

Zertifikatsrichtlinie IAV GmbH

Geräte-CA



Zertifikatsrichtlinie IAV GmbH

Geräte-CA

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

Dateiname: IAV - CP_CPS_Geräte_CA V1.3.docx

Version: 1.3

Status: Freigegeben (extern)

Geheimhaltungsstufe: Öffentlich

	Datum	Name	Abteilung
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	7
1.1	Überblick.....	7
1.1.1	Ziel dieser Richtlinie.....	8
1.1.2	Konventionen.....	8
1.1.3	Gültigkeit.....	8
1.2	Name und Kennzeichnung des Dokuments	8
1.3	PKI-Teilnehmer.....	8
1.3.1	Zertifizierungsstellen	8
1.3.2	Registrierungsstellen	8
1.3.3	Zertifikatsnehmer	8
1.3.4	Zertifikatsnutzer	9
1.3.5	Weitere Teilnehmer	9
1.4	Verwendung von Zertifikaten	9
1.4.1	Erlaubte Verwendungen von Zertifikaten	9
1.4.2	Verbotene Verwendungen von Zertifikaten	9
1.5	Verwaltung der Zertifizierungsrichtlinien.....	9
1.5.1	Zuständigkeit für das Dokument	9
1.5.2	Ansprechpartner und Kontakt	9
1.5.3	Prüfung der Zertifizierungsrichtlinie.....	9
1.6	Definitionen und Abkürzungen	9
2	Verantwortlichkeit für Verzeichnisse und Veröffentlichungen.....	10
2.1	Verzeichnisse	10
2.2	Veröffentlichung von Informationen zur Zertifikatserstellung	10
2.3	Zeitpunkt und Häufigkeit von Veröffentlichungen	10
2.4	Zugriffskontrollen auf Verzeichnisse	11
3	Identifizierung und Authentifizierung.....	11
3.1	Namensregeln	11
3.1.1	Arten von Namen.....	11
3.1.2	Aussagekraft von Namen.....	11
3.1.3	Anonymität oder Pseudonymität der Zertifikatsinhaber	11
3.1.4	Regeln für die Interpretation verschiedener Namensformen	11
3.1.5	Eindeutigkeit von Namen	11
3.1.6	Umgang mit Wildcard Zertifikaten	11
3.1.7	Anerkennung, Authentifizierung und Rolle von Markennamen.....	12
3.2	Identitätsprüfung bei Neuantrag.....	12
3.2.1	Methoden zur Überprüfung des Besitzes des privaten Schlüssels	12
3.2.2	Authentifizierung einer Organisation	12

3.2.3	Anforderungen zur Identifizierung und Authentifizierung natürlicher Personen	12
3.2.4	Nicht überprüfte Zertifikatsnehmerangaben	12
3.2.5	Prüfung der Berechtigung zur Antragstellung.....	12
3.2.6	Kriterien für Cross-Zertifizierung und Interoperabilität	12
3.3	Identifizierung und Authentifizierung bei einer Zertifikatserneuerung	12
3.3.1	Routinemäßige Zertifikatserneuerung	12
3.3.2	Zertifikatserneuerung nach einer Sperrung	12
3.4	Identifizierung und Authentifizierung von Sperranträgen	12
4	Ablauforganisation.....	13
4.1	Zertifikatsantrag	13
4.1.1	Wer kann einen Zertifikatsantrag stellen?	13
4.1.2	Registrierungsprozess und Zuständigkeiten	13
4.2	Bearbeitung von Zertifikatsanträgen	13
4.2.1	Durchführung der Identifizierung und Authentifizierung.....	13
4.2.2	Annahme oder Ablehnung von Zertifikatsanträgen	13
4.2.3	Bearbeitungsdauer von Zertifikatsanträgen.....	13
4.3	Ausstellung von Zertifikaten	13
4.3.1	Aufgaben der Zertifizierungsstelle.....	13
4.3.2	Benachrichtigung des Zertifikatsnehmers	13
4.4	Zertifikatsakzeptanz.....	13
4.4.1	Annahme des Zertifikats	13
4.4.2	Veröffentlichung des Zertifikats durch die CA	14
4.4.3	Benachrichtigung weiterer Instanzen	14
4.5	Verwendung des Schlüsselpaares und des Zertifikats	14
4.5.1	Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer	14
4.5.2	Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer ...	14
4.6	Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (engl. „Certificate Renewal“)	14
4.7	Zertifikatserneuerung mit Schlüsselerneuerung (engl. Re-Keying).....	14
4.8	Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung.....	15
4.8.1	Bedingungen für eine Zertifikatsänderung.....	15
4.8.2	Wer kann eine Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung beantragen?	15
4.8.3	Ablauf der Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung	15
4.8.4	Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats ...	15
4.8.5	Annahme der Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung.....	15
4.8.6	Veröffentlichung der Zertifikatserneuerung durch die CA.....	15
4.8.7	Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines neuen Zertifikats .	16

4.9	Sperrung und Suspendierung von Zertifikaten	16
4.9.1	Gründe für eine Sperrung	16
4.9.2	Wer kann eine Sperrung beantragen?	16
4.9.3	Ablauf einer Sperrung	16
4.9.4	Fristen für einen Sperrantrag	16
4.9.5	Bearbeitungsfristen für die Zertifizierungsstelle	16
4.9.6	Anforderungen zu Sperrprüfungen durch den Zertifikatsnutzer	17
4.9.7	Häufigkeit der Veröffentlichung von Sperrlisten	17
4.9.8	Maximale Latenzzeit für Sperrlisten	17
4.9.9	Verfügbarkeit von Online-Sperrinformationen	17
4.9.10	Anforderungen zur Online-Prüfung von Sperrinformationen	17
4.9.11	Andere Formen zur Anzeige von Sperrinformationen	17
4.9.12	Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels	17
4.9.13	Bedingungen für eine Suspendierung	17
4.9.14	Wer kann eine Suspendierung beantragen?	17
4.9.15	Verfahren für Anträge auf Suspendierung	17
4.9.16	Begrenzungen für die Dauer von Suspendierungen	17
4.10	Statusabfragedienst für Zertifikate (OCSP)	17
4.10.1	Funktionsweise des Statusabfragedienstes	17
4.10.2	Verfügbarkeit des Statusabfragedienstes	18
4.10.3	Optionale Leistungen	18
4.11	Beendigung der Zertifikatsnutzung durch den Zertifikatsnehmer	18
4.12	Schlüssel hinterlegung und Wiederherstellung (engl. „Key Escrow and Recovery“)	18
4.12.1	Richtlinien und Praktiken zur Schlüssel hinterlegung und -wiederherstellung	18
4.12.2	Richtlinien und Praktiken zum Schutz von Sitzungsschlüsseln und deren Wiederherstellung	18
5	Nicht-technische Sicherheitsmaßnahmen	18
6	Technische Sicherheitsmaßnahmen	18
7	Profile für Zertifikate, Sperrlisten und Online-Statusabfragen (OCSP)	19
7.1	Zertifikatsprofile	19
7.1.1	Versionsnummern	19
7.1.2	Zertifikatserweiterungen	19
7.1.3	Algorithmus Bezeichner OIDs	19
7.1.4	Namensformen	19
7.1.5	Namensbeschränkungen	19
7.1.6	OIDs der Zertifikatsrichtlinien	19
7.1.7	Nutzung von Erweiterungen zu Richtlinienbeschränkungen (engl. „Policy Constraints“)	19

7.1.8	Syntax und Semantik von Richtlinienkennungen (engl. „Policy Qualifiers“)	19
7.1.9	Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien (engl. „certificatePolicies“)	20
7.2	Sperrlistenprofile (CRL)	20
7.2.1	Versionsnummer(n)	20
7.2.2	Erweiterungen von Sperrlisten und Sperrlisteneinträgen	20
7.3	Profile des Statusabfragedienstes (OCSP)	20
8	Konformitätsprüfung (engl. "Compliance Audit")	20
8.1	Frequenz und Umstände der Überprüfung	20
8.2	Identität und Qualifikation des Überprüfers	20
8.3	Verhältnis von Prüfer zu Überprüfem	20
8.4	Überprüfte Bereiche	20
8.5	Mängelbeseitigung	20
8.6	Veröffentlichung der Ergebnisse	21
9	Weitere geschäftliche und rechtliche Regelungen	21
9.1	Gebühren	21
9.2	Finanzielle Verantwortung	21
9.3	Vertraulichkeit von Geschäftsinformationen	21
9.3.1	Vertraulich zu behandelnde Daten	21
9.3.2	Nicht vertraulich zu behandelnde Daten	21
9.3.3	Verantwortung zum Schutz vertraulicher Informationen	21
9.4	Schutz personenbezogener Daten	22
9.4.1	Richtlinie zur Verarbeitung personenbezogener Daten	22
9.4.2	Vertraulich zu behandelnde Daten	22
9.4.3	Nicht vertraulich zu behandelnde Daten	22
9.4.4	Verantwortung zum Schutz personenbezogener Daten	22
9.4.5	Nutzung personenbezogener Daten	22
9.4.6	Offenlegung bei gerichtlicher Anordnung oder im Rahmen einer gerichtlichen Beweisführung	22
9.4.7	Andere Umstände einer Veröffentlichung	22
9.5	Urheberrechte	22
9.6	Verpflichtungen	22
9.6.1	Verpflichtung der Zertifizierungsstellen	22
9.6.2	Verpflichtung der Registrierungsstellen	22
9.6.3	Verpflichtung des Zertifikatsnehmers	22
9.6.4	Verpflichtung des Zertifikatsnutzers	22
9.6.5	Verpflichtung anderer Teilnehmer	23
9.7	Gewährleistung	23

9.8	Haftungsbeschränkung	23
9.9	Haftungsfreistellung	23
9.10	Inkrafttreten und Aufhebung.....	23
9.10.1	Inkrafttreten	23
9.10.2	Aufhebung	23
9.10.3	Konsequenzen der Aufhebung.....	23
9.11	Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern	23
9.12	Änderungen der Richtlinie.....	23
9.12.1	Vorgehen bei Änderungen	23
9.12.2	Benachrichtigungsmethode und -fristen	23
9.12.3	Bedingungen für die Änderung des Richtlinienbezeichners (OID).....	23
9.13	Schiedsverfahren.....	24
9.14	Gerichtsstand	24
9.15	Konformität mit geltendem Recht.....	24
9.16	Weitere Regelungen	24
9.16.1	Vollständigkeit.....	24
9.16.2	Abtretung der Rechte.....	24
9.16.3	Salvatorische Klausel.....	24
9.16.4	Rechtliche Auseinandersetzungen / Erfüllungsort	24
9.16.5	Höhere Gewalt.....	24
9.17	Andere Regelungen.....	24
10	Verzeichnisse	24
10.1	Abbildungsverzeichnis	24
10.2	Tabellenverzeichnis	25
10.3	Abkürzungsverzeichnis	25
10.4	Glossar	26
11	Dokumenteninformation	27
12	Anhang.....	29

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 die für die Benutzer und IAV als PKI-Betreiber verbindlichen Vorgaben und Anforderungen zusammen, die im Rahmen der Bereitstellung und des Betriebs der Systemkomponente Geräte-CA sowie für die von ihr ausgestellten [X.509] konformen Zertifikate umzusetzen sind. Die folgende Abbildung veranschaulicht den Geltungsbereich dieser Richtlinie:

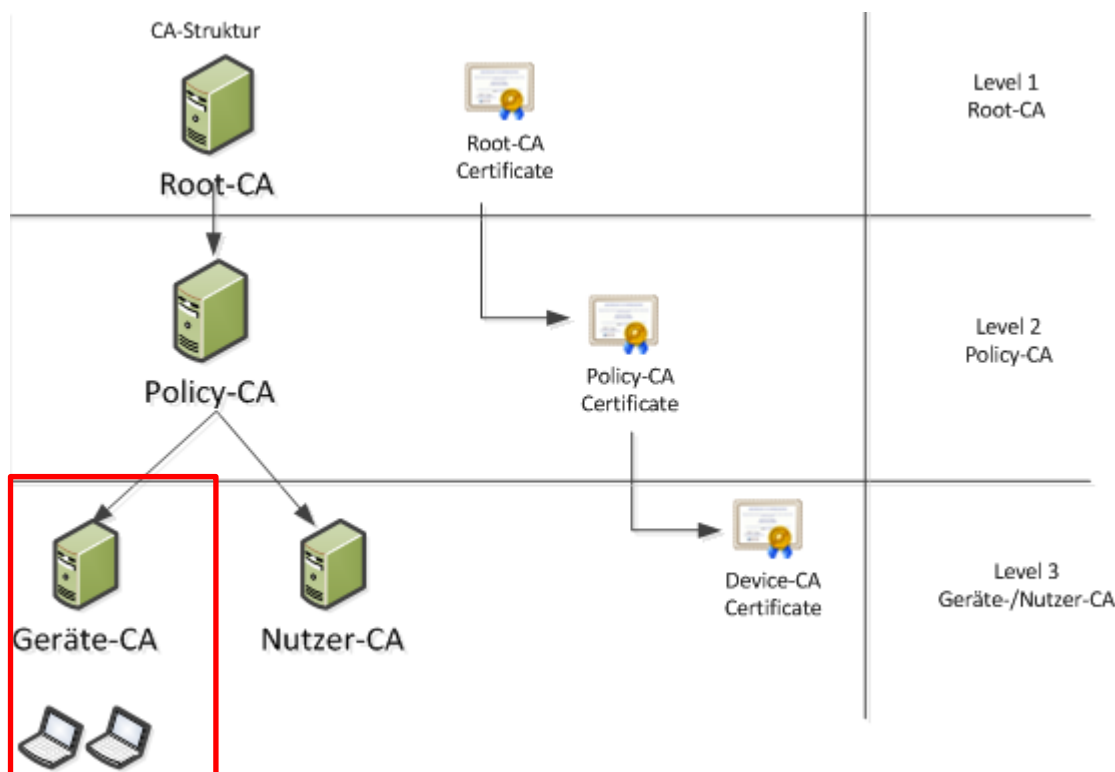


Abbildung 1 Geräte-CA

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 Kapitel 5 und 6 beschrieben und repräsentieren das sog. „Certificate Practice Statement“ (CPS) für die Geräte-CA der IAV-PKI. Für die beiden CAs auf den höheren Stufen (Root- und Policy-CA) gibt es eine eigene zusammengefasste Zertifikatsrichtlinie [IAV_CP_ROOT_POLICY].

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

Die Geräte-CA wird mit der Ausstellung eines signierten CA-Zertifikats von der Policy-CA zertifiziert. Die Vertrauenskette endet bei der Root-CA als oberste Stufe in der Zertifikatshierarchie. Die Root-CA verfügt über ein selbstsigniertes Root-CA-Zertifikat. Die Aufgaben der Geräte-CA liegen in der Ausstellung von Endzertifikaten ausschließlich für IT-Komponenten, -Anwendungen und Endgeräte wie z.B. SSL-Zertifikate für die Absicherung von Kommunikationsverbindungen (durch manuelle Erzeugung), Geräte-Zertifikate für eine 802.1x Authentifizierung im LAN (durch automatische Erzeugung mittels eines Auto-Enrollment-Prozesses) etc. Zertifikate für Personen werden

ausschließlich von einer Nutzer-CA erstellt, die aber ebenfalls nicht im Geltungsbereich dieser Zertifikatsrichtlinie liegt.

1.1.1 Ziel dieser Richtlinie

Diese Richtlinie legt die technischen und organisatorischen Rahmenbedingungen der Geräte-CA (Level 3) der IAV-PKI fest.

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 Geräte-CA
- **soll, (sollte)**
Vorgabe der IAV Geräte-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 Geräte-CA ausgestellten Geräte-Zertifikate.

1.2 Name und Kennzeichnung des Dokuments

Name: Zertifikatsrichtlinie Geräte-CA IAV GmbH
Version: 1.3
Datum: 12.08.2020
OID Geräte-CA: 1.3.6.1.4.1.44741.1.3

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 (vgl. Abbildung in Kapitel 1.1) 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 Geräte-Zertifikate mittels der hier im Fokus stehenden 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 der Geräte-CA eine dedizierte Registrierungsstelle zugeordnet.

Die Erstellung und Erneuerung von Zertifikaten durch die Geräte-CA liegt in der Verantwortung des Bereichs C-I, Abteilung C-IT 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 zugehörigen 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 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	Marc Plagge
Team Manager IAM, IT-Security & Governance	IAM, IT-Security & Governance
Carnotstraße 1	Rockwellstraße 16
10587 Berlin, Germany	38518 Gifhorn, Germany
karsten.keusch[at]iav.de	marc.plagge[at]iav.de
www.iav.de	www.iav.de

Tabelle 1 Ansprechpartner und Kontakt

1.5.3 Prüfung der Zertifizierungsrichtlinie

Diese Richtlinie wird durch den Service Manager der IAV-PKI regelmäßig jedes Jahr oder anlassbezogen überprüft. Der Service Manager der IAV-PKI stellt die Übereinstimmung der CPS mit den Vorgaben der jeweiligen CP sicher.

1.6 Definitionen und Abkürzungen

Siehe Verzeichnisse - 10.3 Abkürzungsverzeichnis.

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

2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

IAV stellt die von Geräte-CA ausgestellten CRLs in einem intern verfügbaren Verzeichnisdienst zur Verfügung. Dieser Verzeichnisdienst ist unter folgenden Adressen erreichbar:

- Für CRLs:
 - o <http://crl.iavtech.net/pki/> (extern)
 - o <http://crl.iav.enxo.org/pki/> (extern / intern)

Außerdem besteht die Möglichkeit, den Status von User-Zertifikaten über einen OCSP-Dienst abzufragen, der unter folgenden Adressen erreichbar ist:

- Für OCSP:
 - o <http://crl.iavtech.net/ocsp>
 - o <http://crl.iav.enxo.org/ocsp>

Diese CP steht ebenfalls intern als auch extern auf einem Webserver zur Verfügung:

- Für CP:
 - o <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 User-CA die folgenden Informationen:

- Sperrliste der Geräte-CA
- CP der Geräte-CA

Kontaktinformationen unter denen eine Sperrung beantragt werden kann

IT-ServiceDesk[at]iav.de

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Für die Veröffentlichung von Zertifikaten und Sperrlisten, die durch die Geräte-CA ausgestellt werden, sowie die zugehörige CP und CPS gelten die folgenden Intervalle:

- Das CA-Zertifikat, welches von der Policy-CA für die Geräte-CA (Level 3) ausgestellt bzw. signiert wird, hat einem Gültigkeitszeitraum von 8 Jahren. Eine Erneuerung muss mindestens eine Woche vor Ablauf erfolgen.
- Geräte-Zertifikate, die von der Geräte-CA ausgestellt werden, haben einen maximalen Gültigkeitszeitraum von 3 Jahren und 3 Monaten²
- Geräte-CA-Sperrlisten nach Sperrungen, sonst alle 7 Tage (siehe Kapitel 4.9.7)
- CP nach Erstellung bzw. Aktualisierung.

² Aufgrund fachlicher Anforderungen kann u.U. auch ein kürzerer Gültigkeitszeitraum für Geräte-Zertifikate möglich sein.

2.4 Zugriffskontrollen auf Verzeichnisse

Grundsätzlich muss der lesende Zugriff auf alle in Kapitel 2.2 aufgeführten Informationen ohne Zugriffskontrolle möglich sein. Geräte-Zertifikate und Sperrlisten müssen von allen IAV-PKI Nutzern jederzeit 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

Geräte-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 Geräte-Zertifikats (DN) muss den Zertifikatsnehmer eindeutig identifizieren. Grundsätzlich können Namen sich dabei auf natürliche Personen oder technische Entitäten beziehen.

Geräte-Zertifikate müssen sich deutlich von Zertifikaten für natürliche Personen unterscheiden.

Bei der Vergabe von Zertifikaten für Anwendungen muss für den Namen der voll qualifizierte Domainname verwendet werden, z.B. "CN=www.iav.de".

3.1.3 Anonymität oder Pseudonymität der Zertifikatsinhaber

Die Geräte-CA darf keine anonymen und pseudonymen Zertifikate ausstellen.

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Der DN eines ausgestellten Geräte-Zertifikats hat sich nach den Vorgaben des Standards [X.501] auszurichten.

3.1.5 Eindeutigkeit von Namen

Es muss sichergestellt werden, dass ein in Geräte-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, z.B. *.child.domain.tld). 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 Geräte-CA.

3.2 Identitätsprüfung bei Neuantrag

3.2.1 Methoden zur Überprüfung des Besitzes des privaten Schlüssels

Die Schlüsselpaare der Geräte-CA werden ausschließlich durch die IAV-PKI generiert.

3.2.2 Authentifizierung einer Organisation

Zertifikate für organisationsbezogene Entitäten (z.B. Anwendungen und Geräte) 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 Registrierungsstelle der Geräte-CA (Level 3) gewährleistet eine zuverlässige Identifizierung und Prüfung der Antragsdaten im Rahmen der Integritäts-, Authentizitäts- und Vertraulichkeitsanforderungen gemäß dieser Sicherheitsrichtlinie, 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.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Geräte-Zertifikate, die für die LAN-Authentifizierung eingesetzt werden, dürfen kurz vor Ablauf Ihrer Gültigkeit automatisch neu ausgestellt (per GPO steuerbar) und per Auto-Enrollment-Funktion auf die entsprechenden Endgeräte verteilt werden. Alle anderen Geräte-Zertifikate sind bzgl. einer Erneuerung manuell zu beantragen.

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?

Geräte-Zertifikate, die von der Geräte-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 Geräte-CA.

4.3 Ausstellung von Zertifikaten

4.3.1 Aufgaben der Zertifizierungsstelle

Eine Ausgabe von Geräte-Zertifikaten darf nur für gültige Zertifikatsanträge erfolgen und muss durch den Betreiber der IAV-PKI dokumentiert werden. 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 zu erstellen und das zugehörige Zertifikat zu erzeugen. Bei der Geräte-CA ist es zulässig, Zertifikate für eine ganze Gruppe von Endgeräten zu beantragen (z.B. für alle Workstations einer Fachabteilung).

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

4.4.2 Veröffentlichung des Zertifikats durch die CA

Die Geräte-Zertifikate der Geräte-CA können bei Bedarf für alle Teilnehmer der IAV-PKI in einem Verzeichnisdienst oder auf einem Webserver veröffentlicht werden.

4.4.3 Benachrichtigung weiterer Instanzen

Für Geräte-Zertifikate gelten keine Vorgaben.

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 Geräte-Zertifikate
- Signatur über ausgestellte Sperrlisten.

Es ist unverzüglich die Sperrung des Zertifikats zu veranlassen, wenn die Angaben im Zertifikat nicht mehr korrekt sind oder wenn der private Schlüssel abhanden, gestohlen oder möglicherweise kompromittiert wurde 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 Geräte-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 anwendungsspezifische Vorkehrungen seitens des Zertifikatsnutzers berücksichtigt und als kompatibel erkannt wurden.

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

Eine Geräte-Zertifikatserneuerung auf Basis eines bestehenden Schlüsselpaares ist für die Geräte-CA nicht zugelassen.

Eine Geräte-Zertifikatserneuerung ist bei der Geräte-CA 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 Geräte-Zertifikatserneuerung, bei der ausschließlich das zugehörige Schlüsselpaar ohne sonstige Datenanpassungen neu generiert wird, ist für die Geräte-CA nicht zugelassen.

Eine Geräte-Zertifikatserneuerung ist bei der Geräte-CA 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 Geräte-Zertifikatserneuerung für Zertifikate der Geräte-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 Geräte-Zertifikaten (von der Geräte-CA ursprünglich ausgestellt) mit Schlüsselwechsel und Datenanpassung führen:

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

4.8.2 Wer kann eine Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung beantragen?

Die Zertifikatserneuerung wird vom Zertifikatsnehmer (in diesem Fall der Betreiber der IAV-PKI) beantragt.

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 Geräte-Zertifikat dem Zertifikatsnehmer in geeigneter Weise sicher zu übermitteln. Die Benachrichtigung des Zertifikatsnehmers muss entsprechend dokumentierter Prozesse erfolgen. Bei einem Auto-Enrollment-Prozess muss keine Benachrichtigung erfolgen. Bei einer manuellen Zertifikatsbeantragung ist der Zertifikatsnehmer zu benachrichtigen.

4.8.5 Annahme der Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

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

4.8.6 Veröffentlichung der Zertifikatserneuerung durch die CA

Durch Geräte-CA erneuerte Geräte-Zertifikate können falls erforderlich in einem Verzeichnisdienst oder auf einem Webserver veröffentlicht werden.

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

Eine Benachrichtigung über ein erneuertes Geräte-Zertifikat an weitere Instanzen ist nicht erforderlich.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Gründe für eine Sperrung

Ein durch die Geräte-CA ausgestelltes Geräte-Zertifikat muss gesperrt werden, wenn mindestens eine der folgenden Situationen eintritt:

- Die im Geräte-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 und auch alle Endbenutzerzertifikate, d.h. damit auch Geräte-Zertifikate gesperrt werden.
- Der private Schlüssel der ausstellenden (hier die Geräte-CA) oder einer übergeordneten CA ist kompromittiert worden.
- Die Algorithmen, die Schlüssellänge oder die Gültigkeitsdauer des Geräte-Zertifikates bieten keine ausreichende Sicherheit mehr. Die Betreiber der IAV-PKI behalten sich vor, die betreffenden Geräte-Zertifikate zu sperren.

4.9.2 Wer kann eine Sperrung beantragen?

Die Sperrung der Geräte-CA können durch die jeweiligen Verantwortlichen gesperrt werden. Hierzu zählen folgende Personen:

- Verantwortliche für die Geräte-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 oder mehrerer Geräte-Zertifikates muss schriftlich erfolgen und die Durchführung der Sperrung ist entsprechend zu dokumentieren.

Der Betreiber der IAV-PKI muss die Sperrung des Geräte-Zertifikates an der entsprechenden Geräte-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 Geräte-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 Geräte-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. Die Prüfung der Gültigkeit obliegt im Verantwortungsbereich der Anwendung bzw. des Verfahren. Die Geräte-CA muss Sperrinformationen in Form von Sperrlisten (z.B. per HTTP) veröffentlichen.

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Die Geräte-CA muss spätestens alle 7 Tage jeweils eine neue Sperrliste ausstellen und publizieren. Eine Neuausstellung hat jeweils mindestens einen Tag vor Ablauf der letzten noch gültigen Sperrliste zu erfolgen.

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 Geräte-CA müssen online in Form von herunterladbaren Sperrlisten zur Verfügung stehen.

4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen

Online Statusprüfungen können zusätzlich mittels eines OCSP-Dienstes für die Prüfung der Geräte-Zertifikate der Geräte-CA bereitgestellt werden.

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 Geräte-CA sind neben dem betroffenen CA-Zertifikat auch alle ausgestellten Geräte-Zertifikate unverzüglich zu sperren.

4.9.13 Bedingungen für eine Suspendierung

Eine temporäre Sperrung bzw. eine Suspendierung von CA-Zertifikaten für die Geräte-CA nicht 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

Der Statusabfragedienst muss über das Protokoll OCSP verfügbar sein. Die Erreichbarkeit des Dienstes muss als URL in den Zertifikaten angegeben werden.

4.10.2 Verfügbarkeit des Statusabfragedienstes

Der Statusabfragedienst muss 24 Stunden an 7 Tagen der Woche verfügbar sein. Die technische Verfügbarkeit muss mehr als 99 % betragen.

4.10.3 Optionale Leistungen

Nichtzutreffend.

4.11 Beendigung der Zertifikatsnutzung durch den Zertifikatsnehmer

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

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

4.12.1 Richtlinien und Praktiken zur Schlüssel hinterlegung und -wiederherstellung

Eine Schlüssel hinterlegung und -wiederherstellung der Geräte-CA ist zulässig. Die notwendigen Sicherheitsmaßnahmen, Praktiken und Prozesse sind im zugehörigen CPS im 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 Geräte-CA in diesem Kapitel in ihren Grundzügen beschrieben. Detaillierte Informationen sollten in einem Sicherheitskonzept festgeschrieben werden. 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 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 Best Practices orientieren z.B. basierend auf den Empfehlungen des BSI [IT-GSHB]. Diese Sicherheitsmaßnahmen werden vom Betreiber und Teilnehmern der IAV-PKI ordnungsgemäß erbracht, 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

Das CA-Zertifikat der Geräte-CA und alle von ihr ausgestellten Maschinenzertifikate 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 dem CA-Zertifikat der Geräte-CA muss die Erweiterung „*keyUsage*“ mit den Werten „*keyCert-Sign*“ 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 die Geräte-CA.

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

Keine Vorgaben für die Geräte-CA.

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

Keine Vorgaben für die Geräte-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 die Geräte-CA.

7.3 Profile des Statusabfragedienstes (OCSP)

Der OCSP Responder stellt OCSP-Antworten (Responses) gemäß [RFC2560] / [RFC5019] zur Verfügung. Die Verwendung des NONCE (Number-used Once) ist aus Gründen der Interoperabilität aktiviert.

8 Konformitätsprüfung (engl. "Compliance Audit")

Die Arbeitsprozesse der Geräte-CA sind regelmäßig bzw. anlassbezogen zu überprüfen.

Audits für den technischen Aufbau der IAV-PKI und den damit verbundenen operativen Abläufen 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 sind interne Audits und Prüfungen in regelmäßigen Abständen vorzunehmen.

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. Es sollten auch externe Auditoren hinzugezogen werden insofern erforderlich.

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 Disaster 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.³

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

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

³ 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.

9.4 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 GmbH 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.

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 Zertifikatsnehmers ist in Kapitel 4.5.2 geregelt. Darüber hinaus muss er den Zertifikatsrichtlinien von IAV folgen.

9.6.5 Verpflichtung anderer Teilnehmer

Von IAV GmbH 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 Geräte-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 1.1.3 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 der 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

Abbildung 1 Geräte-CA	7
-----------------------------	---

10.2 Tabellenverzeichnis

Tabelle 1 Ansprechpartner und Kontakt 9

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. Sperrlistenverteilerpunkt
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
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)

Abkürzung	Erklärung
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
Abkürzung	Erklärung

10.4 Glossar

Begriff	Beschreibung

11 Dokumenteninformation

Änderungshistorie

Version	Datum	Autor	Änderungen

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
[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

Nr.	Dokumenten-Titel	Version	Dateiname und Ablage
[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
[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

