automotive engineering iav

Zertifikatsrichtlinie IAV GmbH

Root- & Policy-CA

Zertifikatsrichtlinie IAV GmbH

Root- & Policy-CA

Geltungsbereich:	IAV Gruppe
Revisionszyklus:	jährlich
Zielgruppe:	alle Entitäten die auf der IAV-PKI aufbauende Dienste und Anwendungen betreiben oder nutzen

Dateiname: IAV - CP_Root_CA_&_Policy_CA V1.11.docx

Version: 1.11

Status: Freigegeben (extern)

Geheimhaltungsstufe: Öffentlich

	Datum	Name	Firma
Erstellt	03.08.2020	Bastian Müller	IAV GmbH
Geprüft	12.08.2020	Karsten Keusch, Marc Plagge	IAV GmbH
Freigegeben	14.08.2020	Matthias Jänicke	IAV GmbH

Inhalt

1 Einleitung

1.1 Überblick

Dieses Dokument beschreibt die verbindliche Zertifikatsrichtlinie (engl. „Certificate Policy“, kurz CP) für die von IAV GmbH betriebene PKI (engl. „Public Key Infrastructure“). Sie fasst für die Benutzer und IAV als PKI-Betreiber verbindlichen Vorgaben und Anforderungen zusammen, die im Rahmen der Bereitstellung und des Betriebs der Systemkomponenten Root- und Policy-CA sowie für die von ihnen ausgestellten [X.509] konformen Zertifikate umzusetzen sind. Die folgende Abbildung veranschaulicht den Geltungsbereich dieser Richtlinie:

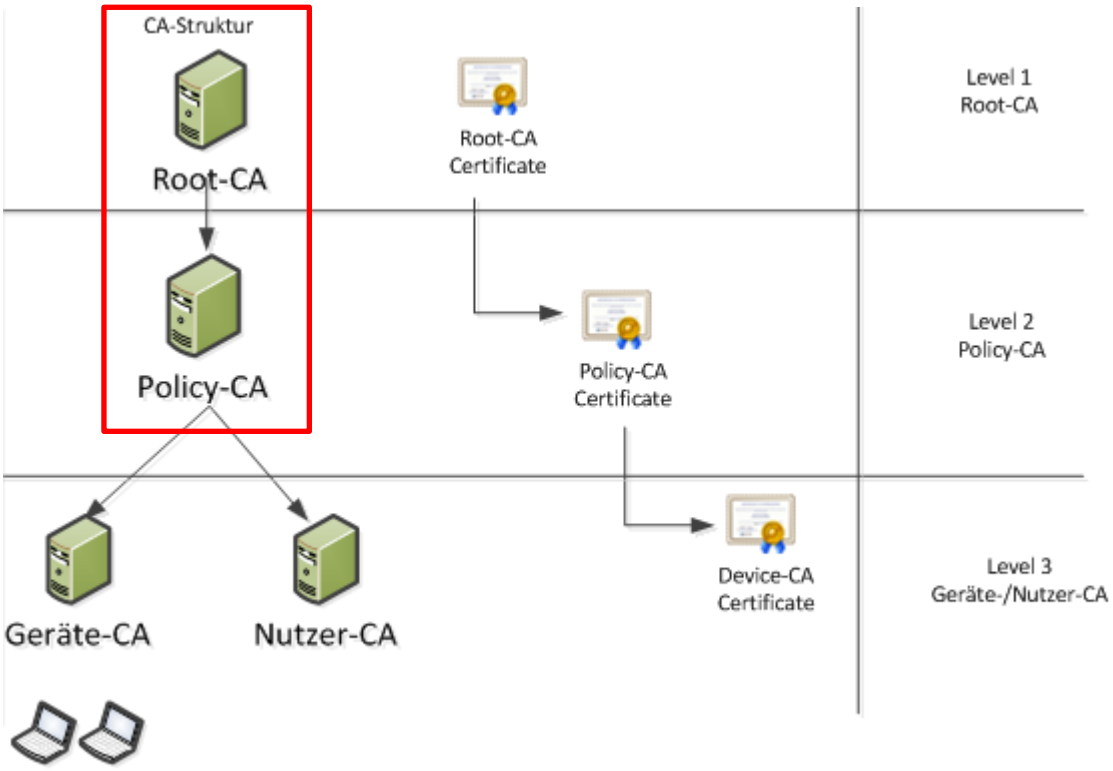

Abbildung 1 IAV Root- & Policy-CA

In dieser CP sind sowohl technische als auch organisatorische Anforderungen formuliert, die den aktuellen Empfehlungen der IT-Sicherheit entsprechen. Die für die Anforderungsumsetzung benötigten nicht-technischen und technischen Maßnahmen werden in den Kapiteln 5 und 6 beschrieben und repräsentieren das sog. „Certificate Practice Statement” (CPS) für die Root- und Policy-CA der IAV-PKI. Für die nachgelagerten CAs auf der untersten Stufe (Geräte- und Nutzer-CA) gibt es jeweils eigene dedizierte Zertifikatsrichtlinien.

Zwecks Vereinfachung, einer besseren Darstellung und Vergleichbarkeit mit anderen CPs orientiert sich die Gliederung des Dokuments nach dem Muster des Internet-Standard RFC 3647 „Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework“ [RFC3647].

Im Zuge der Ausstellung von Zertifikaten bestätigt die Root-CA als oberster Vertrauensanker, dass

- die ausgestellten Zertifikate den Vorgaben und Anforderungen der IAV entsprechen und
- für die CA entsprechende Prozesse und Vorgaben definiert und dokumentiert sind und diese eingehalten werden.

Die Publizierung des Root-CA-Zertifikats erfolgt innerhalb IAV in den zertifikatsnutzenden Anwendungen und Systemen.

1.1.1 Ziel dieser Richtlinie

Diese Richtlinie legt die technischen und organisatorischen Rahmenbedingungen der Root-CA (Level 1) und der untergeordneten Policy-CA (Level 2) der IAV-PKI fest. Die Root-CA der IAV stellt den obersten Vertrauensanker der IAV-PKI-Struktur dar. Damit etabliert sie die Basis für den Schutz von Anwendungen, Dienste, Nutzer, Systeme und Daten durch Authentifizierung, Verschlüsselung und Signatur. Die ihr untergeordnete Policy-CA stellt CA-Zertifikate für nachrangige fachliche CAs (Level 3) aus, die wiederum ausschließlich Endbenutzerzertifikate z.B. für Geräte oder Personen erstellen. Den fachlichen CAs (Level 3) der IAV sind jeweils eigene dedizierte CPs zugeordnet.

1.1.2 Konventionen

In dieser CP werden (analog zum englischen must/shall - should - may in der Standardisierung) die Begriffe muss – soll – kann gemäß dem Standard [RFC2119] verwendet:

- **muss, darf nicht, darf nur**

  Verbindliche Vorgabe der IAV Root-CA und der untergeordneten Policy-CA

- **soll, (sollte)**

  Vorgabe der IAV Root-CA und der untergeordneten Policy-CA, Nichteinhaltung nur in begründeten Ausnahmen

- **kann**

  optional

1.1.3 Gültigkeit

Diese Richtlinie ist ab 01.02.2015 bindend für alle von der IAV Root-CA sowie der ihr untergeordneten IAV Policy-CA ausgestellten CA-Zertifikate.

1.2 Name und Kennzeichnung des Dokuments

Name:	Zertifikatsrichtlinie Root- und Policy-CA IAV GmbH
Version:	1.11
Datum:	12.08.2020
OID Root CA:	1.3.6.1.4.1.44741.1.1
OID Policy-CA:	1.3.6.1.4.1.44741.1.2

1.3 PKI-Teilnehmer

Teilnehmer sind Entitäten (Sub-CAs, Nutzer, Geräte), die auf der IAV-PKI aufbauende Dienste und Anwendungen betreiben oder nutzen.

1.3.1 Zertifizierungsstellen

Den CAs der IAV-PKI obliegt die Ausstellung von Zertifikaten. Für die IAV-PKI wird eine dreistufige Zertifizierungsstruktur mit einem selbstsignierten Root-Zertifikat verwendet. Die Root-CA zertifiziert ausschließlich die nachgelagerte Policy-CA. Diese wiederum zertifiziert ausschließlich nachgelagerte fachliche CAs. Die fachlichen CAs werden verwendet, um Maschinenzertifikate (mittels einer dedizierten Geräte-CA) oder Benutzerzertifikate (mittels einer dedizierten Nutzer-CA) auszustellen.

1.3.2 Registrierungsstellen

Den Registrierungsstellen (RA) obliegen die Überprüfung der Identität und Authentizität von Zertifikatsnehmern. Bei der IAV-PKI ist allen fachlichen CAs, die Endzertifikate für Geräte oder

Personen ausstellen, jeweils mindestens eine ausgezeichnete RA zugeordnet. Weitere Details dazu sind den jeweiligen assoziierten CPs zu entnehmen.

Eine dedizierte Registrierungsstelle für die Root- und Policy-CA ist nicht notwendig (beide sind bei Nichtverwendung offline). Die Erstellung und Erneuerung von Zertifikaten, sowohl durch die Root- als auch durch die Policy-CA, liegt in der Verantwortung der IAV-Geschäftsführung und ist von ihr explizit freizugeben.

1.3.3 Zertifikatsnehmer

Zertifikatsnehmer sind natürliche oder von diesen verantworteten technischen Entitäten (Maschinen oder Programme), die Zertifikate beantragen und innehaben. Die verantwortlichen natürlichen Personen stehen in einem Vertragsverhältnis mit IAV und sind damit berechtigt, Zertifikate zu erhalten.[1]

1.3.4 Zertifikatsnutzer

Zertifikatsnutzer sind alle Personen, Organisationen, Dienste und Anwendungen von IAV, die Zertifikate von Zertifikatsnehmern nutzen können.

1.3.5 Weitere Teilnehmer

Hierbei handelt es sich um externe Teilnehmer, die keine Verpflichtungen gegenüber IAV haben und somit nicht Bestandteil dieser Richtlinie sind.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

Maßgeblich für die erlaubte Verwendung von Zertifikaten müssen die im Zertifikat enthaltenen Attribute zur *KeyUsage* sowie die Vorgaben in der zugehörenden CP des Teilnehmers sein. Die Zertifikate dürfen nur im Zusammenhang mit IAV-Geschäftsprozessen verwendet werden.

1.4.2 Verbotene Verwendungen von Zertifikaten

Eine private Verwendung ausgestellter CA-Zertifikate ist untersagt.

1.5 Verwaltung der Zertifizierungsrichtlinien

1.5.1 Zuständigkeit für das Dokument

Dieses Richtlinien-Dokument wird vom Betreiber der IAV-PKI gepflegt. Für Kontaktinformationen siehe Abschnitt 1.5.2.

1.5.2 Ansprechpartner und Kontakt

Karsten Keusch
Team Manager IAM, IT-Security & Governance

Carnotstraße 1
10587 Berlin, Germany

Marc Plagge
IAM, IT-Security & Governance

Rockwellstraße 16
38518 Gifhorn, Germany

marc.plagge[at]iav.de
www.iav.de

[1] Es kann im Zertifikat einer natürlichen Person eine Organisation oder Funktionseinheit zugeordnet werden.

karsten.keusch[at]iav.de
www.iav.de

Tabelle 1 Ansprechpartner und Kontakt

1.5.3 Prüfung der Zertifizierungsrichtlinie

Diese Richtlinie wird durch den Serviceverantwortlichen der IAV-PKI regelmäßig alle zwei Jahre oder anlassbezogen überprüft. Der Systemverantwortliche der IAV-PKI stellt die Übereinstimmung der CPS mit den Vorgaben der jeweiligen CP sicher.

1.6 Definitionen und Abkürzungen

1.7 Siehe Andere Regelungen

Nichtzutreffend.

Verzeichnisse - 10.3 Abkürzungsverzeichnis.

2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

IAV stellt die von der Root- und Policy-CA ausgestellten CRLs in einem intern als auch extern verfügbaren Verzeichnisdienst zur Verfügung. Dieser Verzeichnisdienst ist unter folgenden Adressen erreichbar:

- Für CRLs:
  - http://crl.iavtech.net/pki/ (extern)
  - http://crl.iav.enxo.org/pki/ (extern / intern)
- Diese CP steht ebenfalls intern als auch extern auf einem Webserver zur Verfügung:
- Für CP:
  - https://www.iav.com/certificate-policy (extern / intern)

Der vollständige zertifikatsspezifische Link ist dem Zertifikat selbst zu entnehmen.

Es werden regelmäßig Sperrlisten (engl. „Certification Revocation Lists“ kurz CRLs) aktualisiert und zur Verfügung gestellt. Der Link ist den jeweiligen Zertifikaten zu entnehmen.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

- IAV veröffentlicht für die Root- und Policy-CA die folgenden Informationen:
- Sperrliste der Root-CA
- Sperrliste der Policy-CA
- CP der Root- / Policy-CA

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Für die Veröffentlichung von Root-CA-/Policy-CA-Zertifikaten, Sperrlisten sowie CP und CPS gelten die folgenden Intervalle:

- Selbstsignierte Root-CA-Zertifikate unmittelbar nach Erzeugung mit Fingerprints und einem Gültigkeitszeitraum von 32 Jahren. Eine Erneuerung muss mindestens eine Woche vor Ablauf erfolgen.

- CA-Zertifikate, die von der Root-CA für nachfolgende CAs (Level 2) ausgestellt bzw. signiert werden, unmittelbar nach Erzeugung mit Fingerprints und einem Gültigkeitszeitraum von 16 Jahren. Eine Erneuerung muss mindestens eine Woche vor Ablauf erfolgen.
- CA-Zertifikate, die von der Policy-CA für nachfolgende CAs (Level 3) ausgestellt bzw. signiert werden, unmittelbar nach Erzeugung mit Fingerprints und einem Gültigkeitszeitraum von 8 Jahren. Eine Erneuerung muss mindestens eine Woche vor Ablauf erfolgen.
- Root-CA-Sperrlisten nach Sperrungen, sonst eine Woche vor Ablauf des Gültigkeitszeit-raum von 365 Tagen (siehe Kapitel 4.9.7)
- Policy-CA-Sperrlisten nach Sperrungen, sonst eine Woche vor Ablauf des Gültigkeitszeit-raum von 365 Tagen (siehe Kapitel 4.9.7)
- CP nach Erstellung bzw. Aktualisierung.

2.4 Zugriffskontrollen auf Verzeichnisse

Grundsätzlich muss der lesende Zugriff auf alle in Kapitel 2.2 aufgeführten Informationen ohne Zugriffskontrolle möglich sein. CA-Zertifikate und Sperrlisten müssen von allen IAV-PKI Nutzern abrufbar sein. Ein schreibender Zugriff für Änderungen der Verzeichnisinhalte (Zertifikate und Sperrlisten), Verzeichnisstruktur sowie CA-Konfigurationsänderungen muss ausschließlich auf Verantwortliche der IAV-PKI begrenzt sein. Diese CP kann von allen IAV-PKI Nutzern gelesen werden (vgl. Kap. 2.1).

3 Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

Root- und Policy-CA-Zertifikate müssen grundsätzlich Angaben zum Aussteller (*issuer*) und Zertifikatnehmer bzw. Endanwender (*subject*) enthalten. Diese Namen sind entsprechend dem Standard [X.501] als (*DistinguishedName = DN*) zu vergeben.

Die Namensregeln sind im Namenskonzept der IAV-PKI [IAV_NAMES_PKI] detailliert ausgewiesen.

3.1.2 Aussagekraft von Namen

Der Name eines ausgestellten Root- oder Policy-CA-Zertifikats (*DN*) muss den Zertifikatsnehmer eindeutig identifizieren. Grundsätzlich können Namen sich dabei auf natürliche Personen oder technische Entitäten beziehen.

3.1.3 Anonymität oder Pseudonymität der Zertifikatsinhaber

Die Root- als auch die Policy-CA dürfen keine anonymen und pseudonymen Zertifikate ausstellen.

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Der DN eines ausgestellten Root- oder Policy-CA-Zertifikats hat sich nach den Vorgaben des Standards [X.501] auszurichten.

3.1.5 Eindeutigkeit von Namen

Es muss sichergestellt werden, dass ein in Root- oder Policy-CA-Zertifikaten verwendeter Name (*DN*) des Zertifikatnehmers innerhalb der IAV-PKI und über den Lebenszyklus des Zertifikats hinaus stets eindeutig ist und stets dem gleichen Zertifikatnehmer zugeordnet ist. Abweichungen hiervon sind nur unter den unter 3.1.6 beschriebenen Voraussetzungen zulässig.

Darüber hinaus muss jedem Zertifikat durch die ausstellende Root- oder Policy-CA eine eindeutige Seriennummer zugeordnet werden, die eine eindeutige und unveränderliche Zuordnung zum Zertifikatnehmer ermöglicht.

3.1.6 Umgang mit Wildcard Zertifikaten

Wildcard Zertifikate werden nur für einen untergeordneten Namensraum angeboten (Child Domain). Dieser Namensraum ist einem IT Service fest zugeordnet und eindeutig. Die Beantragung von Wildcard Zertifikaten ist auf die Verantwortlichen des jeweiligen IT Services beschränkt. Die Verantwortlichen können für einen befristeten Zeitraum dritte Personen zur Beantragung berechtigen.

3.1.7 Anerkennung, Authentifizierung und Rolle von Markennamen

Keine Vorgaben für Root- und Policy CA.

3.2 Identitätsprüfung bei Neuantrag

3.2.1 Methoden zur Überprüfung des Besitzes des privaten Schlüssels

Die Schlüsselpaare der Root- und Policy-CA werden ausschließlich durch die IAV-PKI generiert.

3.2.2 Authentifizierung einer Organisation

Zertifikate für organisationsbezogene Entitäten (z.B. Sub-CA) werden immer von natürlichen Personen beantragt, deren Authentifizierung gemäß Kapitel 3.2.3 erfolgt.

3.2.3 Anforderungen zur Identifizierung und Authentifizierung natürlicher Personen

Die Registrierungsstellen der untergeordneten Sub-CAs (Level 3) gewährleisten eine zuverlässige Identifizierung und Prüfung der Antragsdaten im Rahmen der Integritäts-, Authentizitäts- und Vertraulichkeitsanforderungen gemäß ihrer Sicherheitsrichtlinie (siehe CP / CPS für Geräte-CA und Nutzer-CA), die sich am aktuellen Stand der Technik orientiert.

3.2.4 Nicht überprüfte Zertifikatsnehmerangaben

Es sind ausschließlich Angaben zur Authentifikation und Identifikation von Zertifikatsnehmern zu überprüfen. Andere Informationen des Zertifikatsnehmers dürfen nicht berücksichtigt werden.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Der Prozess für die Prüfung der Berechtigung zur Antragsstellung muss dokumentiert werden (CPS).

3.2.6 Kriterien für Cross-Zertifizierung und Interoperabilität

Nichtzutreffend. Eine Cross-Zertifizierung mit anderen Organisationen ist derzeit nicht geplant.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Keine Vorgaben für Root- und Policy-CA.

3.3.2 Zertifikatserneuerung nach einer Sperrung

Der Betreiber der IAV-PKI muss eine zuverlässige Identifizierung und Prüfung der bisherigen Antragsdaten im Rahmen seiner Sicherheitsrichtlinie gewährleisten.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Der Betreiber der IAV-PKI muss im Rahmen seiner Sicherheitsrichtlinie eine zuverlässige Identifizierung und Authentisierung des Antragstellers gewährleisten.

4 Ablauforganisation

4.1 Zertifikatsantrag

4.1.1 Wer kann einen Zertifikatsantrag stellen?

Zertifikate, die von der Root- oder Policy-CA ausgestellt werden sollen, können von den in Kapitel 1.3.3 benannten Zertifikatsnehmern beantragt werden. Ein geeignetes Verfahren für den Nachweis der Verantwortung muss dokumentiert sein.

4.1.2 Registrierungsprozess und Zuständigkeiten

Die Registrierung muss ein dokumentierter Prozess sein, der die Anforderungen der Identifizierung in Kapitel 3.2.3 erfüllt.

4.2 Bearbeitung von Zertifikatsanträgen

4.2.1 Durchführung der Identifizierung und Authentifizierung

Vor einer Registrierung sind die Zertifikatsnehmer zuverlässig nach einem dokumentierten Prozess zu identifizieren. Die Identifizierung und Authentifizierung ist gemäß den Vorgaben im Kapitel 3.2 durchzuführen.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Die Vorgaben zur Annahme eines Zertifikatsantrages sind zu dokumentieren. Eine Annahme darf nur für identifizierte Antragsteller erfolgen.

4.2.3 Bearbeitungsdauer von Zertifikatsanträgen

Keine Vorgaben für Root- und Policy-CA.

4.3 Ausstellung von Zertifikaten

4.3.1 Aufgaben der Zertifizierungsstelle

Eine Ausgabe von Zertifikaten darf nur für gültige Zertifikatsanträge erfolgen, die bei der Root- und Policy-CA manuell zu erstellen und durch den Betreiber der IAV-PKI zu dokumentieren sind. Die Aktionen bei der Zertifikatsausgabe müssen anhand dokumentierter Prozesse erfolgen. Dabei muss sichergestellt sein, dass eine eindeutige Verbindung von Zertifikatsnehmer und dem zugehörigen Schlüsselpaar besteht. Die Prüfung muss anhand dokumentierter Prozesse erfolgen. Nach Bearbeitung des Zertifikatsantrages ist das Schlüsselpaar im Sicherheitsbereich der IAV-PKI im Vier-Augen-Prinzip zu erstellen und das zugehörige Zertifikat zu erzeugen.

4.3.2 Benachrichtigung des Zertifikatsnehmers

Die Benachrichtigung des Zertifikatsnehmers hat anhand entsprechend dokumentierter Prozesse zu erfolgen.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme des Zertifikats

Der Prozess für die sichere Zertifikatsübergabe und die Bedingungen, die zu einer Annahme des Zertifikates durch den Teilnehmer führen, müssen dokumentiert werden. Die Annahme des Zertifikates muss mit der Bestätigung des Empfangs bzw. mit der Nutzung des Zertifikats erfolgen.

4.4.2 Veröffentlichung des Zertifikats durch die CA

Die CA-Zertifikate der Root- und der Policy-CA müssen für alle Teilnehmer der IAV-PKI veröffentlicht werden.

4.4.3 Benachrichtigung weiterer Instanzen

Eine Benachrichtigung weiterer Instanzen ist nicht erforderlich insofern die Root-CA, Policy-CA sowie die untergeordneten Sub-CA's (Level 3) im gleichem Verantwortungsbereich der IAV verbleiben.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Die Nutzung des privaten Schlüssels muss ausschließlich dem Zertifikatsnehmer vorbehalten sein.

Der im Zertifikat referenzierte private Schlüssel des Zertifikatsnehmers darf nur für Anwendungen benutzt werden, die in Übereinstimmung mit den im Zertifikat angegebenen Nutzungsarten stehen (siehe Kapitel 1.4.1).

Folgende Nutzungsarten sind zulässig:

- Signatur über ausgestellte Sub-CA-Zertifikate, d.h. Selbstsignierung bei Root-CA, Ausstellung des Policy-CA Zertifikats und Ausstellung von Sub-CA-Zertifikaten (Level 3).
- Signatur über ausgestellte Sperrlisten.

Es ist unverzüglich die Sperrung des Zertifikats zu veranlassen, wenn der private Schlüssel kompromittiert ist oder das Zertifikat nicht länger benötigt wird (siehe Kapitel 4.9).

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Die ausgestellten Zertifikate der Root- und Policy-CA können von allen Zertifikatsnutzern verwendet werden. Es kann jedoch nur dann darauf vertraut werden, wenn

- die Zertifikate entsprechend den dort vermerkten Nutzungsarten (Schlüsselverwendung, erweiterte Schlüsselverwendung, ggf. einschränkende Extensions) benutzt werden,
- die Verifikation der Zertifikatskette bis zu dem intern vertrauenswürdigen Root-CA-Zertifikat erfolgreich durchgeführt werden kann,
- der Status der Zertifikate über eine Sperrlistenprüfung positiv auf Gültigkeit überprüft wurde und
- alle weiteren in Vereinbarungen oder an anderer Stelle angegebenen Vorsichtsmaßnahmen getroffen wurden, eventuelle Einschränkungen im Zertifikat und jegliche anwendungsspezifischen Vorkehrungen seitens des Zertifikatsnutzers berücksichtigt und als kompatibel erkannt wurden.

4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (engl. „Certificate Renewal")

Eine CA-Zertifikatserneuerung auf Basis eines bestehenden Schlüsselpaares ist sowohl für die Root- als auch für die Policy-CA nicht zugelassen.

Eine Zertifikatserneuerung ist bei beiden CAs mit einer technischen Neuzertifizierung gleichzusetzen, d.h. das Zertifikat selbst, dessen Inhalte und das zugehörige Schlüsselpaar werden neu generiert und technische Parameter können u.U. angepasst werden (siehe Kapitel 4.8).

4.7 Zertifikatserneuerung mit Schlüsselerneuerung (engl. „Re-Keying“)

Eine CA-Zertifikatserneuerung, bei der ausschließlich das zugehörige Schlüsselpaar ohne sonstige Datenanpassungen neu generiert wird, ist sowohl für die Root- als auch für die Policy-CA nicht zugelassen.

Eine CA-Zertifikatserneuerung ist bei beiden CAs mit einer technischen Neuzertifizierung gleichzusetzen, d.h. das Zertifikat, dessen Inhalte sowie das zugehörige Schlüsselpaar werden neu generiert und technische Parameter angepasst (siehe Kapitel 4.8).

4.8 Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Im Rahmen der IAV-PKI findet eine CA-Zertifikatserneuerung für die Root- als auch für die Policy-CA antragsbasiert immer mit einem Wechsel des Schlüsselpaars und einer Anpassung von Zertifikatsinhalten sowie technischen Parametern statt.

Technisch bedeutet dies eine Neuzertifizierung.

4.8.1 Bedingungen für eine Zertifikatsänderung

Die nachfolgenden Gründe müssen zu einer Erneuerung von CA-Zertifikaten (von der Root- oder Policy-CA ursprünglich ausgestellt) mit Schlüsselwechsel und Datenanpassung führen:

- Routinemäßige Zertifikatserneuerung
    - bei bevorstehendem Ablauf der Gültigkeit des CA-Zertifikates oder
    - bereits erfolgtem Ablauf der Gültigkeit des Zertifikates.
- CA-Zertifikatsbeantragung nach einer Sperrung des bisherigen CA-Zertifikates.
- Die Daten des CA-Zertifikates entsprechen nicht oder nicht mehr den Tatsachen.
- Die Algorithmen, die Schlüssellänge oder die Gültigkeitsdauer des CA-Zertifikates bieten keine ausreichende Sicherheit mehr oder eine Erneuerung der Zertifikatsstruktur ist zwingend erforderlich.

4.8.2 Wer kann eine Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung beantragen?

Die Zertifikatserneuerung für die Root- oder Geräte-CA wird vom Zertifikatsnehmer (in diesem Fall der Betreiber der IAV-PKI) beantragt und ist von der Geschäftsführung der IAV zu prüfen, zu genehmigen und zu dokumentieren.

4.8.3 Ablauf der Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Der Prozess der Zertifikatserneuerung entspricht dem Verfahren der erstmaligen Antragsstellung (siehe Kapitel 4.1 ff.). Die Bearbeitung eines Antrags auf Zertifikatserneuerung muss ein dokumentierter Prozess sein, der die Anforderungen der Identifizierung nach Kapitel 3.2.3 erfüllt.

4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Nach Erstellung ist das entsprechende CA-Zertifikat dem Zertifikatsnehmer in geeigneter Weise sicher zu übermitteln. Die Benachrichtigung des Zertifikatsnehmers muss entsprechend dokumentierter Prozesse erfolgen.

4.8.5 Annahme der Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Die Annahme des CA-Zertifikates hat mit der Bestätigung des Empfangs bzw. mit der Nutzung des CA-Zertifikats zu erfolgen. Der Prozess für die sichere Zertifikatsübergabe und Bedingungen, die zu einer Annahme des CA-Zertifikates durch den Zertifikatsnehmer führen, muss dokumentiert werden.

4.8.6 Veröffentlichung der Zertifikatserneuerung durch die CA

Erneuerte Root- und Policy-CA-Zertifikate müssen unverzüglich allen Teilnehmern der IAV-PKI unter Berücksichtigung einer kaskadierten Erneuerung der abhängigen Endbenutzerzertifikate bekannt gemacht werden.

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

Eine Benachrichtigung über ein erneuertes CA-Zertifikat der Root- oder Policy-CA an weitere Instanzen ist nicht erforderlich insofern die Root-CA, Policy-CA sowie die untergeordneten Sub-CA's (Level 3) im gleichem Verantwortungsbereich der IAV verbleiben. Für Endbenutzerzertifikate gelten ebenso keine Vorgaben.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Gründe für eine Sperrung

Ein durch die Root- oder Policy-CA ausgestelltes CA-Zertifikat muss gesperrt werden, wenn mindestens eine der folgenden Situationen eintrifft:

- Die im CA-Zertifikat enthaltenen Angaben sind nicht oder nicht mehr gültig.
- Der Zertifikatsnehmer hält Verpflichtungen gemäß dieser CP bzw. des CPS nicht ein (siehe Kapitel 4.5).
- Die IAV-PKI stellt ihren Zertifizierungsbetrieb ein. In diesem Fall müssen sämtliche von ihr ausgestellten CA-Zertifikate als auch Endbenutzerzertifikate gesperrt werden.
- Der private Schlüssel der ausstellenden oder einer übergeordneten CA ist kompromittiert worden. In diesem Fall müssen sämtliche von diesen CAs ausgestellten CA-Zertifikate gesperrt werden.
- Die Algorithmen, die Schlüssellänge oder die Gültigkeitsdauer des CA-Zertifikates bieten keine ausreichende Sicherheit mehr. Die Betreiber der IAV-PKI behalten sich vor, die betreffenden CA-Zertifikate zu sperren.

4.9.2 Wer kann eine Sperrung beantragen?

Die Sperrung der Root-CA, Policy-CA und nachgelagerte Sub-CAs können durch die jeweiligen Verantwortlichen gesperrt werden. Hierzu zählen folgende Personen:

- Verantwortliche für die Root- und Policy-CA
- Beauftragter für Informationssicherheit der IAV

Die jeweilige ausführende CA muss die Prüfung und Durchführung der Sperrung dokumentieren.

4.9.3 Ablauf einer Sperrung

Die Beantragung einer Sperrung eines CA-Zertifikates muss schriftlich erfolgen und die Durchführung der Sperrung ist entsprechend zu dokumentieren.

Der Betreiber der IAV-PKI muss die Sperrung des CA-Zertifikates an der entsprechenden CA durchführen und die entsprechende Sperrliste unmittelbar veröffentlichen. Der Zertifikatsnehmer ist über die Sperrung des Zertifikates zu unterrichten.

Der Verfahrensablauf für die Verarbeitung des Sperrantrags ist detailliert zu dokumentieren.

4.9.4 Fristen für einen Sperrantrag

Die Zertifikatsnehmer sind bei bekannt werden eines Sperrgrundes verpflichtet, unverzüglich die Sperrung des entsprechenden Root- oder Policy-CA-Zertifikats zu veranlassen, d.h. Sperranträge sind unmittelbar nach Eintreten der Bedingung für eine Sperrung an die sperrberechtigten Personen der IAV-PKI zu übergeben.

4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle

Eine CA-Zertifikatssperrung muss unverzüglich nach Zugang des Sperrantrages und im Falle einer durchgeführten negativ ausgefallenen Risikoüberprüfung durch die sperrberechtigten Personen der IAV-PKI erfolgen.

4.9.6 Anforderungen zu Sperrprüfungen durch den Zertifikatsnutzer

Sperrinformationen müssen mittels Sperrlisten veröffentlicht werden. Zur Prüfung der Gültigkeit von Zertifikaten muss der Zertifikatsnutzer jeweils die aktuell veröffentlichte Sperrliste verwenden. Die Root- und Policy-CA müssen Sperrinformationen in Form von Sperrlisten (z.B. per HTTP und / oder LDAP) veröffentlichen.

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Die Root- und Policy-CA müssen spätestens alle 365 Tage jeweils eine neue Sperrliste ausstellen und publizieren. Eine Neuausstellung hat jeweils mindestens eine Woche vor Ablauf der letzten noch gültigen Sperrliste zu erfolgen.

Ist die Sperrung einer nachgeordneten Sub-CA notwendig, muss die entsprechende Sperrliste umgehend nach Sperrung publiziert werden. Sie ersetzt die bisher gültige Sperrliste unabhängig von deren ursprünglich angegebenen Gültigkeitsdauer.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die Veröffentlichung von Sperrlisten ist unmittelbar nach deren Erzeugung zu veranlassen. Die maximale Latenzzeit für Sperrlisten muss dokumentiert sein.

4.9.9 Verfügbarkeit von Online-Sperrinformationen

Sperrinformationen der Root- und Policy-CA müssen online in Form von herunterladbaren Sperrlisten zur Verfügung stehen.

4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen

Nichtzutreffend. Online Sperrungen und Statusprüfungen (z.B. mittels eines OCSP-Dienstes) stehen für die Prüfung der CA-Zertifikate der Root- und Policy-CA nicht zur Verfügung.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Nichtzutreffend. Andere Formen zur Anzeige von Sperrinformationen werden nicht angeboten.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Bei einer Kompromittierung des privaten Schlüssels der Root- oder der Policy-CA sind neben dem betroffenen CA-Zertifikat auch alle von der jeweils betroffenen CA ausgestellten Zertifikate unverzüglich zu sperren.

4.9.13 Bedingungen für eine Suspendierung

Eine temporäre Sperrung bzw. eine Suspendierung von CA-Zertifikaten ist weder für die Root- noch für die Policy-CA erlaubt. Einmal gesperrte CA-Zertifikate dürfen nicht reaktiviert werden.

4.9.14 Wer kann eine Suspendierung beantragen?

Nichtzutreffend.

4.9.15 Verfahren für Anträge auf Suspendierung

Nichtzutreffend.

4.9.16 Begrenzungen für die Dauer von Suspendierungen

Nichtzutreffend.

4.10 Statusabfragedienst für Zertifikate (OCSP)

4.10.1 Funktionsweise des Statusabfragedienstes

Nichtzutreffend.

4.10.2 Verfügbarkeit des Statusabfragedienstes

Nichtzutreffend.

4.10.3 Optionale Leistungen

Nichtzutreffend.

4.11 Beendigung der Zertifikatsnutzung durch den Zertifikatsnehmer

Eine Beendigung der Zertifikatsnutzung durch den Zertifikatsnehmer muss entweder durch die Sperrung des Zertifikates oder indem nach Ablauf der Gültigkeit kein neues Zertifikat beantragt wird erfolgen. Im Fall einer Kündigung durch den Zertifikatsnehmer muss das Zertifikat gesperrt werden.

4.12 Schlüsselhinterlegung und Wiederherstellung (engl. „Key Escrow and Recovery“)

4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

Eine Schlüsselhinterlegung und -wiederherstellung der Root- und Policy CA ist zulässig. Die notwendigen Sicherheitsmaßnahmen, Praktiken und Prozesse sind im zugehörigen CPS (Kapitel 5 und 6) detailliert zu hinterlegen.

4.12.2 Richtlinien und Praktiken zum Schutz von Sitzungsschlüsseln und deren Wiederherstellung

Sitzungsschlüssel der Geräte-CA werden mit gängigen kryptographischen Mechanismen abgesichert und nicht wiederhergestellt.

5 Nicht-technische Sicherheitsmaßnahmen

Die Gewährleistung geeigneter infrastruktureller, organisatorischer und personeller Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb der IAV-PKI. Diese nicht-technischen Sicherheitsmaßnahmen werden für die Root- und Policy-CA in diesem Kapitel in ihren Grundzügen beschrieben. Detaillierte Informationen sind Organisationshandbuch festgeschrieben [IAV_ORG_PKI]. Die nicht-technischen Sicherheitsmaßnahmen erfolgen anhand dokumentierter Prozesse und orientieren sich am aktuellen Stand der Technik und Best Practices z.B. basierend auf den Empfehlungen des BSI [IT-GSHB]. Die Prozesse und begleitenden Sicherheitsmaßnahmen sind vom Betreiber und Teilnehmern der IAV-PKI ordnungsgemäß zu erbringen, um die in Kapitel 4 beschriebenen Betriebsanforderungen zu erfüllen.

6 Technische Sicherheitsmaßnahmen

Die Gewährleistung geeigneter technischer Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb der IAV-PKI. Diese Sicherheitsmaßnahmen werden für die Root- und Geräte-CA in diesem Kapitel in ihren Grundzügen beschrieben. Detaillierte Informationen sollten in einem Sicherheitskonzept festgeschrieben werden. Technische Sicherheitsmaßnahmen erfolgen anhand dokumentierter Prozesse und Vorgaben, die sich am aktuellen Stand der Technik und Good Practices orientieren z.B. basierend auf den Empfehlungen des BSI [IT-GSHB]. Diese Sicherheitsmaßnahmen werden vom Betreiber und Teilnehmern der IAV-PKI ordnungsgemäß zu erbringen, um die in Kapitel 4. beschriebenen Anforderungen zu erfüllen.

Die verwendeten kryptographischen Verfahren und Protokolle müssen dem aktuellen Stand der Sicherheitsbetrachtungen kryptographischer Verfahren z.B. basierend auf [BSI-TR] und den jeweils gültigen gesetzlichen Vorgaben unter Berücksichtigung der technischen Möglichkeiten betroffener Anwendungen entsprechen.

7 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen (OCSP)

7.1 Zertifikatsprofile

Die Profile für Zertifikate und Sperrlisten werden anhand des Dokuments „IAV-PKI Zertifikatsprofile“ [IAV_PROFILE] im Detail spezifiziert.

7.1.1 Versionsnummern

CA-Zertifikate der Root- und Policy CA müssen konform der internationalen Norm [X.509] in der Version 3 (Typ 0x2) ausgestellt werden.

7.1.2 Zertifikatserweiterungen

Grundsätzlich sind alle Zertifikatserweiterungen nach den Standards [X.509], [PKIX] und [PKCS] zulässig.

In den CA-Zertifikaten müssen die Erweiterung „*keyUsage*“ mit den Werten „*keyCertSign*" und „*cRLSign*" sowie die Erweiterung „*basicConstraints*“ mit dem Wert "*CA=True*" aufgenommen werden.

Folgende Zertifikatserweiterungen müssen kritisch sein:

- *KeyUsage*,
- *BasicConstraints* (nur obligatorisch, wenn es sich um ein CA-Zertifikat handelt).

Grundsätzlich wird empfohlen, möglichst wenige Zertifikatserweiterungen auf kritisch („critical“) zu setzen.

7.1.3 Algorithmus Bezeichner OIDs

Objekt Identifikatoren für Algorithmen sind nach den Vorgaben des Standards [PKIX] zu verwenden.

7.1.4 Namensformen

Siehe Kapitel 3.1.

7.1.5 Namensbeschränkungen

Siehe Kapitel 3.1.

7.1.6 OIDs der Zertifikatsrichtlinien

Es wird empfohlen, die OID dieser CP als nicht kritische Erweiterung in das Attribut „*certificatePolicies*“ mit einem Verweis auf den Ort der Ablage einzutragen, wo diese Policy gespeichert wird.

7.1.7 Nutzung von Erweiterungen zu Richtlinienbeschränkungen (engl. „Policy Constraints“)

Keine Vorgaben für Root- und Policy-CA.

7.1.8 Syntax und Semantik von Richtlinienkennungen (engl. „Policy Qualifiers“)

Keine Vorgaben für Root- und Policy-CA.

7.1.9 Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien (engl. „certificatePolicies“)

Keine Vorgaben für Root- und Policy-CA.

7.2 Sperrlistenprofile (CRL)

7.2.1 Versionsnummer(n)

Es müssen Sperrlisten gemäß der internationalen Norm [X.509] in der Version 1 (Typ 0x0) oder 2 (Typ 0x1) eingesetzt werden.

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

Keine Vorgaben für Root- und Policy-CA.

7.3 Profile des Statusabfragedienstes (OCSP)

Nichtzutreffend.

8 Konformitätsprüfung (engl. "Compliance Audit")

Die Arbeitsprozesse der Root- und Policy-CA sind regelmäßig bzw. anlassbezogen zu überprüfen.

Audits für den technischen Aufbau der IAV-PKI und die damit verbundenen operativen Abläufe sind in regelmäßigen Abständen durch interne oder extern bestellte Auditoren nach den in der IAV für solche Vorgänge festgelegten Regeln durchzuführen. Die Ergebnisse der Audits müssen nicht veröffentlicht werden.

8.1 Frequenz und Umstände der Überprüfung

Grundsätzlich müssen interne Audits und Prüfungen im Rahmen des Audit-Managements von IAV durchgeführt werden.

8.2 Identität und Qualifikation des Überprüfers

Die internen Prüfungen sind durch die Unternehmenssicherheit, durch den Betreiber sowie die Leitung der IAV-PKI vorzunehmen. Die Prüfer müssen über das Know-how sowie die notwendigen Kenntnisse auf dem Gebiet Public Key Infrastructure (PKI) verfügen, um die Prüfungen vornehmen zu können. Gegebenenfalls müssen externe Auditoren hinzugezogen werden.

8.3 Verhältnis von Prüfer zu Überprüftem

Der Prüfer darf nicht in den Produktionsprozess der IAV-PKI eingebunden sein. Eine Selbstüberprüfung ist nicht ausreichend.

8.4 Überprüfte Bereiche

Es können alle für die IAV-PKI relevanten Bereiche überprüft werden. Die Prüfungsinhalte obliegen dem Prüfer.

8.5 Mängelbeseitigung

Festgestellte Mängel müssen in Abstimmung zwischen den Betreibern der IAV-PKI und Prüfer zeitnah beseitigt werden. Der Prüfer ist über die Beseitigung der Mängel zu informieren. Die umgesetzten Maßnahmen für die Mängelbeseitigung sind zu dokumentieren.

8.6 Veröffentlichung der Ergebnisse

Eine Veröffentlichung der Prüfungsergebnisse muss nicht stattfinden.

9 Weitere geschäftliche und rechtliche Regelungen

Das folgende Kapitel bezieht sich auf die komplette IAV-PKI, d.h. es umfasst alle Systemkomponenten, d.h. neben der Root- und Policy-CA auch die nachgelagerten fachlichen CAs (zur Zeit Geräte-CA und Nutzer-CA) auf Level 3.

9.1 Gebühren

Nichtzutreffend.

9.2 Finanzielle Verantwortung

Nichtzutreffend.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertraulich zu behandelnde Daten

Die folgenden geschäftlichen Informationen und Daten, welche nicht unter Kapitel 9.3.2 fallen, sind als vertraulich zu behandeln:

- Protokollierungen der CA-Anwendungen
- Privates Schlüsselmaterial
- Transaktionsprotokollierungen
- Interne / externe Auditberichte
- Business Continuity und Desaster Recovery Pläne
- Technische und organisatorische Schutzmaßnahmen, die den Betrieb der IAV-PKI, d.h. die verwendete Hardware, Software sowie die benötigten Administrationsprozesse absichern. Hierzu zählen auch CPS und das Organisationshandbuch.
- Daten, die u.U. in Zertifikatsanträgen enthalten sind, aber nicht im ausgestellten Zertifikat auftauchen (Serverinformationen, IP-Adressen etc.)

9.3.2 Nicht vertraulich zu behandelnde Daten

Alle Informationen und Daten, die in herausgegebenen CA-Zertifikaten, Geräte- oder Nutzer-Zertifikaten und Sperrlisten explizit (z.B. E-Mailadresse) oder implizit (z.B. Daten über die Zertifizierung) enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft.[2]

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

IAV GmbH trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen.

9.4 Schutz personenbezogener Daten

Nichtzutreffend.

9.4.1 Richtlinie zur Verarbeitung personenbezogener Daten

Nichtzutreffend.

9.4.2 Vertraulich zu behandelnde Daten

Nichtzutreffend.

9.4.3 Nicht vertraulich zu behandelnde Daten

Nichtzutreffend.

9.4.4 Verantwortung zum Schutz personenbezogener Daten

Nichtzutreffend.

9.4.5 Nutzung personenbezogener Daten

Nichtzutreffend.

9.4.6 Offenlegung bei gerichtlicher Anordnung oder im Rahmen einer gerichtlichen Beweisführung

Nichtzutreffend.

9.4.7 Andere Umstände einer Veröffentlichung

Nichtzutreffend.

9.5 Urheberrechte

IAV ist Urheber dieses Dokumentes. Das Dokument kann unverändert an Dritte weitergegeben werden.

9.6 Verpflichtungen

Beantragende Systembetreiber und Genehmiger innerhalb des Beantragungsprozesses werden auf die Verpflichtungen hingewiesen und stimmen mit der Freigabe des Antrages ausdrücklich zu.

9.6.1 Verpflichtung der Zertifizierungsstellen

IAV GmbH verpflichtet sich, den Bestimmungen dieser CP zu folgen.

---

[2] Dies ist begründet durch den öffentlichen Charakter eines Zertifikats bzw. einer Sperrliste, da diese z.B. (externen) Kommunikationspartnern zur Verfügung gestellt werden, um z.B. die Gültigkeit einer erstellten Signatur (Vertrauenskette, Gültigkeitszeitraum etc.) überprüfbar zu machen.

9.6.2 Verpflichtung der Registrierungsstellen

IAV GmbH sowie die in die Registrierung eingebundenen Stellen verpflichten sich, den Bestimmungen dieser CP zu folgen.

9.6.3 Verpflichtung des Zertifikatsnehmers

Die Verpflichtung des Zertifikatsnehmers ist in Kapitel 4.5.1 geregelt.

9.6.4 Verpflichtung des Zertifikatsnutzers

Die Verpflichtung des Zertifikatsnutzers ist in Ziffer 4.5.2 geregelt. Darüber hinaus muss er den Zertifikatsrichtlinien von IAV GmbH folgen.

9.6.5 Verpflichtung anderer Teilnehmer

Von IAV-PKI beauftragte Dienstleister werden auf die Einhaltung dieser CP verpflichtet.

9.7 Gewährleistung

Nichtzutreffend.

9.8 Haftungsbeschränkung

Nichtzutreffend.

9.9 Haftungsfreistellung

Bei der unsachgemäßen Verwendung eines von der Root- & Policy-CA ausgestellten Zertifikats und dem zugehörigen privaten Schlüssel oder einer Verwendung des Schlüsselmaterials, beruhend auf fälschlichen oder fehlerhaften Angaben bei der Beantragung, ist IAV von der Haftung freigestellt.

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Diese CP tritt an dem Tag in Kraft, an dem es gemäß Kapitel 2.2 veröffentlicht wird.

9.10.2 Aufhebung

Dieses Dokument ist so lange gültig, bis es durch eine neue Version ersetzt wird oder der Betrieb der IAV-PKI eingestellt wird.

9.10.3 Konsequenzen der Aufhebung

Von den Konsequenzen der Aufhebung diese CP bleibt die Verantwortung zum Schutz vertraulicher Informationen und personenbezogener Daten unberührt.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

In dieser Zertifizierungsrichtlinie werden keine entsprechenden Regelungen getroffen.

9.12 Änderungen der Richtlinie

9.12.1 Vorgehen bei Änderungen

Änderungen der CP werden rechtzeitig vor ihrem Inkrafttreten veröffentlicht.

9.12.2 Benachrichtigungsmethode und -fristen

Die Zertifikatsnehmer werden rechtzeitig vor dem Inkrafttreten auf die Änderung der CP hingewiesen. Beschäftigten von IAV sowie externen Mitarbeitern gegenüber gilt die im Intranet von IAV bekannt gemachte jeweils aktuelle Fassung der CP.

9.12.3 Bedingungen für die Änderung des Richtlinienbezeichners (OID)

Der Richtlinienbezeichner ändert sich bis zum Ende der Gültigkeit der zugehörigen Zertifizierungsinstanz nicht.

9.13 Schiedsverfahren

Nichtzutreffend.

9.14 Gerichtsstand

Sitz:	Berlin
Registergericht:	Amtsgericht Charlottenburg
Registernummer:	HRB 21 280
USt-Ident-Nummer:	DE 136647090

9.15 Konformität mit geltendem Recht

Die von der IAV-PKI ausgestellten Zertifikate sind nicht konform zu qualifizierten Zertifikaten gemäß Signaturgesetz.

9.16 Weitere Regelungen

9.16.1 Vollständigkeit

Alle Regelungen in dieser CP gelten für die Betreiber und Nutzer der IAV-PKI. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2 Abtretung der Rechte

Nichtzutreffend.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Zertifizierungsrichtlinie unwirksam sein oder werden, so lässt dies den übrigen Inhalt der Zertifizierungsrichtlinie unberührt. Auch eine Lücke berührt nicht die Wirksamkeit der Zertifizierungsrichtlinie im Übrigen. Anstelle der unwirksamen Bestimmung gilt diejenige wirksame Bestimmung als vereinbart, welche der ursprünglich gewollten am nächsten kommt oder nach Sinn und Zweck der Zertifizierungsrichtlinie geregelt worden wäre, sofern der Punkt bedacht worden wäre.

9.16.4 Rechtliche Auseinandersetzungen / Erfüllungsort

Nichtzutreffend.

9.16.5 Höhere Gewalt

Nichtzutreffend.

9.17 Andere Regelungen

Nichtzutreffend.

10 Verzeichnisse

10.1 Abbildungsverzeichnis

10.2 Tabellenverzeichnis

10.3 Abkürzungsverzeichnis

Abkürzung	Erklärung
AD	Active Directory
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority, dt. Zertifizierungsstelle
CDP	Certificate Distribution Point, dt. Sperrlistenverteilpunkt
CMC	Certificate Management over CMS
CN	Common Name (Bestandteil des Distinguished Name)
CP	Certificate Policy; dt. Zertifizierungsrichtlinie einer PKI
CPS	Certificate Practice Statement, dt. Regelungen für den Zertifizierungsbetrieb
CRA	Central Registration Authority, dt. Zentrale Registrierungsstelle
CRL	Certificate Revocation List, dt. Sperrliste
DN	Distinguished Name
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IAV	Ingenieurgesellschaft Auto und Verkehr
IT	Information Technology
LAN	Local Area Network

Abkürzung	Erklärung
LDAP	Lightweight Directory Access Protocol
LDAPs	Lightweight Directory Access Protocol secure
LRA	Local Registration Authority, dt. lokale Registrierungsstelle
O	Organization (Bestandteil des Distinguished Name)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit (Bestandteil des Distinguished Name)
PIN	Personal Identification Number; dt. Persönliche Identifikationsnummer
PKCS#10	Public Key Cryptographic Standard – Certificate Request Standard
PKI	Public Key Infrastructure, dt. Zertifizierungsinfrastruktur
PROFI	Prozesse für IAV
PW	Personalwesen IAV
RA	Registration Authority, dt. Registrierungsstelle
RFC	Request for Comment, Dokumente für weltweite Standardisierungen
RFC3647	Dieser RFC dient der Beschreibung von Dokumenten, die den Betrieb einer PKI beschreiben
Root-CA	Oberste Zertifizierungsinstanz einer PKI
SCEP	Simple Certificate Enrollment Protocol
Sperrliste	Signierte Liste einer CA, die gesperrte Zertifikate enthält
SW	Software
X.500	Protokolle und Dienste für ISO konforme Verzeichnisse
X.509	Zertifizierungsstandard
Zertifikat	Sichere Zuordnung von öffentlichen Schlüsseln zu einem Teilnehmer

10.4 Glossar

Begriff	Beschreibung

11 Dokumenteninformation

Änderungshistorie

Version	Datum	Autor	Änderungen
0.1	17.11.14	Ulrich Müller	Initiale Struktur
0.2	19.11.14	Ulrich Müller	Erstellung Inhalte Kapitel 1-4
0.3	20.11.14	Ulrich Müller	Erstellung Inhalte Kapitel 5-10
0.4	21.11.14	Ulrich Müller	Erstellung einer Draftversion als Vorlage für erste Prüfung durch IAV
1.0	02.12.14	Stephan Wappler	IBM internes Review der Draftversion
1.2	12.12.14	Ulrich Müller	Einarbeitung Ergebnisse aus dem Workshop vom 11.12.14
1.3	16.12.14	Ulrich Müller	Einarbeitung weiterer Ergebnisse aus dem Workshop vom 15.12.14
1.4	23.01.15	IAV	Feedback seitens IAV
1.6	02.11.15	Peter Steiert	Freigabefassung
1.7	16.11.15	Karsten Meichsner	Korrekturen bezüglich Anmerkungen IT-Sicherheitsbeauftragter
1.8.	19.11.15	Karsten Meichsner	Korrektur Klimatisierung und Notstromversorgung.
1.9	25.09.17	Marc Plagge	Anpassung Root- und Policy CRL Intervall auf 365
1.10	03.06.20	Bastian Müller	Aktualisierungen und Anpassung Ansprechpartner / Verantwortliche
1.11	03.08.20	Bastian Müller	Vollständige Überarbeitung

Verteiler

Empfänger	Firma/Abteilung	E-Mail-Adresse	Bemerkung
Karsten Keusch	IAV / C-IT	karten.keusch[at]iav.de	
Marc Plagge	IAV / C-IT	marc.plagge[at]iav.de	
Bastian Müller	IAV / C-IT	bastian.mueller[at]iav.de	

Mitgeltende Dokumente

Nr.	Dokumenten-Titel	Version	Dateiname und Ablage
[01]	[IAV_ORG_PKI]	1.1	IAV (2014): IAV-PKI Organisationshandbuch
[02]	[IAV_NAMES_PKI]	1.10	IAV (2015): IAV-PKI Profile
[03]	[IAV_PROFILE]	1.10	IAV (2015): IAV-PKI Profile

Nr.	Dokumenten-Titel	Version	Dateiname und Ablage
[04]	[IAV_PASSWORT]		IAV (2013): IAV IT-SecurityPolicy – Passwortsicherheit 212D
[05]	[IAV_BACKUP]		IAV (2014): IAV IT-Security Policy – Backup und Archivierung SP-208D.IAV
[06]	[IAV_CP_ROOT_POLICY]	1.10	IAV (2020): IAV Certificate Policy – Root- und Policy-CA
[07]	[IAV_ESKALATIONSPROZEDUR]		IAV (2015): Sicherheitsvorfälle und IT-Security Eskalationsprozedur DP-402D.IAV
[08]	[IAV_BENUTZERIDENTIFIKATION]		IAV (2016): IAV IT-SecurityPolicy – Benutzeridentifikation DD-740D.IAV
[09]	[IAV_KRYPTO]		IAV (2015): IAV IT-SecurityPolicy Anwendung kryptografischer Verfahren SP-220D.IAV
[10]	[IAV_NETZWERK]		IAV (2017): IAV IT-SecurityPolicy Netzwerke/Datenkommunikation SP-207D.IAV
[11]	[IAV_EDV_RAUM]		IAV (2015): IAV IT-SecurityPolicy - Baulich technische Anforderungen an EDV-Räume DP-409D.IAV

Weitere Referenzierungen

Quelle	Herausgeber (Erscheinungsdatum): Titel
[BSI-TR]	BSI Technische Richtlinie – Kryptographische Verfahren: Empfehlungen und Schlüssellängen - BSI TR-02102-1, Version 2014-01, Stand 10.2.2014 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102_pdf
[IT-GSHB]	IT-Grundschutz – die Basis für IT-Sicherheit, http://www.bsi.bund.de/gshb/
[PKCS]	RSA Security Inc., RSA Laboratories "Public Key Cryptography Standards", http://www.rsasecurity.com/rsalabs
[PKIX]	RFCs und Spezifikationen der IETF Arbeitsgruppe Public Key Infrastructure (X.509)
[RFC2119]	Key words for use in RFCs to Indicate Requirement Levels, Network Working Group, 1997 https://www.ietf.org/rfc/rfc2119.txt
[RFC2560]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP https://www.ietf.org/rfc/rfc2560.txt

Quelle	Herausgeber (Erscheinungsdatum): Titel
[RFC3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003 https://www.ietf.org/rfc/rfc3647.txt
[RFC5019]	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments https://www.ietf.org/rfc/rfc5019.txt
[X.501]	Information technology – Open Systems Interconnection - The Directory: Models https://www.itu.int/rec/T-REC-X.501
[X.509]	Information technology - Open Systems Interconnection - The Directory: Authentication framework https://www.itu.int/rec/T-REC-X.509
[X.520]	Information technology - Open Systems Interconnection - The Directory: Selected attribute types https://www.itu.int/rec/T-REC-X.520

12 Anhang

IAV GmbH
Carnotstraße 1
10587 Berlin
GERMANY

Tel. +49 30 3997-80
Fax +49 30 3997-89790
contact@iav.com

www.iav.com