.1.2) außer bei Microsoft-CAs.

[**TYP_CA**]: Ein Schlüsselwechsel der Root-CA erfolgt so rechtzeitig, dass die Anforderungen des benutzten Gültigkeitsmodells (Schalenmodell, Kettenmodell, Hybridmodell) erfüllt sind.

5.7 Kompromittierung und Notfallplanung

Sollten die Schlüssel einer Zertifizierungsstelle kompromittiert sein, werden die jeweiligen Zertifikatsnehmer und Zertifikatsnutzer zeitnah informiert.

Sollten die Schlüssel einer Zertifizierungsstelle zerstört und nicht wiederherstellbar sein, werden die jeweiligen Zertifikatsnehmer zeitnah informiert.

Die Verantwortlichen einer CA verfügen für den Fall einer Kompromittierung oder Zerstörung von Schlüsselmaterial über einen dokumentierten Notfallplan. Neue Schlüsselpaare und Zertifikate werden zeitnah erzeugt und den Zertifikatsnehmern zur Verfügung gestellt.

5.7.1 Behandlung von Vorfällen und Kompromittierungen

Entsprechende Vorfälle werden als Sicherheitsvorfall (Security Incident) bewertet und behandelt.

5.7.2 Kompromittierung von Rechnerressourcen, Software oder Daten

Entsprechende Vorfälle werden als Sicherheitsvorfall (Security Incident) bewertet und behandelt.

5.7.3 Kompromittierung des privaten Schlüssels einer CA

Bei Kompromittierung des privaten Schlüssels einer CA werden das CA-Zertifikat und alle Zertifikate, die von dieser ausgegeben sind, schnellstmöglich gesperrt.

5.7.4 Möglichkeiten zur Geschäftsweiterführung nach einer Kompromittierung

Keine Vorgaben

5.8 Schließung von CA oder RA

Die Schließung einer CA oder RA erfolgt anhand eines dokumentierten Prozesses.

Betroffene der Schließung einer CA **MÜSSEN** spätestens drei Monate vor Betriebseinstellung von einer Schließung in Kenntnis gesetzt werden.

Betroffene der Schließung einer RA werden mit ausreichendem zeitlichem Vorlauf von einer Schließung in Kenntnis gesetzt.

6 TECHNISCHE SICHERHEITSMASSNAHMEN

6.1 Erzeugung und Installation von Schlüsselpaaren

Die Volkswagen PKI erzeugt kryptographisch sichere Schlüsselpaare.

6.1.1 Erzeugung von Schlüsselpaaren

[**TYP_CA**]: Schlüssel **MÜSSEN** in einem Hardware Security Module (HSM) erzeugt werden. Ein eingesetztes HSM **MUSS** über eine aussagekräftige Sicherheitszertifizierung verfügen.

[**TYP_PERSON**]: Schlüssel zur Signatur **SOLLEN** auf einer Chipkarte erzeugt werden. Der eingesetzte Chip **SOLL** über eine aussagekräftige Sicherheitszertifizierung verfügen.

Es **KANN** zulässig sein, dass ein Antragsteller einen privaten Schlüssel selbst erzeugt. Siehe dazu Abschnitt 3.2.1.

Die Volkswagen PKI erzeugt RSA-Schlüssel. Schlüssel für andere Verschlüsselungsverfahren **KÖNNEN** erstellt werden, wobei Verschlüsselungsverfahren und Schlüssellänge als sicher angesehen sein **MÜSSEN**.

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Werden private Schlüssel durch eine CA erzeugt, werden diese entsprechend Abschnitt 4.4.1 an die Zertifikatsnehmer ausgeliefert.

6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

Soweit Schlüssel durch den Zertifikatsnehmer erzeugt werden, **MÜSSEN** öffentliche Schlüssel in Form von PKCS#10 Requests der ausstellenden CA zur Verfügung gestellt werden.

6.1.4 Lieferung öffentlicher CA-Schlüssel an Zertifikatsnutzer

Öffentliche Schlüssel der CAs der Volkswagen PKI sind in den korrespondierenden Zertifikaten innerhalb der Volkswagen AG veröffentlicht. Dieses erfolgt auch außerhalb der Volkswagen AG, wenn die von einer CA signierten Zertifikate dort genutzt werden.

6.1.5 Schlüssellängen

[**TYP_CA**]: Die RSA-Schlüssellänge beträgt mindestens 2048 Bit.

[**TYP_INTERN**, **TYP_PERSON, TYP_PROZESS, TYP_MASCHINE**]: Die Länge für von der Volkswagen PKI erstellten RSA-Schlüssel beträgt mindestens 1024 Bit. Die Länge für von Antragstellern erstellten RSA-Schlüssel **SOLL** mindestens 1024 Bit betragen; die Volkswagen PKI **BRAUCHT** die Längen der von Antragstellern erstellten Schlüsseln **NICHT** auf Mindestlängen zu überprüfen.

6.1.6 Festlegung der Parameter öffentlicher Schlüssel und Qualitätssicherung

Die Betreiber der Volkswagen PKI **SOLLEN** sich an Empfehlungen zuverlässiger Sicherheitsorganisationen (z. B. BSI) orientieren.

6.1.7 Schlüsselverwendungen

Siehe Abschnitt 1.4.1.

6.2 Schutz des privaten Schlüssels und Anforderungen an kryptographische Module

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

Die verwendeten kryptographischen Module genügen anerkannten (Sicherheits-) Standards. Diese **SOLLEN** die Anforderungen der Standards FIPS PUB 140-1, 140-2 (Level 2 oder höher) erfüllen, über eine EAL4-Zertifizierung (oder höher) verfügen oder einem vergleichbaren Standard genügen.

6.2.2 Mehrpersonen-Zugriffsicherung auf private Schlüssel

[**TYP_CA**]: Eine Freischaltung eines HSMs zur Nutzung der privaten Schlüssel erfolgt durch mehrere Personen nach einem n-von-m-Prinzip.

6.2.3 Hinterlegung privater Schlüssel

Eine Hinterlegung privater Schlüssel bei Dritten **DARF NICHT** erfolgen.

Siehe auch Abschnitt 4.12.1.

6.2.4 Sicherung privater Schlüssel (Backup)

[**TYP_CA**]: Von den CA-Schlüsseln, die auf einem HSM erzeugt wurden, wird eine geschützte Sicherung so erstellt, dass die Schlüssel nur nach Rückübertragung in ein HSM genutzt werden können. Der Zugriff auf die Schlüssel im HSM und der auf die Schlüssel in

der geschützten Sicherung **MÜSSEN** durch vergleichbare Sicherheitsverfahren geschützt sein.

[**TYP_PERSON**]: Sicherungen von privaten Schlüsseln mit dem Nutzungszweck **dataEncryption KÖNNEN** angefertigt werden. Ob und wie eine solche Sicherung erfolgt, ist im jeweiligen CPS definiert.

6.2.5 Archivierung privater Schlüssel

Neben den in Abschnitt 6.2.4 beschriebenen Szenarien erfolgt keine Archivierung privater Schlüssel.

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

[**TYP_CA**]: Außer zur Sicherung und Wiederherstellung (siehe Abschnitt 6.2.4) oder zur Synchronisation mehrerer HSMs für dieselbe CA **DARF** ein privater CA-Schlüssel **NICHT** in ein oder aus einem kryptographischen Modul übertragen werden.

[**TYP_INTERN**, **TYP_PERSON, TYP-MASCHINE, TYP_PROZESS**]: Soweit private Schlüssel in oder aus kryptographischen Modulen übertragen werden, ist der Transfer im CPS der jeweiligen CA beschrieben.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

[**TYP_CA**]: Private Schlüssel **MÜSSEN** in HSMs gespeichert sein (siehe Abschnitte 6.1.1 und 6.2.4).

[**TYP_INTERN, TYP_PERSON, TYP-MASCHINE, TYP_PROZESS**]: siehe CPS der jeweiligen CA.

6.2.8 Aktivierung privater Schlüssel

[**TYP_CA**]: Private Schlüssel **DÜRFEN NUR** unter Einhaltung des 4-Augen Prinzips von dafür autorisierten Funktionsträgern aktivierbar sein.

[**TYP_PERSON**]: Private Schlüssel **DÜRFEN NUR** durch Eingabe einer PIN aktivierbar sein.

6.2.9 Deaktivierung privater Schlüssel

Eine Deaktivierung privater Schlüssel (nach deren Nutzung) erfolgt durch die jeweilige Anwendung.

[**TYP_PERSON**]: Eine dauerhafte Deaktivierung privater Schlüssel **SOLL** erfolgen, wenn eine PIN mehrmals falsch eingegeben wurde. Die Anzahl möglicher Reaktivierungsprozesse (unter Nutzung einer PUK) **KANN** begrenzt werden.

6.2.10 Zerstörung privater Schlüssel

[**TYP_CA**]: Es ist sichergestellt, dass private Signaturschlüssel einer CA nach Ende ihres Lebenszyklus nicht mehr benutzt werden. Dazu **SOLLEN** sie zerstört werden.

6.2.11 Bewertung kryptographischer Module

Siehe Abschnitt 6.2.1.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Alle von der Volkswagen PKI produzierten öffentlichen Schlüssel sind in Form erstellter Zertifikate in Verzeichnissen gespeichert und **SOLLEN** zudem in der Datenbank der ausstellenden CA abgelegt werden.

Siehe dazu auch Abschnitt 2.1.

Eine Archivierung erfolgt bis mindestens 10 Jahre nach Ablauf eines Zertifikats.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Bei der Festlegung von Gültigkeitsperioden wird beachtet, dass verwendete Schlüssellängen oder verwendete Algorithmen i.d.R. nur für eine begrenzte Dauer ausreichende Sicherheit bieten.

[**TYP_CA**]: Zertifikate einer Sub-CA **DÜRFEN NUR** eine maximale Gültigkeitsdauer von 10 Jahren besitzen. Die maximale Gültigkeit von Zertifikaten ist im CPS der signierenden CA benannt.

6.4 Aktivierungsdaten

Eine RA legt und dokumentiert einen Prozess zur sicheren Übermittlung von Aktivierungsdaten fest.

6.4.1 Erzeugung und Installation von Aktivierungsdaten

Aktivierungsdaten von CA-Schlüsseln **SOLLEN** sich aus mindestens zwei Geheimnissen zusammensetzen.

6.4.2 Schutz von Aktivierungsdaten

Keine Vorgaben

6.4.3 Andere Aspekte von Aktivierungsdaten

Keine Vorgaben

6.5 Sicherheitsmaßnahmen für IT-Systeme

6.5.1 Spezifische technische Sicherheitsanforderungen für IT-Systeme

Alle IT-Komponenten der Volkswagen PKI erfüllen die für sie geltenden Sicherheitsanforderungen der IT-Sicherheitsrichtlinien (siehe [2]).

IT-Systeme (Server) für den OCSP- und Web-Sperrdienst **SOLLEN** mit geeigneten Maßnahmen gegen unberechtigte Manipulation geschützt werden.

Ressourcenanforderungen einer CA an CPU und Speicher **SOLLEN** überwacht und Auswertungen vorgenommen werden. Die dabei gewonnenen Erkenntnisse fließen in die Kapazitätsplanung der CA ein.

Siehe auch Abschnitt 6.7.

6.5.2 Beurteilung der IT-Systemsicherheit

Eine Beurteilung **SOLL** im Rahmen interner Audits erfolgen.

6.6 Technische Maßnahmen während des Lebenszyklusses

Der Betreiber der Volkswagen PKI **MUSS** über aktuelle Sicherheitsstandards informiert sein.

Mindestanforderungen des BSI **SOLLEN** eingehalten werden, sofern diese für den Einsatzbereich der Volkswagen PKI relevant sind und den laufenden Betrieb von Applikationen innerhalb der Volkswagen AG nicht gefährden.

6.6.1 Sicherheitsmaßnahmen bei der Systementwicklung

Keine Vorgaben

6.6.2 Sicherheitsmaßnahmen beim Systemmanagement

Alle IT-Komponenten der Volkswagen PKI erfüllen die für sie geltenden Sicherheitsanforderungen der IT-Sicherheitsrichtlinien (siehe [2]).

6.6.3 Sicherheitsmaßnahmen während des Lebenszyklusses

Keine Vorgaben

6.7 Sicherheitsmaßnahmen für Netze

Alle IT-Komponenten der Volkswagen PKI erfüllen die für sie geltenden Sicherheitsanforderungen der IT-Sicherheitsrichtlinien (siehe [2]).

CAs oder RAs **DÜRFEN NUR** in internen Netzwerkzonen der Volkswagen AG betrieben werden, die die jeweiligen Sicherheitsanforderungen erfüllen.

Zentrale IT-Komponenten der Volkswagen PKI werden in Netzwerkbereichen betrieben, die die hohen Sicherheitsanforderungen der Dienste erfüllen.

IT-Systeme der RAs **MÜSSEN** mittels geeigneter technischer Sicherheitsmaßnahmen gegenüber dem Intranet der Volkswagen AG abgesichert sein.

Es **SOLLEN** nur die zur Funktion der RAs sowie zur Administration der Systeme notwendigen Kommunikationsbeziehungen von bzw. mit einer CA oder RA zugelassen werden.

6.8 Zeitstempel

Keine Vorgaben

7 PROFILE VON ZERTIFIKATEN, SPERRLISTEN UND OCSP

7.1 Zertifikatsprofile

7.1.1 Versionsnummern

Zertifikate der Volkswagen PKI sind konform zum Standard X.509 v3 (Typ 0x2).

7.1.2 Zertifikatserweiterungen

Für eine CA sind zu nutzende Zertifikatserweiterungen festgelegt.

Folgende Zertifikatserweiterungen sind als kritisch (critical) definiert:

- KeyUsage
- [**TYP_CA**]: BasicConstraints

Grundsätzlich **SOLLEN** möglichst wenige Zertifikatserweiterungen als kritisch definiert werden.

Zertifikate, die für sichere E-Mail nutzbar sein sollen, **MÜSSEN** die E-Mail-Adresse des Zertifikatsnehmers enthalten. Die E-Mail Adresse ist dann in einer der folgenden Erweiterungen enthalten:

- Subject Alternative Name (rfc822Name), bevorzugt
- Innerhalb des Distinguished Name (E=)

[**TYP_PERSON**]: In Zertifikaten dieses Typs **MUSS** die E-Mail-Adresse des Zertifikatsinhabers im Subject Alternative Name (rfc822Name) enthalten sein.

[**TYP_MASCHINE**]: Der (primäre) Systemname **SOLL** im Distingushed Name (CN=) enthalten sein.

7.1.3 Algorithmen OIDs

Keine Vorgaben

7.1.4 Namensformate

Siehe Abschnitte 3.1.1 und 3.1.2.

7.1.5 Namensbeschränkungen

siehe Abschnitt 3.1.5.

7.1.6 OIDs der Zertifikatsrichtlinien

Diese hier vorliegende Richtlinie besitzt eine OID. Diese OID **SOLL** in das Attribut „certificatePolicies“ eines Zertifikats eingetragen und dabei als nicht kritisch definiert werden.

7.1.7 Nutzung der Erweiterung „PolicyConstraints”

Keine Vorgaben

7.1.8 Syntax und Semantik der Erweiterung „PolicyQualifiers“

Keine Vorgaben

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung „CertificatePolicies“

Keine Vorgaben

7.2 Sperrlistenprofile

Eine Sperrliste enthält folgende Attribute:

- „**Version**“
- „**Signature, Issuer Name**“
- „**Date Issued**“
- „**Issued Date for Next Update**“
- „**Revoked Certificates**“

Im Attribut **cRLReason KANN** eine CA den Grund einer Sperrung aufführen.

7.2.1 Versionsnummern

Die Sperrlisten **SOLLEN** das Format Version 2 oder höher haben.

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

Sperrlisten **SOLLEN** folgende Erweiterungen enthalten, die jeweils als unkritisch zu definieren sind:

- „**cRLNumber**“
- „**authority key identifier**“ des CA-Zertifikats
- “**id-ce-deltaCRLIndicator**“ (wenn es sich um eine Delta-CRL handelt)

7.3 Profile des Statusabfragedienstes (OCSP)

Ein Zertifikat zur Signatur der OCSP-Anfrage **KANN** anhand der Erweiterung der Extended KeyUsage „OCSP signing“ identifiziert werden.

7.3.1 Versionsnummern

Das OCSP **SOLL** in der Version 1 eingesetzt werden.

7.3.2 OCSP Erweiterungen

Stellt eine CA eine OCSP-Statusprüfung zur Verfügung, sind die genutzten Erweiterungen dokumentiert.

8 COMPLIANCE-AUDITS UND ANDERE BEWERTUNGEN

8.1 Häufigkeit und Bedingungen für Audits

Prozesse und Systeme der Volkswagen PKI sind in der (internen) Auditplanung der Volkswagen AG angemessen berücksichtigt.

8.2 Identität/Qualifikation des Prüfers

Interne Audits **SOLLEN** durch Auditoren der IS-Sicherheitsorganisation (ISSO) oder externe Dienstleister durchgeführt werden. Der Beauftragende prüft u. a. die Fachkompetenz externer Dienstleister vor Beauftragung.

8.3 Stellung des Prüfers zum Bewertungsgegenstand

Keine Vorgaben

8.4 Durch Prüfung abzudeckende Themen

Der Prüfer **SOLL** abzudeckende Themenbereiche nach eigenem Ermessen prioritätsgesteuert auswählen.

8.5 Reaktionen auf Unzulänglichkeiten

Reaktionen auf Unzulänglichkeiten werden mit den betroffenen Stellen bei Vorliegen des Audit-Berichts vereinbart.

Bei schwerwiegenden Verstößen **KÖNNEN** Organisationseinheiten Rechte zum Betrieb einer PKI Komponente oder zur Nutzung entzogen werden.

8.6 Information über Bewertungsergebnisse

Leiter einer PKI-Stelle werden über die sie betreffenden Audit-Ergebnisse informiert.

9 Sonstige finanzielle und rechtliche Angelegenheiten

9.1 Preise

9.1.1 Preise für Zertifikate oder Zertifikatserneuerungen

Keine Vorgaben

9.1.2 Preise für den Zugriff auf Zertifikate

Keine Vorgaben

9.1.3 Preise für Sperrungen oder Statusinformationen

Keine Vorgaben

9.1.4 Preise für andere Dienstleistungen

Keine Vorgaben

9.1.5 Regelungen zur Kostenrückerstattung

Keine Vorgaben

9.2 Finanzielle Zuständigkeiten

9.2.1 Versicherungsdeckung

Keine Vorgaben

9.2.2 Andere Posten

Keine Vorgaben

9.2.3 Versicherung oder Gewährleistung für Endnutzer

Keine Vorgaben

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Definition von vertraulichen Informationen

Generell sind Informationen, die beim Betrieb von Prozessen oder Komponenten der Volkswagen PKI anfallen, entsprechend der Datenschutzrichtlinie der Volkswagen AG (siehe [1]) zu behandeln.

Programm-, Konfigurations- und Auswertungsdaten der Volkswagen PKI sowie alle Unterlagen über Sicherheitsmaßnahmen der PKI-Komponenten werden (auch ohne entsprechende Kennzeichnung) als „vertraulich“ behandelt. Darunter fällt auch das CPS einer CA.

9.3.2 Informationen, die nicht vertraulich behandelt werden

Als öffentlich gelten alle Informationen, die in veröffentlichten Zertifikaten enthalten sind sowie die in Abschnitt 2.2 genannten Informationen.

9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen

Jeder Funktionsträger der Volkswagen PKI ist zur Wahrung der Vertraulichkeit der ihm zugänglichen Informationen verpflichtet.

9.4 Datenschutz von Personendaten

9.4.1 Datenschutzkonzept

Funktionsträger der Volkswagen PKI **MÜSSEN** verpflichtet sein, personenbezogene Informationen vertraulich zu behandeln. Eine Verwendung, Speicherung oder Weitergabe personenbezogener Daten, welche über die vorgesehene Nutzung innerhalb der Volkswagen PKI hinausgehen, **DARF NICHT** erfolgen.

9.4.2 Als persönlich behandelte Daten

Keine Vorgaben. Es gilt das Datenschutzkonzept der Volkswagen AG [1].

9.4.3 Daten, die nicht als persönlich behandelt werden

Keine Vorgaben. Es gilt das Datenschutzkonzept der Volkswagen AG [1].

9.4.4 Zuständigkeiten für den Datenschutz

Keine Vorgaben. Es gilt das Datenschutzkonzept der Volkswagen AG.

9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten

[**TYP_PERSON**]: Es **SOLL** gewährleistet werden, dass Zertifikatsinformationen (auch) extern veröffentlicht werden können. Dies **KANN** im Rahmen betrieblicher Mitbestimmung geschehen.

9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften

Wenn gesetzliche Zwänge bestehen, werden erteilte Auskünfte dokumentiert.

9.4.7 Andere Bedingungen für Auskünfte

Auskunft an Dritte **DARF NUR** im Rahmen externer Verzeichnisdienste und der dafür vorgesehenen Zugriffsmöglichkeiten erfolgen.

9.5 Urheberrechte

9.6 Zusicherungen und Garantien

9.6.1 Zusicherungen und Garantien einer CA

Keine Vorgaben. Die Einhaltung von Urheberrechten richtet sich nach den allgemeinen gesetzlichen Vorschriften.

9.6.2 Zusicherungen und Garantien einer RA

Siehe Abschnitt 9.6.1.

9.6.3 Zusicherungen und Garantien der Zertifikatsnehmer

Ein Teilnehmer der Volkswagen PKI ist verpflichtet, die mit der Aushändigung des Schlüsselträgers oder PIN-Briefs kommunizierten Anweisungen zum Umgang mit Schlüsselträger und Zertifikat einzuhalten.

[**TYP_PERSON**]: Der Zertifikatsnehmer ist verpflichtet, eine ihm zugewiesene PIN geheim zu halten und einen Zugriff durch Dritte auf seine privaten Schlüssel zu verhindern.

9.6.4 Zusicherungen und Garantien der Zertifikatsnutzer

Keine Vorgaben

9.6.5 Zusicherungen und Garantien anderer Teilnehmer

Keine Vorgaben

9.7 Haftungsausschlüsse

Keine Vorgaben

9.8 Haftungsbeschränkungen

Keine Vorgaben

9.9 Schadensersatz

Keine Vorgaben

9.10 Gültigkeitsdauer der CP und Beendigung der Gültigkeit

9.10.1 Gültigkeitsdauer der CP

Diese CP gilt ab dem Zeitpunkt ihrer Veröffentlichung und bleibt gültig, solange Zertifikate, die auf Basis dieser CP erstellt wurden, gültig sind.

9.10.2 Beendigung der Gültigkeit

Keine Vorgaben

9.10.3 Auswirkung der Beendigung und Weiterbestehen

Keine Vorgaben

9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern

Keine Vorgaben

9.12 Änderungen der CP

Änderungen zu dieser CP werden in dieses Dokument eingearbeitet und veröffentlicht. Dabei **KANN** die Dokumenten-OID geändert werden.

9.12.1 Verfahren für Ergänzungen

Keine Vorgaben

9.12.2 Benachrichtigungsmechanismen und –fristen

Keine Vorgaben

9.12.3 Bedingungen für Änderungen der OID

Keine Vorgaben

9.13 Verfahren zur Schlichtung von Streitfällen

Keine Vorgaben

9.14 Zugrunde liegendes Recht

Diese CP und der Betrieb der CAs der Volkswagen PKI unterliegen dem deutschen Recht.

Soweit keine anderen Aussagen getätigt werden, unterliegt der Betrieb einer RA dem Recht des jeweiligen Landes, in dem diese betrieben wird.

9.15 Einhaltung geltenden Rechts

Dieses wird gewährleistet.

9.16 Sonstige Bestimmungen

9.16.1 Vollständigkeitserklärung

Folgende Dokumente sind Gegenstand geltender Vereinbarungen zwischen der Volkswagen PKI und den Teilnehmern (Zertifikatsnehmern und Zertifikatsnutzern)

- Die zum Zeitpunkt einer Anwendung der PKI gültige CP

9.16.2 Abgrenzungen

Keine Vorgaben

9.16.3 Salvatorische Klausel

Wenn eine Bestimmung dieser CP unwirksam ist oder unwirksam wird, wird dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt.

9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

Keine Vorgaben

9.16.5 Höhere Gewalt

Keine Vorgaben

9.17 Andere Bestimmungen

Keine Vorgaben

10 ANHANG

10.1 Quellenverzeichnis

Quelle	Dokument
[1]	Datenschutzrichtlinie der Volkswagen AG Die Bezeichnung der jeweils gültigen Datenschutzrichtlinie findet sich in [A1].
[2]	IT-Sicherheitskonzept der Volkswagen AG Die Bezeichnung des jeweils gültigen IT-Sicherheitskonzepts findet sich in [A1].

10.2 Anlagen

Das vorliegende Dokument wird durch eine Anlage 1 ergänzt, die an gleicher Stelle wie das vorliegende Dokument publiziert wird und Informationen enthält, die sich während des Lebenszyklus der PKI erwartungsgemäß ändern werden (z.B. Dokumentnamen oder Abteilungsbezeichnungen).

Anlagen	Dokumenten
[A1]	Volkswagen_PKI_CP_Anlage1_v<n.n>.pdf Die Anlage wird an gleicher Stelle wie das vorliegende Dokument publiziert, es gilt die jeweils neuste Version für „v<n.n>“.