Zertifikatsrichtlinie IAV GmbH

Zertifikatsrichtlinie IAV GmbH

User-CA

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

Dateiname: IAV - CP_User_CA V1.0.6.docx

Version: 1.0.6

Status: Freigegeben (extern)

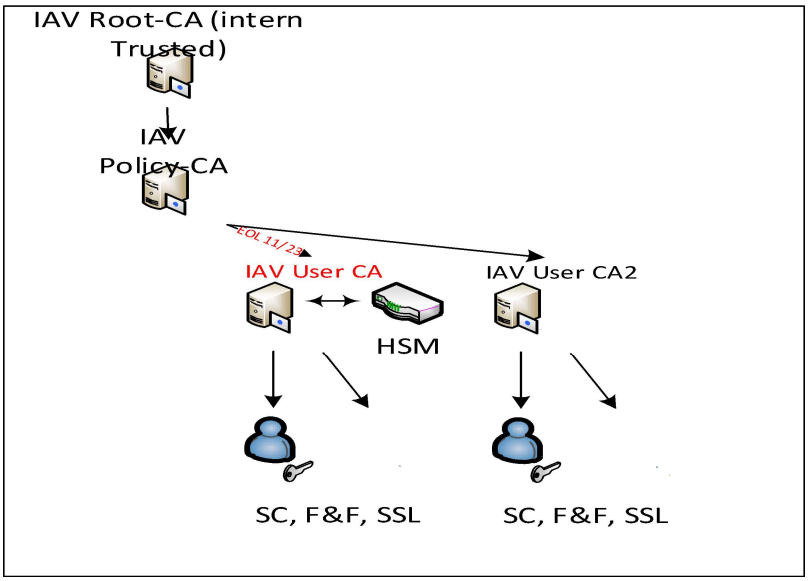
Geheimhaltungsstufe: Öffentlich

	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

1.1 Überblick



[X.509]

Abbildung 1 IAV User 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 User-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“ [RFC3647].

Die User-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 User-CA liegen in der Ausstellung von Endzertifikaten ausschließlich für IAV-Personal.

1.1.1 Ziel dieser Richtlinie

Diese Richtlinie legt die technischen und organisatorischen Rahmenbedingungen der User-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

- **soll, (sollte)**
  Vorgabe, Nichteinhaltung nur in begründeten Ausnahmen
- **kann**
  optional

1.1.3 Gültigkeit

Diese Richtlinie ist ab 01.01.2017 bindend für alle von der IAV User-CA ausgestellten Nutzerzertifikate.

1.2 Name und Kennzeichnung des Dokuments

Name:	Zertifikatsrichtlinie User-CA IAV GmbH
Version:	1.0.6
Datum:	12.08.2020
OID User-CA:	1.3.6.1.4.1.44741.1.4

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 fachliche Nutzer-CA wird verwendet, um Nutzer-Zertifikate auszustellen.

1.3.2 Registrierungsstellen

Den Registrierungsstellen (RA) obliegen die, für den Nutzer stellvertretende Beantragung von Smartcards, Überprüfung der Identität und Authentizität von Zertifikatsnehmern. Bei der IAV-PKI sind der User-CA dedizierte Registrierungsstellen an den Standorten:

- Berlin
- Chemnitz
- Gifhorn
- Stollberg

zugeordnet.

Die Erstellung und Erneuerung von Zertifikaten durch die Nutzer-CA liegt in der Verantwortung des Zertifikatsnehmers und dem Registrierungsstellen-Personal und ist von diesen explizit freizugeben.

1.3.3 Zertifikatsnehmer

Zertifikatsnehmer der User-CA sind natürliche Personen die Zertifikate beantragen und innehaben. Die verantwortlichen natürlichen Personen stehen in einem Vertragsverhältnis mit IAV und sind damit berechtigt Zertifikate zu erhalten.

1.3.4 Zertifikatsnutzer

Zertifikatsnutzer sind alle Personen, Organisationen, Dienste und Anwendungen der 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 aktuell nicht Bestandteil dieser Richtlinie sind.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

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

Auf den von der User-CA ausgegebenen Smartcards sind Zertifikate zur Authentifizierung, Signierung/Verifikation und Ver-/Entschlüsselung enthalten und zur Nutzung in den entsprechenden Anwendungen vorgesehen.

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	Product Owner IAM & IT-Security
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

Table 1 Ansprechpartner und Kontakt

1.5.3 Prüfung der Zertifizierungsrichtlinie

Diese Richtlinie wird durch den Serviceverantwortlichen der IAV-PKI regelmäßig jedes Jahr 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

Siehe Verzeichnisse - 10.3 Abkürzungsverzeichnis.

2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

IAV stellt die von der User-CA ausgestellten User-Zertifikate im intern verfügbaren Active Directory Verzeichnis zur Verfügung.

Sperrinformationen und CA-Zertifikate stehen über ein zentral im Intra-/Internet verfügbares Verzeichnis unter folgenden Adressen zur Verfügung:

- Für CRLs:
  - http://crl.iavtech.net/pki/ (extern)
  - 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:
  - http://crl.iavtech.net/ocsp
  - http://crl.iav.enxo.org/ocsp

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 User-CA die folgenden Informationen:

- Sperrliste der User-CA
- CP der User-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 User-CA ausgestellt werden, sowie die zugehörige CP/CPS gelten folgende Intervalle:

- Das CA-Zertifikat, welches von der Policy-CA für die Nutzer-CA (Level 3) ausgestellt bzw. signiert wird, hat einem Gültigkeitszeitraum von 8 Jahren. Eine Erneuerung und Veröffentlichung erfolgt mindestens 42 Monate vor Ablauf des CA-Zertifikats.
- Nutzer-Zertifikate, die von der User-CA ausgestellt werden, haben einen maximalen Gültigkeitszeitraum von 3 Jahren
- Verschlüsselungszertifikate der Nutzer werden direkt nach Erstellung des Zertifikats im lokalen AD veröffentlicht.
- User-CA-Sperrlisten werden nach Sperrungen, jedoch mindestens täglich mit einer Gültigkeitsdauer von 7 Tagen (siehe Kapitel 4.9.7) veröffentlicht

- Die CP wird nach Erstellung bzw. Aktualisierung veröffentlicht.

2.4 Zugriffskontrollen auf Verzeichnisse

Grundsätzlich ist der lesende Zugriff auf alle in Kapitel 2.2 aufgeführten Informationen ohne Zugriffskontrolle möglich. Nutzer-Zertifikate und Sperrlisten sind von allen IAV-PKI Nutzern jederzeit abrufbar. Ein schreibender Zugriff für Änderungen der Verzeichnisinhalte (Zertifikate und Sperrlisten), Verzeichnisstruktur sowie CA-Konfigurationsänderungen ist ausschließlich auf Verantwortliche und Systeme der IAV-PKI begrenzt. 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

Nutzer-Zertifikate enthalten grundsätzlich Angaben zum Aussteller (*issuer*) und Zertifikatnehmer bzw. Endanwender (*subject*). Diese Namen werden entsprechend dem Standard [X.501] als (*DistinguishedName* = *DN*) vergeben.

Die Namensregeln und -inhalte sind im Zertifikatsprofil der IAV-PKI [IAV_PROFILE] detailliert ausgewiesen.

3.1.2 Aussagekraft von Namen

Der Name eines ausgestellten Nutzer-Zertifikats (*DN*) bezieht sich im Rahmen der Nutzer-CA auf natürliche Personen und identifiziert den Zertifikatsnehmer eindeutig.

Bei der Vergabe von Zertifikaten für Nutzer wird für den Namen der voll qualifizierte Name der Person verwendet, z.B. "*CN=Lars Müller*".

Nutzer-Zertifikate unterscheiden sich deutlich von Zertifikaten für nicht-natürliche Personen durch die Inhalte im CN-Attribut, der E-Mailadresse und dem Universal Principle Name (UPN).

3.1.3 Anonymität oder Pseudonymität der Zertifikatsinhaber

Die User-CA stellt keine anonymen und pseudonymen Zertifikate aus.

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Der DN eines ausgestellten Nutzer-Zertifikats richtet sich nach den Vorgaben des Standards [X.520].

3.1.5 Eindeutigkeit von Namen

Um sicherzustellen, dass ein eindeutiger Bezug zwischen Nutzer und Zertifikat vorhanden ist. enthält der Name (*DN*) des Zertifikatnehmers innerhalb der IAV-PKI und über den Lebenszyklus des Zertifikats hinaus den Namen des Nutzers im CN und die dem Nutzer zugewiesene AD-Nutzerkennung im Attribut *serialNumber* des DN.

Darüber hinaus wird jedem Nutzer-Zertifikat durch die ausstellende User-CA eine eindeutige Seriennummer zugeordnet, die eine eindeutige und unveränderliche Zuordnung zum Zertifikatsnehmer ermöglicht.

3.1.6 Anerkennung, Authentifizierung und Rolle von Markennamen

Keine Vorgaben für User-CA.

3.2 Identitätsprüfung bei Neuantrag

3.2.1 Methoden zur Überprüfung des Besitzes des privaten Schlüssels

Die Schlüsselpaare der Nutzer-Zertifikate werden:

- Oncard (auf der Karte) für Authentifizierung und Signatur
- Offcard (im IT-System vor der Zertifizierung) für Ver-/Entschlüsselung

generiert.

Die Überprüfung des Besitzes des privaten Schlüssels erfolgt bei der Zertifizierung durch Erzeugung eines signierten Zertifikatsrequests, der an die CA übergeben wird.

3.2.2 Authentifizierung einer Organisation

Nichtzutreffend.

3.2.3 Anforderungen zur Identifizierung und Authentifizierung natürlicher Personen

Die Registrierungsstelle der User-CA (Level 3) gewährleistet eine zuverlässige Identifizierung und Prüfung der Antragsdaten im Vorfeld der Beantragung und Ausgabe der Chipkarte. Dazu überprüft die Registrierungsstelle die Identität des Nutzers anhand eines gültigen amtlichen Ausweisdokuments.

3.2.4 Nicht überprüfte Zertifikatsnehmerangaben

Es werden ausschließlich Angaben zur Authentifikation und Identifikation von Zertifikatsnehmern überprüft. Andere Informationen des Zertifikatsnehmers werden nicht berücksichtigt.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Zur Antragsstellung auf Chipkarten der IAV Nutzer-CA ist Personal der IAV berechtigt.

3.2.6 Kriterien für Cross-Zertifizierung und Interoperabilität

Nichtzutreffend.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Nutzer-Zertifikate können über den Self-Service vor Ablauf ihrer Gültigkeit während einer 4-wöchigen Karenzzeit eigenständig durch den Nutzer erneuert werden.

3.3.2 Zertifikatserneuerung nach einer Sperrung

Nach einer Sperrung ist eine Zertifikatserneuerung nicht mehr möglich. Der Nutzer muss einen neuen Kartenantrag stellen.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Der Betreiber der IAV-PKI führt im Rahmen einer Sperrung eine zuverlässige Identifizierung und Authentisierung des Antragstellers mittels IAV-weit geltenden Fragen für das Challenge/Response Verfahren durch.

Falls der Nutzer nicht zweifelsfrei identifiziert werden kann, kann eine Sperrung durch die Legitimierung im Rahmen des IT-Security Policy Detaildokumentes [IAV_BENUTZERIDENTIFIKATION] erfolgen.

4 Ablauforganisation

4.1 Zertifikatsantrag

4.1.1 Wer kann einen Zertifikatsantrag stellen?

Nutzer-Zertifikate, die von der Nutzer-CA ausgestellt werden, können von den in Kapitel 1.3.3 benannten Zertifikatsnehmern beantragt werden. Eine Nachverfolgung der Antragsstellung ist über die entsprechenden Systeme (Benutzerverwaltung, Kartenmanagement und CA) sichergestellt.

4.1.2 Registrierungsprozess und Zuständigkeiten

Die Registrierung erfolgt über die Benutzerverwaltung und stellt einen dokumentierten Prozess dar, 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 und Ausgabe der Chipkarten werden die Zertifikatsnehmer eindeutig und zweifelsfrei in der Registrierungsstelle identifiziert. 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 im Organisationshandbuch [IAV_ORG_PKI] dokumentiert. Eine Annahme von Zertifikatsanträgen erfolgt nur für identifizierte Antragsteller.

4.2.3 Bearbeitungsdauer von Zertifikatsanträgen

Keine Vorgaben für User-CA.

4.3 Ausstellung von Zertifikaten

4.3.1 Aufgaben der Zertifizierungsstelle

Eine Ausgabe von User-Zertifikaten erfolgt nur für gültige Zertifikatsanträge die durch den Betreiber der IAV-PKI dokumentiert werden. Die Aktionen bei der Zertifikatsausgabe erfolgen anhand dokumentierter IAV-Prozesse. Damit wird sichergestellt, dass eine eindeutige Verbindung zwischen Zertifikatsnehmer und zugehörigen Schlüsselpaar besteht. Nach Bearbeitung der Zertifikatsanträge sind die Schlüsselpaare im Bereich der Registrierungsstelle der IAV-PKI zu erstellen, die zugehörigen Zertifikate zu erzeugen und auf die Karte zu übertragen.

4.3.2 Benachrichtigung des Zertifikatsnehmers

Sofern eine Benachrichtigung des Zertifikatsnehmers erforderlich ist, erfolgt diese anhand dokumentierter Prozesse.

4.4 Zertifikatsannahme und Verhalten für eine Zertifikatsannahme

4.4.1 Annahme des Zertifikats

Die Chipkarte mit Zertifikaten wird dem Nutzer durch Registrierungsstellen-Mitarbeiter/-innen übergeben und die Ausgabe quittiert. Der Nutzer wird angewiesen, seinen Zugang zum Self-Service Portal zu benutzen und die im persönlich bekannten Daten für eine spätere Identifikation einzugeben.

4.4.2 Veröffentlichung des Zertifikats durch die CA

Die Verschlüsselungszertifikate des Nutzers werden für alle Teilnehmer der IAV-PKI im internen Verzeichnisdienst veröffentlicht.

4.4.3 Benachrichtigung weiterer Instanzen

Für Nutzer-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 ist durch die Chipkarte und dessen zugehörige PIN ausschließlich dem Zertifikatsnehmer vorbehalten.

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:

- Authentifizierung
- Signatur von Daten/Dokumenten
- Verschlüsselung von Daten/Kommunikation

Zertifikatsnutzer sind unterwiesen unverzüglich eine Sperrung der Zertifikate zu veranlassen, wenn:

- die Angaben im Zertifikat nicht mehr korrekt sind oder
- die Chipkarte abhanden, gestohlen oder möglicherweise 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 Nutzer-CA können von allen Zertifikatsnutzern verwendet werden. Es kann jedoch nur dann darauf vertraut werden, wenn:

- die Zertifikate entsprechend den festgelegten 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/Onlinestatusprüfung 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 Zertifikatserneuerung auf Basis eines bestehenden Schlüsselpaares ist nicht zugelassen.

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

4.7 Zertifikatserneuerung mit Schlüsselerneuerung (engl. Re-Keying)

Eine Zertifikatserneuerung, bei der ausschließlich das zugehörige Schlüsselpaar ohne sonstige Datenanpassungen neu generiert und zertifiziert wird, ist für die Nutzer-CA zugelassen. Die Zertifikatserneuerung erfolgt über einen nutzerbezogenen Self-Service unter Verwendung der gültigen, zu erneuernden Karte.

4.8 Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Im Rahmen der IAV-PKI findet keine -Zertifikatserneuerung für Nutzer-Zertifikate der Nutzer-CA statt.

Sofern eine Datenanpassung die Ausstellung neuer Zertifikate erfordert, muss der Nutzer einen Neuantrag stellen.

4.8.1 Bedingungen für eine Zertifikatsänderung

Die nachfolgenden Gründe führen zu einer Erneuerung von Nutzer-Zertifikaten (mit Schlüsselwechsel und Datenanpassung):

- Routinemäßige Zertifikatserneuerung bei bevorstehendem Ablauf der Gültigkeit des Nutzer-Zertifikates
- Die Algorithmen, die Schlüssellänge oder die Gültigkeitsdauer des Nutzer-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?

Eine Zertifikatserneuerung mit Datenanpassung ist nicht möglich. Sofern dies erforderlich ist, beantragt der Nutzer eine neue Chipkarte.

4.8.3 Ablauf der Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Gemäß 4.8.2 nicht relevant.

4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Gemäß 4.8.2 nicht relevant.

4.8.5 Annahme der Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Gemäß 4.8.2 nicht relevant.

4.8.6 Veröffentlichung der Zertifikatserneuerung durch die CA

Durch die Nutzer-CA erneuerte Verschlüsselungs-Zertifikate werden im internen Verzeichnisdienst veröffentlicht.

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

Eine Benachrichtigung über erneuerte Nutzer-Zertifikate an weitere Instanzen erfolgt nicht.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Gründe für eine Sperrung

Durch die Nutzer-CA ausgestellte Zertifikate werden gesperrt, wenn mindestens eine der folgenden Situationen eintrifft:

- Die im Nutzer-Zertifikat enthaltenen Angaben sind nicht oder nicht mehr gültig und die Karte wird zurückgegeben.

- 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 werden sämtliche von ihr ausgestellten CA-Zertifikate und auch alle Endbenutzerzertifikate, d.h. damit auch Nutzer-Zertifikate gesperrt.
- Der private Schlüssel der ausstellenden oder einer übergeordneten CA ist kompromittiert worden.
- Die Algorithmen, die Schlüssellänge oder die Gültigkeitsdauer der Zertifikate bieten keine ausreichende Sicherheit mehr. Die Betreiber der IAV-PKI behalten sich vor, die betreffenden Zertifikate zu sperren.
- Dauerhafter oder temporärer Verlust bzw. Bekanntwerden der PIN des Trägermediums (Chipkarte)

4.9.2 Wer kann eine Sperrung beantragen?

Die Sperrung von Zertifikaten der Nutzer-CA kann durch die nachfolgenden Verantwortlichen veranlasst werden:

- den Zertifikatsnehmer selbst
- andere Mitarbeiter der IAV
- Vorgesetzte des Zertifikatsnehmers
- Beauftragte für Informationssicherheit der IAV
- Geschäftsleitung der IAV

Die jeweilige ausführende CA dokumentiert die Prüfung und Durchführung der Sperrung.

4.9.3 Ablauf einer Sperrung

Bezüglich der Sperrung sind zwei Fälle zu unterscheiden:

- Temporäre Sperrung
- Dauerhafte Sperrung

Eine temporäre Sperrung (CRL Reason-Code: *certificateHold*) erfolgt zunächst durch die Registrierungsstelle bzw. den Service-Desk sofern der Zertifikatsnehmer seine Karte vergessen hat und er eine temporäre Ersatzkarte beantragt. Die temporäre Sperrung umfasst die auf der vergessenen Karte enthaltenen Zertifikate für Signatur und Authentifizierung. Sofern der Nutzer seine personenbezogene Karte wieder vorweisen kann und die temporäre Ersatzkarte zurückgibt, erfolgt eine Rücknahme der temporären Sperrung.

In allen anderen Fällen erfolgt eine dauerhafte Sperrung, die durch die Registrierungsstelle, den Service-Desk oder die Verantwortlichen der IAV-User-PKI durchgeführt werden.

Die Sperrung der -Zertifikate an der entsprechenden Nutzer-CA wird durchgeführt und die entsprechende Sperrliste unmittelbar veröffentlicht. Der Zertifikatsnehmer ist, außer im Fall zivil- oder strafrechtlicher Untersuchungen, 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

Zertifikatsnehmer sind bei Eintreten eines der in 4.9.1 genannten Sperrgrundes verpflichtet, unverzüglich die Sperrung des entsprechenden Zertifikats zu veranlassen, d.h. Sperranträge werden unmittelbar nach Eintreten der Bedingung für eine Sperrung an die sperrberechtigten Personen/Abteilungen der IAV-PKI übergeben.

4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle

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

4.9.6 Anforderungen zu Sperrprüfungen durch den Zertifikatsnutzer

Die Nutzer-CA veröffentlicht Sperrinformationen in Form von Sperrlisten (z.B. per HTTP) und per Onlinevalidierungsdienst (OCSP). Die Prüfung des Sperrstatus und der Gültigkeit obliegt dem Verantwortungsbereich der Anwendung bzw. des Verfahrens.

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Die Nutzer-CA stellt täglich eine neue Sperrliste aus, die maximal 7 Tage gültig ist.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die Veröffentlichung von Sperrlisten erfolgt unmittelbar nach deren Erzeugung.

4.9.9 Verfügbarkeit von Online-Sperrinformationen

Sperrinformationen der Nutzer-CA stehen online in Form von herunterladbaren Sperrlisten zur Verfügung. Darüber hinaus steht ein Online Validierungsdienst (OCSP) über HTTP zur Verfügung, gegen den die Nutzerzertifikate geprüft werden können.

4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen

Online Statusprüfungen stehen über einen OCSP-Dienst zur Prüfung von Nutzer-Zertifikaten der User-CA bereit.

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 Nutzer-CA werden bis zur Klärung des Sachverhaltes keine weiteren Zertifikate ausgegeben und eine Risikoabschätzung durchgeführt. Auf deren Basis werden entsprechende Maßnahmen ergriffen, die auch eine Sperrung der Nutzer-CA und von ihr ausgestellten Zertifikate beinhalten kann.

Bei einer Kompromittierung des privaten Schlüssels eines Antragsstellers werden die für ihn ausgestellten Zertifikate gesperrt und der Antragssteller stellt einen Kartenneuantrag.

4.9.13 Bedingungen für eine Suspendierung

Eine temporäre Sperrung bzw. eine Suspendierung von Nutzer-Zertifikaten ist für den Fall einer zeitlich begrenzten Ausgabe einer temporären Ersatzkarte erlaubt. Bei Rückgabe der temporären Ersatzkarte können die Zertifikate der nicht-manipulierten Karte wieder aktiviert werden.

4.9.14 Wer kann eine Suspendierung beantragen?

Eine Suspendierung der Zertifikate wird durch den Zertifikatsinhaber bei der Beantragung einer temporären Ersatzkarte in der Ausgabestelle angefordert und von der Ausgabestelle durchgeführt.

4.9.15 Verfahren für Anträge auf Suspendierung

Die Suspendierung erfolgt bei Ausgabe einer temporären Ersatzkarte durch die Registrierungsstelle.

4.9.16 Begrenzungen für die Dauer von Suspendierungen

Die Suspendierung erfolgt für die Dauer der Ausgabe der temporären Ersatzkarte.

4.10 Statusabfragedienst für Zertifikate (OCSP)

4.10.1 Funktionsweise des Statusabfragedienstes

Der Online-Statusabfragedienst (OCSP) ist im Intra-/Internet über das HTTP-Protokoll verfügbar. Die Erreichbarkeit des Dienstes ist als URL im Attribut *AuthorityInformationAccess* (AIA) der Zertifikate angegeben.

4.10.2 Verfügbarkeit des Statusabfragedienstes

Der Statusabfragedienst ist 24 Stunden an 7 Tagen der Woche verfügbar. Die technische Verfügbarkeit beträgt mehr als 99 %.

4.10.3 Optionale Leistungen

Nichtzutreffend.

4.11 Beendigung der Zertifikatsnutzung durch den Zertifikatsnehmer

Bei einer Beendigung der Zertifikatsnutzung durch den Zertifikatsnehmer erfolgt eine Sperrung der dem Nutzer zugehörigen Zertifikate.

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

4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

Es erfolgt eine Schlüsselhinterlegung und -wiederherstellung von Schlüsseln zu Verschlüsselungszertifikaten. Die notwendigen Sicherheitsmaßnahmen, Praktiken und Prozesse sind im zugehörigen CPS im Kapitel 5 und 6 detailliert dokumentiert.

4.12.2 Richtlinien und Praktiken zum Schutz von Sitzungsschlüsseln und deren Wiederherstellung

Sitzungsschlüssel der Nutzer-CA werden mit gängigen kryptographischen Mechanismen abgesichert. Eine Wiederherstellung von Sitzungsschlüsseln ist nicht umgesetzt.

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 Nutzer-CA in diesem Kapitel in ihren Grundzügen beschrieben. Detaillierte Informationen sind im 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 werden vom Betreiber und Teilnehmern der IAV-PKI ordnungsgemäß erbracht, 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 Nutzer-CA in diesem Kapitel in ihren Grundzügen beschrieben. Detaillierte Informationen sind in einem Sicherheitskonzept festgeschrieben. 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 entsprechen gängigen Standards und werden im Dokument „IAV-PKI Zertifikatsprofile“ [IAV_PROFILE] im Detail spezifiziert.

7.1.1 Versionsnummern

Das CA-Zertifikat der Nutzer-CA und alle von ihr ausgestellten Maschinenzertifikate werden konform der internationalen Norm [X.509] in der Version 3 (Typ 0x2) ausgestellt.

7.1.2 Zertifikatserweiterungen

Grundsätzlich sind alle Zertifikatserweiterungen nach den Standards [X.509], [PKIX] und [PKCS] zulässig. Die verwendeten Zertifikatserweiterungen sind im Dokument „IAV-PKI Zertifikatsprofile“ [IAV_PROFILE] für die einzelnen Zertifikatstypen detailliert dargestellt.

7.1.3 Algorithmus Bezeichner OIDs

Die Verwendung von Objekt Identifikatoren für Algorithmen erfolgt gemäß den Vorgaben des Standards [PKIX].

7.1.4 Namensformen

Siehe Kapitel 3.1.

7.1.5 Namensbeschränkungen

Siehe Kapitel 3.1.

7.1.6 OIDs der Zertifikatsrichtlinien

Die OID dieser CP ist, als nicht kritische Erweiterung, in das Attribut „*certificatePolicies*“, mit einem Verweis auf den Ort der Ablage der Policy, eingetragen.

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

Keine Vorgaben für die Nutzer-CA.

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

Keine Vorgaben für die Nutzer-CA.

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

Keine Vorgaben für die Nutzer-CA.

7.2 Sperrlistenprofile (CRL)

7.2.1 Versionsnummer(n)

Es werden Sperrlisten gemäß der internationalen Norm [X.509] in der Version 2 (Typ 0x1) ausgestellt.

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

Die verwendeten Sperrlistenerweiterungen sind im Dokument „IAV-PKI Zertifikatsprofile“ [IAV_PROFILE] für die einzelnen Zertifikatstypen detailliert dargestellt.

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 Nutzer-CA werden regelmäßig bzw. anlassbezogen überprüft.

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

8.1 Frequenz und Umstände der Überprüfung

Grundsätzlich werden interne Audits und Prüfungen in regelmäßigen Abständen vorgenommen.

8.2 Identität und Qualifikation des Überprüfers

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

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 ist nicht erforderlich.

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.[1]

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.

---

[1] 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.

9.4.2 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.

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 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 User-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 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

10.2 Tabellenverzeichnis

10.3 Abkürzungsverzeichnis

Abkürzung	Erklärung
AD	Active Directory
BSI	Bundesamt für Sicherheit in der Informationstechnik

Abkürzung	Erklärung
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
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

Abkürzung	Erklärung
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
0.9	21.10.16	Karsten Meichsner	Vorabversion
1.0	16.01.19	Marc Plagge	Finale Version
1.0.3	03.06.20	Bastian Müller	Aktualisierungen und Anpassung Ansprechpartner / Verantwortliche
1.0.4	03.08.20	Bastian Müller	Vollständige Überarbeitung
1.0.5	29.10.21	Marc Plagge	Neue CAs
1.0.6	17.03.23	Marc Plagge	Update Personendaten

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	

Empfänger	Firma/Abteilung	E-Mail-Adresse	Bemerkung
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
[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",

Quelle	Herausgeber (Erscheinungsdatum): Titel
	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

IAV GmbH
Carnotstraße 1
10587 Berlin
GERMANY

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

www.iav.com