VDEW

Verband der
Elektrizitätswirtschaft e.V.

Energiewirtschaft, Informationsmanagement
Nummer 01/2007

Herausgeber:
Verband der Elektrizitäts-
wirtschaft – VDEW – e.V.
Robert-Koch-Platz 4
10115 Berlin

Ansprechpartner:
Energiewirtschaft,
Informationsmanagement
Beate Becker
Tel. 030 / 72 61 47-209
Fax 030 / 72 61 47-215
beate_becker@vdew.net

Energie-Info

PKI-Zertifikatsrichtlinie (Certificate Policy) des VDEW

Berlin, 10. Januar 2007

Public Key Infrastructur (PKI)-Zertifikatsrichtlinie

10. Januar 2007

Die VDEW-Projektgruppe „Sicherheit beim elektronischen Datenaustausch“ hat die PKI-Zertifikatsrichtlinie (Certificate Policy) des VDEW überarbeitet und ist an den RFC 3647 angepasst worden.

Die PKI-Richtlinie erfüllt zwei Aufgaben

1. Sie dient als dringende Vorgabe/Empfehlung des VDEW bei der Verwendung von Zertifikaten im Rahmen des elektronischen Geschäftsverkehrs
2. Sie ist das Musterdokument für Marktteilnehmer zur externen Veröffentlichung einer Certificate Policy oder eines Certification Practice Statements (CPS) nach VDEW-Empfehlungen.

Das Dokument ist formal nach dem Standard RFC 3647 aufgebaut und stellt dadurch eine größere Transparenz und Vergleichbarkeit her. Durch das Dokument soll eine „sichtbare Vergleichbarkeit“ der Policies und damit der Sicherheitsanforderungen erreicht werden. Außerdem wird durch eine Selbsterklärung der Marktteilnehmer die Einhaltung des Mindestsicherheitsniveaus bestätigt.

PKI-Zertifikatsrichtlinie

(Certificate Policy)

des VDEW

Dringende Empfehlungen/Vorgaben des VDEW bei der Verwendung von Zertifikaten im Rahmen des elektronischen Geschäftsverkehrs

und gleichzeitig

Musterdokument für Marktteilnehmer zur externen Veröffentlichung einer Certificate Policy oder eines Certification Practice Statements (CPS) nach VDEW Empfehlungen

Stand: 10. Januar 2007

Version 1.9

Inhaltsverzeichnis

0 Organisatorische Vorbemerkungen

0.1 Vorbemerkung zum gemeinsamen Verständnis dieses Dokumentes

0.1.1 Zielsetzung des Dokumentes

Für organisationsübergreifenden Electronic Data Interchange (EDI) ist ein Vertragsverhältnis zwischen den Partnern sinnvoll, für den elektronischen Rechnungsaustausch ist dieser Vertrag sogar vorgeschrieben. Er hat in diesem Fall gemäß §14 Absatz 3 Umsatzsteuergesetz sich an der EU-Empfehlung 94/820/EG zu orientieren. Der Vertrag muss dann Passagen enthalten, die „Echtheit der Herkunft“ und „Unversehrtheit des Inhaltes“ vertraglich garantieren.

Ziel auf Verbandsebene ist es, dafür ein konfektioniertes Dokument zu liefern, auf das die Partner in bilateralen Verträgen verweisen können. Das vorliegende Dokument enthält Vorgaben und Aussagen zu Sicherheitsrahmenbedingungen, die die Vertragspartner ihrerseits akzeptieren sollten. Dies sollte der Einfachheit halber in Form eines eigenen, redaktionell angepassten Dokumentes geschehen, das dann als Vertragsanlage dient.

Eine EDI-Beziehung sollte also prinzipiell 3 Dokumente als Vertragsgrundlage haben:

1. Standard-EDI-Vertrag nach 94/820/EG
2. Anlage 1 Interoperabilität
   Hinweis auf die verwendeten EDI-Nachrichtenformate gemäß der VDEW-Marktschnittstellen und ihrer notwendigen technischen Rahmenbedingungen.
3. Anlage 2 Sicherheit
   Jeweilige Certificate Policy oder vergleichbare Dokumente der Vertragspartner mit Verweis auf die VEDIS-Empfehlungen zu Sicherheitsrahmenbedingungen.

Dadurch wird mit minimalem Aufwand eine solide Vertragsgrundlage definiert, die generell wünschenswert und im Fall von elektronischen (Netznutzungs-) Rechnungen gesetzlich vorgeschrieben ist.

0.1.2 Zentrale Abkürzungen

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
PDS	PKI Disclosure Statement
PKI	Public Key Infrastructure

RA	Registration Authority
VDEW	Verband der Elektrizitätswirtschaft
VEDIS	Verbindlichkeit und Sicherheit im Electronic Data Interchange der deutschen Elektrizitätswirtschaft

Weitere Abkürzungen befinden sich im Anhang 1.

0.1.3 Begriffsdefinitionen CP / CPS / PDS

Zertifikatsrichtlinie (CP, Certificate Policy) des Verbandes (VDEW-CP)
Generelle, verbindliche Anforderungen aus Verbandssicht, unabhängig von der konkreten Ausprägung, an den PKI-Betrieb beim teilnehmenden Marktteilnehmer. Das CP ist konform zu den prinzipiellen VEDIS-Empfehlungen in den bereits veröffentlichten technischen und organisatorischen Policy-Dokumenten.

Zertifikatsrichtlinie (CP, Certificate Policy) des Marktteilnehmers (CP des EVU)
Generelle, verbindliche Anforderungen, unabhängig von der konkreten Ausprägung, an den PKI-Betrieb in allen Unternehmensbereichen und Mehrheitsbeteiligungen des Marktteilnehmers. Die konkreten und umfassenderen Aussagen werden in dem CPS beschrieben.

Das CP kann ganz oder in Teilen veröffentlicht werden (siehe auch PDS) und damit das Sicherheitsniveau der PKI charakterisieren. Die Veröffentlichung auf den Webseiten des Marktteilnehmers wird ausdrücklich empfohlen. Das CP des EVU ist konform zu den Anforderungen des VDEW-CP und damit zu den prinzipiellen VEDIS-Empfehlungen in den bereits veröffentlichten technischen und organisatorischen Policy-Dokumenten.

CPS (Certification Practice Statement) des Marktteilnehmers
Beschreibung der Umsetzung des PKI-Betriebs im Rahmen der Freiheitsgrade, die die CP lässt. Das CPS ist in der Regel ein nicht-veröffentlichtes Dokument.

Referenz auf Standards
CP / CPS wurde früher im RFC 2527 spezifiziert. Dieser wurde zum 1.12.2003 durch den RFC 3647 abgelöst.

Das VEDIS-CPS Version 1 ist noch nach altem Standard aufgebaut.

Das vorliegende Dokument ersetzt die Version 1 und wird entsprechend dem internationalen Sprachgebrauch abkürzend CP genannt (VEDIS-CP Version 2).

PDS (PKI Disclosure Statement)
Um ein kleineres Dokument einem Vertrag zugrunde legen zu können, kann auch ein PDS verwendet werden. Das PDS enthält die Anteile eines CP und/oder CPS, die der Marktteilnehmer mit anderen austauschen möchte, um den anderen eine Entscheidung über die Vertrauenswürdigkeit der PKI zu ermöglichen.

Es sind die Minimalaussagen, die eine Einschätzung des Sicherheitsniveaus der betreffenden PKI ermöglichen. Auch sie müssen „Mindestsicherheitsniveau“ und „Vergleichbarkeit“ durch Selbsterklärung bestätigen.

[PDS wurde definiert in ETSI TS 101456 Version 1.1.1, Dezember 2000]

„A PDS is a supplementary document that provides a concise, clear and conspicuous framework to disclose and emphasize critical information about the policies an practices of a CA or a PKI that is normally adressed in much greater detail by an associated CP or CPS“

Das vorliegende Dokument ist dazu geeignet und wird ausdrücklich so positioniert, in bilateralen Verträgen zum Datenaustausch mit Geschäftspartnern als Versicherung zu dienen, wie zertifikatsbasierte Sicherheitsrahmenbedingungen prinzipiell gelebt werden.

§14 Absatz 3 des deutschen Umsatzsteuerrechts verlangt als Vertragsgrundlage zum elektronischen Rechnungsaustausch einen EDI-Vertrag gemäß 94/820/EG. Darin müssen Vorkehrungen deutlich werden, die die „Echtheit der Herkunft“ und „Unversehrtheit des Inhaltes“ der ausgetauschten Rechnungsdaten garantieren. Dies leistet dieses Dokument.

Das vorliegende Dokument ist nach RFC 3647 aufgebaut und enthält alle seine Gliederungspunkte. In der Überschrift ist durch ein (CP) angedeutet, welche Punkte als CP-relevant angesehen werden und somit als zwingende Vorgabe zu betrachten sind. Diese Priorisierung ist konform zur Praxis der European Bridge-CA und der VDEW-Empfehlungen vom 1.9.2003. Weil jedoch der RFC 3647 keine Trennung vorgesehen hat, werden alle Gliederungspunkte nach RFC 3647 hier aufgeführt, auch wenn zu einigen Punkten im vorliegenden Dokument keine Aussagen gemacht werden.

1 Einleitung (CP)

Dies ist die dringende Empfehlung für eine Zertifikatsrichtlinie (im Folgenden oft Certificate Policy oder CP genannt) für Teilnehmer am sicheren elektronischen Datenaustausch in der deutschen Stromwirtschaft. Sie enthält Vorgaben und Anforderungen an eine Teilnehmer-PKI sowie an die zum Einsatz kommenden Zertifikate.

Aufgrund der besonderen Rolle des Datenaustauschs als organisationsübergreifender Vertrauensraum werden im Rahmen des VEDIS-Projektes technische und organisatorische Konformitätsanforderungen formuliert. Dabei wird (analog zum englischen must–shall–may in der Standardisierung RFC 2119) die Begriffe Muss–Soll–Kann verwendet.

Teilnehmer müssen sich an drei grundsätzlichen Wertmaßstäben zur Erreichung und Gewährleistung angemessener Sicherheit orientieren und diese nach dem Selbsterklärungsprinzip den betroffenen Geschäftspartnern bestätigen:

1) technische Konformität
2) vergleichbare Sicherheitsaussagen
3) Einhaltung des Mindestsicherheitsniveaus

Die technische Konformität zur Erreichung von Interoperabilität wird im Dokument „Technische PKI-Interoperabilität“ beschrieben. Seine Aussagen orientieren sich an den Vereinbarungen im Rahmen des deutschen Signaturbündnisses.

Das vorliegende Dokument adressiert den 2. und 3. Wertmaßstab.

Ein Teilnehmer muss zukünftig eine eigene CP (oder dessen Umsetzung als CPS) erstellen, die mit dieser Gliederung nach RFC 3647 konform ist (Vergleichbarkeit).

Ziel ist, das Vertrauensniveau zwischen Teilnehmern am sicheren Datenaustausch durch Transparenz zu steigern.

Weiteres Ziel ist es, Mindestanforderungen („Muss“) an teilnehmende PKI und deren Architektur festzulegen, die Teil der Vertragsdokumente im Rahmen von bilateralen Verträgen (insbesondere EDI-Verträgen) sein sollten (Mindestsicherheitsniveau).

Ausdrückliches Ziel im Bereich der elektronischen Signaturen ist es, ein so angemessenes Sicherheitsniveau zu erreichen, dass fortgeschrittene Signaturen, die in diesem Umfeld erzeugt wurden, als angemessen sicher eingestuft werden können.

Der formale Aufbau nach RFC 3647 soll eine größere Transparenz und Vergleichbarkeit als bei der bisher üblichen Praxis erreichen. Durch das Dokument soll eine

sichtbare Vergleichbarkeit der Policies und

damit der **Sicherheitsanforderungen** erreicht und per **Selbsterklärung durch den Marktteilnehmer** bestätigt werden.

Weitergehende Maßnahmen, wie Auditierung, Zertifizierung etc., sind nicht vorgesehen.

Das vorliegende Dokument bzw. seine mitgliedsspezifische Ausprägung sollte als Referenzdokument für vertragliche Regelungen zwischen Marktteilnehmern dienen können (d. h. als Referenz für bilaterale Verträge geeignet sein).

Im Rahmen dieser CP werden ausschließlich an Organisationen ausgestellte Zertifikate betrachtet, die ihrerseits wieder Personenzertifikate (End Entity) ausstellen. Die Zertifikatsnutzung (KeyUsage) umfasst

- Elektronische Signatur (ContentCommitment, früher NonRepudiation),
- Authentifizierung (DigitalSignature) und
- Verschlüsselung (DataEncipherment, KeyEncipherment).

Andere KeyUsages für End-Entity-Zertifikate werden in dieser CP nicht betrachtet.

Zusätzliche Vorgabe ist, dass diese Zertifikate zur sicheren E-Mail-Kommunikation nach dem S/MIME-Format genutzt werden können.

Hinweis: Nach einer internationalen Normungsübereinkunft wird bei der Interpretation der Key-Usage-Bits der Begriff „NonRepudiation“ durch den Begriff „ContentCommitment“ ersetzt und damit zukünftig Missverständnisse bei der Key-Usage DigitalSignature und NonRepudiation vermieden.

1.1 Überblick (CP)

Im vorliegenden Dokument werden (unabhängig vom Empfehlungscharakter von Verbandsdokumenten) die

- nicht diskutierbaren Anforderungen aus Sicht des Verbandes (Muss, darf nicht)
- die wünschenswerten Empfehlungen (Soll, sollte) und die
- optionalen Hinweise (Kann, Empfehlung)

festgelegt. Es dient zur Schaffung organisationsübergreifender Vertrauensbeziehungen. Hierbei sollen eigene oder am Markt vorhandene Public-Key Infrastrukturen verwendet werden, um Integrität und Authentizität in sicheren organisationsübergreifenden elektronischen Geschäftsprozessen abzubilden.

Beim Marktteilnehmer sollten auf Basis dieses Dokumentes ein externes und ein internes Dokument mit gleichem Aufbau (Kapiteln) entstehen:

1) Im externen Dokument **muss** ein Marktteilnehmer diese allgemeinen Vorgaben bestätigen und diese ohne Preisgabe von technischen oder organisatorischen Details auch veröffentlichen (CP).
2) In einem internen Dokument **sollten** alle Festlegungen revisionssicher dokumentiert werden (CPS). Dieses Dokument wird zu den einzelnen Punkten auch firmenvertrauliche Aussagen enthalten.

Das CP **sollte** in bilateralen Kommunikationsbeziehungen Vertragsbestandteil sein und wird in der gültigen Version vom Marktteilnehmer veröffentlicht.

Das CPS **sollte** Teil der Verfahrensdokumentation im Sinne der Abgabenordnung sein und wird im Allgemeinen nicht veröffentlicht.

Mit der Einrichtung einer PKI nach den VEDIS-Empfehlungen wird für die betroffenen Arbeitsplätze eine Vertrauensinfrastruktur aufgebaut, die technische und organisatorische Anforderungen und Auswirkungen auf die Kommunikationsstrukturen außerhalb des Unternehmens hat.

Die Anforderungen, die das Sicherheitsniveau betreffen, **müssen** von allen Teilnehmern eingehalten werden. Ihre Einhaltung wirkt sich auf die Glaubwürdigkeit und das Vertrauen in die Infrastruktur aus, das Kommunikationspartner dieser Infrastruktur und ihren Prozessen entgegenbringen können.

1.2 Name und Kennzeichnung des Dokuments (CP)

Diese Certifikate Policy trägt den Titel:
„PKI-Zertifikatsrichtlinie des VDEW“.

Version: 1.9

Object Identifier (OID): siehe Anhang 1, wichtige Begriffe

1.3 PKI-Teilnehmer (CP)

Teilnehmer sind Organisationen, die eine eigene Public Key Infrastruktur betreiben oder einen Zertifizierungsdienstleister beauftragt haben.

1.3.1 Zertifizierungsstellen (CP)

Zertifizierungsstellen (CA) sind Stellen, die Zertifikate innerhalb oder im Auftrag der Teilnehmerorganisationen ausstellen, die die Verpflichtungen dieser CP erfüllen.

Diese CP bezieht sich auf die CA, die im Namen des Marktteilnehmers (Issuer) selbst oder in ihrem Namen betrieben werden und auf weitere CA, die konform zu dieser CP sind.

1.3.2 Registrierungsstellen (CP)

In der Registrierungsstelle, welche die Verpflichtungen dieser CP erfüllt, wird innerhalb oder im Auftrag der Teilnehmerorganisationen die zweifelsfreie Identifizierung des Antragstellers (Muss-Bedingung) durchgeführt. RA und CA **müssen** über angemessen sichere Transportwege kommunizieren.

1.3.3 Zertifikatsnehmer (CP)

Zertifikatsnehmer sind natürliche oder juristische Personen oder von diesen verantwortete technische Einheiten (Maschinen oder Programme). Diese haben ein Vertragsverhältnis mit der CA über die Ausstellung von Zertifikaten.

Zertifikatsnehmer von End-Entity-Zertifikaten sind ausschließlich natürliche Personen, die dem Marktteilnehmer oder seinen Mehrheitsbeteiligungen angehören oder für diese tätig sind. Zertifikatsnehmer können auch Partner oder Fremdkräfte sein, welche die Sicherheitsvoraussetzungen erfüllen und in einem Geschäfts- oder Vertragsverhältnis mit dem Marktteilnehmer oder eines Tochterunternehmens stehen.

Zertifikatsnehmer können auch Treuhänder für technische Einheiten (Maschinen oder Programme) sein, in denen so genannte Maschinenzertifikate zum Einsatz kommen.

1.3.4 Zertifikatsnutzer (CP)

Zertifikatsnutzer sind alle Einheiten, die Zertifikate der PKI verwenden. Als Beispiel seien andere Marktteilnehmer genannt, die Zertifikate für die sichere E-Mail-Kommunikation nutzen.

1.3.5 Andere Teilnehmer

Teilnehmer, die keine Verpflichtungen im Rahmen dieser CP eingegangen sind, sind nicht Bestandteil dieser Policy und werden nicht betrachtet.

1.4 Verwendung von Zertifikaten (CP)

Der Marktteilnehmer **muss** innerhalb seiner CP die erlaubte Verwendung von Zertifikaten vorgeben.

Im Rahmen der PKI können personenbezogene und nicht personenbezogene Zertifikate genutzt werden. Maßgeblich für die erlaubte Verwendung von Zertifikaten **müssen** die im Zertifikat enthaltenen Attribute zur KeyUsage sowie die Vorgaben in der zugehörenden CP des Teilnehmers sein.
Nicht-personenbezogene Zertifikate **müssen** als solche maschinell erkennbar sein.

1.4.1 Erlaubte Verwendungen von Zertifikaten (CP)

Zertifikate können von Zertifikatsnehmern für sichere Anwendungen zur Authentisierung, elektronischen Signatur sowie zur Nachrichtenentschlüsselung gebraucht werden.
Zertifikatsnutzer können Zertifikate zur Validierung von Authentisierungen und elektronischen Signaturen sowie zur Nachrichtenverschlüsselung nutzen.

1.4.2 Verbotene Verwendungen von Zertifikaten (CP)

Das Signaturzertifikat darf nicht zum Verschlüsseln verwendet werden und umgekehrt. Zertifikate natürlicher Personen dürfen keine Aussteller-Zertifikate (CA-Zertifikate) sein.

1.4.3 Pflege der Richtlinie (Certificate Policy, CP)

Änderungen an dieser CP **müssen** innerhalb angemessener Zeit aktualisiert und veröffentlicht werden. Der VDEW empfiehlt 2 Wochen.

1.4.4 Zuständigkeit für das Dokument (CP)

Für das vorliegende Dokument ist der

Verband der Elektrizitätswirtschaft e.V.
Robert-Koch-Platz 4
10115 Berlin

zuständig.

Beim Marktteilnehmer ist der Herausgeber (Issuer-Name) im Zertifikat die verantwortliche Organisationseinheit.

1.4.5 Ansprechpartner / Kontaktperson (CP)

Verband der Elektrizitätswirtschaft e.V.
Frau Beate Becker
Robert-Koch-Platz 4
10115 Berlin

Im Marktteilnehmer-CP steht hier der Name der verantwortlichen Person beim Marktteilnehmer.

1.4.6 Zuständiger für die Anerkennung einer CPS in Hinblick auf dieses CP (CP)

CPS-Dokumente **müssen** innerhalb eines Unternehmens auf CP-Vorgabenkonformität durch eine autorisierte Instanz geprüft werden. Eine anerkannte CPS kann als CP-konform gelten.

1.4.7 CPS-Aufnahmeverfahren (CP)

Für die Anerkennung der CPS **muss** ein definiertes Gremium zuständig sein.

Dieses **sollte** nach Verbandsempfehlung mindestens einen Vertreter gemäß 1.3.1 und einen Vertreter des Bereichs, der die CPS verantwortet, enthalten.

Der Marktteilnehmer bestätigt im Rahmen einer Selbsterklärung,

- dass seine CA den Anforderungen dieser VDEW-CP entspricht und
- dass in der angegebenen Teilnehmer-CP die Umsetzung dieser Anforderungen beschrieben ist.

Entspricht die CA den Anforderungen nicht in allen Punkten, so beschreibt der Teilnehmer im Rahmen einer Erklärung zur teilweisen Nicht-Konformität die Stellen, wo keine Entsprechung gegenüber dieser CP vorliegt.

Der Kommunikationspartner entscheidet, basierend auf den Informationen dieser Selbsterklärung, über die Aufnahme der CA (und damit auch der entsprechenden CPS).

Der Teilnehmer stimmt zu, Änderungen, die nicht mit der bestehenden CP/CPS im Einklang stehen, wie auch die Beendigung seiner Zertifizierungsdienstleistungen, vorher den Kommunikationspartnern anzuzeigen.

1.5 Begriffe und Abkürzungen (CP)

Siehe Vorbemerkungen und Anhang 1
„Wichtige Begriffe und Definitionen in einer PKI“

Es wird für Leser, die in der Terminologie einer PKI nicht ausreichend bewandert sind, dringend empfohlen, vor der weiteren Lektüre sich diese Begriffsdefinitionen zu erarbeiten.

1.5.1 Deutsche Begriffe

Keine weiteren Ausführungen

1.5.2 Englische Begriffe

Keine weiteren Ausführungen

1.5.3 Abkürzungen

Keine weiteren Ausführungen

1.5.4 Quellen

- [RFC 3647], S. Chokhani et. Al., “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”,
- Abrufbar unter http://www.faqs.org/rfcs/rfc3647.html .

- [EB-CA S/MIME] European Bridge-CA, “Sichere E-mail: Testspezifikation Interoperabilität und Funktionalität für den Austausch sicherer E-Mails mit Zertifikaten unter der European Bridge-CA“,
- Abrufbar unter http://www.bridge-ca.org/ .
- [ECRYPT] European Network of Excellence in Cryptology (ECRYPT), D.SPA.10 – ECRYPT Yearly Report on Algorithms and Keysizes,
- Abrufbar unter http://www.ecrypt.eu.org .
- [SigAlg], Bundesnetzagentur, “Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG“ vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, jährliche Veröffentlichung im Bundesanzeiger.

2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen (CP)

Der Zertifizierungsdienstleister ist ausführendes Organ für die Bereitstellung von Zertifikaten und Sperrlisten. Bei den sensiblen Verzeichnisinformationen **muss** die notwendige Datenqualität gewährleistet sein. Sensible Daten sind Namen, Zertifikate, E-Mail-Adressen und Sperrlisten.

2.1 Verzeichnisse (CP)

Der Teilnehmer **muss** einen öffentlichen Zugriff auf Sperrdaten zur Verfügung stellen. Dies **muss** über eine im Zertifikat hinterlegte HTTP- oder LDAP-Adresse geschehen. Es **sollten** beide Wege (HTTP und LDAP) zur Verfügung stehen.

Der Teilnehmer gewährleistet eine ordnungsgemäße Erbringung der Verzeichnisdienstleistungen im Rahmen seiner Sicherheits-Policy und orientiert sich am aktuellen Stand der Technik.

Zertifikate **sollte**n in einem extern zugreifbaren Verzeichnis für externe Zertifikatsnutzer bereitgestellt werden. Dort **sollte** der Zugriff vollqualifiziert, z. B. über die E-Mail-Adresse, über LDAP und/oder HTTP erfolgen. Eine Wildcard-Suche führt zu keinem Treffer bzw. ist ausgeschlossen (SPAM-Schutz). Die Veröffentlichung der Zertifikate in weiteren Repositories durch Synchronisationsmechanismen ist möglich.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung (CP)

Der Teilnehmer erklärt sein Einverständnis, die den Betrieb der PKI betreffenden Teile seiner CP den anderen Teilnehmern am Verfahren zugänglich zu machen.

Inhaltlich verantwortlich ist
Bereich, Abteilung, ggf. Name (eindeutige Identifizierung)

Nach Freigabeerteilung wird die CP extern unter
xxx.yyy.zzz/pki/cp (Vorschlag)
veröffentlicht.

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen (CP)

Der Teilnehmer **muss** Zeitpunkt und Häufigkeit der Veröffentlichung von Verzeichnis-Informationen (Sperrinformation, Zertifikatsliste) angeben. Die Veröffentlichung von Sperrinformationen **muss** unverzüglich nach durchgeführter Sperrung des entsprechenden Zertifikates erfolgen.

Die Veröffentlichung von Policies, Änderungen an der teilnehmenden PKI und deren Architektur, **muss** rechtzeitig gegenüber den Teilnehmern am Verfahren erfolgen.

Zertifikate **sollten** nach ihrer Produktion im externen Verzeichnisdienst veröffentlicht werden. Die Gültigkeit einer CRL **sollte** maximal einen Monat betragen und sie **muss** nach einem neuen Eintrag umgehend erneuert werden.

Neue Versionen einer CP werden nach Freigabe innerhalb von 2 Wochen veröffentlicht.

2.4 Zugriffskontrollen auf Verzeichnisse (CP)

Schreibender Zugriff kann nur durch autorisierte Instanzen vorgenommen werden. Extern erfolgt der lesende Zugriff vollqualifiziert, z. B. über die E-Mail-Adresse über LDAP und/oder HTTP. Eine Wildcard-Suche führt zu keinem Treffer bzw. ist ausgeschlossen (siehe auch 2.1).

Der Betreiber der Verzeichnisdienste **muss** eine ordnungsgemäße Zugriffskontrolle auf die entsprechenden Verzeichnisse gewährleisten, die unkontrollierte Änderungen dieser Informationen verhindert.

3 Identifizierung und Authentifizierung (CP)

Es werden CA, RA und natürliche Personen betrachtet.

3.1 Namensregeln

Natürliche Personen können ein Pseudonym haben (z. B. Leiter Rechnungswesen). Die Zuordnung des Pseudonyms zu einer natürlichen Person **muss** dokumentiert werden. Auf bilaterale Nachfrage **muss** die Identität im Einzelfall offen gelegt werden.

3.1.1 Arten von Namen (CP)

Die Namensregeln für den „Subject DistinguishedName“ (Subject DN) und „Issuer DistinguishedName“ (Issuer DN) **müssen** nach dem X.501-Standard definiert sein. In Subject DN und Issuer DN **muss** das Attribut „CommonName“ (CN) enthalten sein.

Es wird **empfohlen,** die E-Mail Adresse gesondert in das Feld „SubjectAltName“ zu schreiben. Die Namensregeln **sollen** gemäß RFC 822 erfolgen. E-Mail-Adressen **können** Teil des DN sein.

3.1.2 Notwendigkeit für aussagefähige Namen (CP)

Zertifikate können sich auf natürliche oder juristische Personen oder technische Geräte beziehen.

Sie **müssen** jeweils als solche eindeutig kenntlich sein.

Der Charakter anderer Zertifikate (Server-, Rollen-, Organisations-Zertifikate) **muss** eindeutig für die Empfänger erkennbar sein.

Die in Zertifikaten benutzten Namen, d. h. die im Feld "Zertifikatsnehmer" (subject) angegebenen technischen Namen, sollen aussagefähig sein.

3.1.3 Anonymität oder Pseudonyme von Zertifikatsnehmern (CP)

Ein als Pseudonym oder anonym ausgestelltes Zertifikat **muss** als solches ebenfalls kenntlich sein. Bevorzugter Grund für Pseudonyme ist die Zweckgebundenheit der Zertifikate, nicht die Anonymisierung der Person aus anderen Gründen. Dies kann betreffen

- Signatur (z. B. Leiter Rechnungswesen)
- Verschlüsselung (z. B. info@xxx.com)
- Authentisierung (z. B. Corporate Directory-Administrator)

Auch wenn Zertifikate mit Pseudonymen erstellt werden, **muss** durch die RA bzw. CA die reale Identität der Zertifikatsnehmer in den Unterlagen festgehalten werden.

3.1.4 Regeln für die Interpretation verschiedener Namensformen (CP)

Namensgebung nach X.500 / RFC-822

Die Attribute der Namen (DistinguishedName nach [X.501]) sind wie folgt interpretierbar:

G	Vorname(n) der natürlichen Person entsprechend dem zur Identifizierung vorgelegten Dokument
SN	Familienname der natürlichen Person entsprechend dem zur Identifizierung vorgelegten Dokument
CN	Gebräuchlicher Name: Bei natürlichen Personen ohne Pseudonym ist es die Zusammensetzung „Familienname, Rufname“, bei Personen mit Pseudonym ist es die Zusammensetzung „Pseudonym:PN“, bei juristischen Personen ist es die offizielle Bezeichnung der Firma oder Behörde. Bei technischen Komponenten (Server) ist es der Name des Servers, des Dienstes oder der Applikation, welche(r) das Zertifikat benutzt.
PSEUDO	Pseudonym ist bei Personen mit Pseudonym identisch zu CN
SER	Seriennummer, welche die Eindeutigkeit des Namens in der PKI sicherstellt.
O	Name der Firma oder Behörde, welcher dem Zertifikatsnehmer angehört oder sonst verbunden ist bzw. von der die technische Komponente betrieben wird. Die Zugehörigkeit eines Zertifikatsnehmers zu einer Firma oder Behörde **muss** durch einen Firmenausweis oder ein gleichwertiges Dokument bei der Identifizierung belegt werden. Der Organisationsname O **muss** der komplette Firmenname oder Behördenname aus dem Handelsregister o. ä. oder ein geläufiger Kurzname sein. Der Zertifikatsnehmer **muss** glaubhaft machen, dass ein Kurzname auf die Organisation zutrifft.
OU	Organisationseinheit (Abteilung, Bereich oder andere Unterteilung) der Firma oder Behörde. Eine Organisationseinheit OU kann nur festgelegt werden, wenn eine Organisation O festgelegt wurde. Die Zugehörigkeit eines Zertifikatsnehmers zu einer Organisationseinheit **muss** durch die Organisation in einem Firmenausweis oder durch ein gleichwertiges Dokument für die Identifizierung belegt werden.
C	Das aufzuführende Land im ISO 3166 Code ergibt sich wie folgt: Ist eine Organisation O im Namen vorhanden, so liegt im Land C der Sitz der Organisation. Gibt es keine Organisation O im Namen, so hat sich der Zertifikatsnehmer mit einem Dokument aus dem Land C identifiziert.

Für Verschlüsselungs- bzw. Authentifizierungszertifikate **sollte** (im SubjectAltName als RFC822) die E-Mail Adresse des Zertifikatshalters eingetragen sein. Es wird **empfohlen,** im Signaturzertifikat die E-Mail-Adresse des Zertifikatshalters (SubjectAltName) einzutragen. Zertifikate, die für sichere E-Mail eingesetzt werden, **müssen** die E-Mail-Adresse enthalten.

3.1.5 Eindeutigkeit von Namen (CP)

Bei der Vergabe von Namen (Nutzer – oder PKI-Zertifikate) **muss** sichergestellt sein, dass der gewählte Distinguished Name des Zertifikatshalters innerhalb der ausstellenden CA eindeutig ist. Der Name des Ausstellerzertifikates **muss** innerhalb der teilnehmenden PKI eindeutig sein.

3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen

Keine Vorgaben

3.2 Erstmalige Überprüfung der Identität (CP)

Die Prozesskette für die Beantragung und Erstellung eines Zertifikates **muss** technisch wie organisatorisch einen Missbrauch des Antragsweges zur Besitzerlangung eines Zertifikates mit den zugehörigen öffentlichen und privaten Schlüsseln auf Basis von falschen Identitäten oder sonstigen falschen Angaben ausschließen.

(VEDIS-Vorgabe: zweifelsfreie Identifizierung)

Zertifikate für technische Einheiten (z. B. Maschinenzertifikate) **müssen** einer natürlichen Person als Treuhänder zugeordnet werden.

3.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

Die Registrierungsstelle muss Prozesse und Vorgaben entsprechend ihrer Sicherheitsrichtlinie definieren, die eine ordnungsgemäße Prüfung der Zuordnung des privaten Schlüssels zu dem berechtigten Zertifikatsteilnehmer gewährleisten.

3.2.2 Authentifizierung von Organisationszugehörigkeiten

keine Vorgaben

3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikats-Antragstellers (CP)

Persönliche Identifizierung, z. B. unter Vorlage eines amtlichen Lichtbildausweises.
Dies kann auch zu einem früheren Zeitpunkt stattgefunden haben, z. B. bei der Einstellung eines Mitarbeiters.

Die Registrierungsstelle **muss** eine zuverlässige Identifizierung und vollständige Prüfung der Antragsdaten im Rahmen seiner Sicherheitspolicy gewährleisten, die sich an den aktuellen Stand des Grundschutzes orientiert.

3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Die Überprüfung der Angaben zum Zertifikatsnehmer **muss** durch einen Vergleich der Daten des Antragstellers auf dem Antragsformular mit den Daten des Ausweises und den Eintragungen in dem zentralen Verzeichnisdienst oder ähnlich verlässlichen Datenbasen durch die Registrierungsstelle erfolgen. Diese Verifizierung schließt Fehler in der Schreibweise der Namen und Organisationsdaten aus, bzw. es werden widersprüchliche Eingaben erkannt. Die Registrierungsstelle **muss** gewährleisten, dass ungeprüfte Angaben **nicht** die Verbindung der Person zum Schlüsselpaar, Schlüsselaktivierungsdaten, Name und E-Mail-Adresse betreffen.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Die Berechtigung der Mitarbeiter, z. B. am elektronischen Geschäftsverkehr teilnehmen zu dürfen, **muss** überprüft werden. Dies **sollte** im Rahmen einer internen Rollen- und Rechtedefinition erfolgen.

3.2.6 Kriterien für den Einsatz interoperierender Systeme/Einheiten

Bei der Interoperation von wesentlichen Diensten, z. B. Registrierung und Zertifizierung, **müssen** Kriterien zugrunde gelegt werden, die das Ergebnis der zweifelsfreien Identifizierung, z. B. in Form von eindeutigen Registrierungsdaten, nicht beeinträchtigen. Dies gilt für alle Betriebsprozesse, die 3.2 betreffen. Dies gilt insbesondere, wenn die Zertifizierung durch einen externen Dienstleister erfolgt, während andere PKI-Betriebsprozesse ganz oder teilweise im eigenen Hause stattfinden. (Beispiel: inkonsistente Umwandlung von deutschen Umlauten)

3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (rekeying)

Identifikation und Authentisierung anlässlich einer Schlüssel- bzw. Zertifikatserneuerung für CA, RA und End-Entities dürfen die zweifelsfreie Identifizierung nicht beeinträchtigen.

Es können jedoch die Anforderungen an die Zahl der Identitätsbeweise geringer sein als bei der „Erst-Registrierung“, wenn die RA bereits Identitätsbeweise archiviert hat.

Die Aufhebung einer Suspendierung **muss** angemessen sicher erfolgen.

3.3.1 Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Schlüsselerneuerung

Innerhalb der Registrierungsstellen erfolgt die Verwaltung der Nutzer der Public Key Infrastruktur, die unter anderem den Lebenszyklus der Zertifikate überwacht. Eine Rezertifizierung (auf Basis des alten Schlüssels) kann mit gültigem Zertifikat im

Selbstbedienungs (SB)-Verfahren möglich sein; ebenso ein Rekeying (auf Basis eines neuen Schlüssels).

3.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen (CP)

Die Registrierungsstelle gewährleistet eine zuverlässige Identifizierung und Prüfung der Antragsdaten im Rahmen der Integritäts-, Authentizitäts- und Vertraulichkeitsanforderungen.

Ein gesperrtes (revoziertes) Zertifikat **ist nicht** im SB-Verfahren erneuerbar. Der weitere Personalisierungsprozess wird von der Registrierungsstelle wie bei der Erstpersonalisierung umgesetzt.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Registrierungsstelle **muss** im Rahmen ihrer Sicherheitsrichtlinie (CPS) eine zuverlässige Identifizierung und Authentisierung des Antragstellers gewährleisten. Der Prozess **muss** von der Registrierungsstelle dokumentiert werden.

Die Sperrung eines Nutzerzertifikates **sollte** durch eine der folgenden Personen beantragt werden:

- Nutzer
- disziplinarischer Vorgesetzter des Nutzers
- Personalabteilung
- CA-Verantwortlicher
- IT-Sicherheitsbeauftragter

Die Sperrung erfolgt nach geeigneter Identifizierung und Authentisierung des Nutzers.

Eine Sperrung eines Nutzerzertifikates durch andere Personen **sollte** nur schriftlich oder authentisiert unter der Angabe von Sperrgründen in der Registrierungsstelle beantragt werden.

4 Betriebsanforderungen

Die Berechtigung, ein Nutzerzertifikat in der Registrierungsstelle zu beantragen, haben alle natürlichen Personen, die Mitarbeiter des Marktteilnehmers oder Mehrheitsbeteiligungen sind oder in deren Auftrag tätig sind und im Rahmen ihrer Tätigkeitsbeschreibung Nutzer der IT-Infrastruktur sind. Gemäß CP der PKI sind die entsprechenden Rollen:

- User / Benutzer (intern)
- Ggf. Treuhänder (für Externe, für Maschinen/Programme)

4.1 Zertifikatsantrag

Mittelbar für technische Zertifikate Treuhänder oder unmittelbar für Personenzertifikate natürliche und juristische Personen.

Die verantwortliche natürliche oder juristische Person kann Personen-, Organisations- oder Zertifikate für technische Einheiten beantragen. Ein geeignetes Verfahren für den Nachweis der Verantwortung muss in der Sicherheitspolicy beschrieben sein.
Der Zertifikatsantrag soll die zweifelsfreie Identifizierung des Antragstellers unterstützen und **muss** das Ergebnis des Antragsprozesses dokumentieren.

Er **sollte** dazu geeignete Felder enthalten:
Zwingend erforderlich sind dazu Name, Vorname, E-Mail-Adresse, intern eindeutige ID, wie z. B. Personalnummer und Unterschrift/Signatur.

4.1.1 Wer kann einen Zertifikatsantrag stellen

Zertifikate können nur in eigenem Namen beantragt werden.

4.1.2 Registrierungsprozess und Zuständigkeiten (CP)

Generell **muss** es sich um einen im CPS dokumentierten Prozess handeln, so dass nachgewiesen werden kann, dass eine zweifelsfreie Identifizierung nach den in 3.2 beschriebenen Vorgaben stattgefunden hat.

Der Zertifikatsantrag **muss** Angaben enthalten, die dem Anspruch auf zweifelsfreie Identifizierung des Zertifikatsnehmers ermöglichen.

4.2 Verarbeitung des Zertifikatsantrags

Grundsätzlich **muss** die Reihenfolge

- Beantragung
- Registrierung

- Zertifizierung
- Zertifikatsveröffentlichung

eingehalten werden. Ein nicht vollständiger Prozessschritt verhindert die weiteren Schritte. Ein „Nachreichen“ **ist nicht** möglich.

4.2.1 Durchführung der Identifizierung und Authentifizierung

Grundlage für die verbindliche Durchführung der Identifizierung und Authentifizierung des Antragstellers für ein Nutzerzertifikat ist das Vorliegen eines vollständig ausgefüllten Antragsformulars, ggf. einschließlich der Unterschrift/el. Signatur des Treuhänders. Im Anschluss wird bei der Beantragung von Nutzerzertifikaten die Identität des Antragstellers durch Legitimierung, Identifizierung, persönlich Bekanntsein überprüft.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Die Entscheidung über eine Annahme oder Ablehnung des Zertifikatsantrages für ein Nutzerzertifikat wird durch den Mitarbeiter in der Registrierungsstelle getroffen.

Voraussetzungen für die Annahme sind:

- vollständig ausgefülltes Antragsformular
- positive Identitätskontrolle
- positives Ergebnis der Verifikation der Antragsdaten

Ablehnungsgründe bei der Beantragung von Nutzerzertifikaten sind:

- fehlende Angaben
- fehlende Unterschriften
- Unstimmigkeiten bei der Verifikation der Nutzerdaten

Aufnahme oder Ablehnung eines Zertifikatsantrages werden dem jeweiligen Antragsteller gemeldet.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Keine Vorgaben im CP

4.3 Ausgabe von Zertifikat/Schlüsselmaterial

Der Ausgabeprozess für die Nutzerzertifikate wird ausschließlich durch einen autorisierten Mitarbeiter der Registrierungsstelle durchgeführt.

Der Gesamtprozess ist verbindlich zu dokumentieren. Es ist nachzuweisen, dass der Antragsteller im Besitz des privaten Schlüssels ist. Die Ausgabe erfolgt durch persönliches Abholen des personalisierten Schlüsselmaterialträgers durch den Mitarbeiter in der

Registrierungsstelle oder durch einen analogen Prozess, der Missbrauch verhindert. Der Mitarbeiter bestätigt schriftlich den Empfang des Schlüsselmaterialträgers, der Zertifikate und der Schlüssel durch seine Unterschrift auf dem zuvor verwendeten Formular. Ein elektronisches Verfahren ist zulässig.

4.3.1 Aktionen des Zertifizierungsdiensteanbieters bei der Ausgabe von Zertifikaten

Die CA bestätigt eine erfolgreiche Beantragung gegenüber der RA möglichst im PKCS#10-Format.

Eine Ausgabe von Zertifikaten darf nur für angenommene Zertifikatsanträge erfolgen. Die Aktionen bei der Ausgabe **müssen** anhand dokumentierter Prozesse erfolgen. Dabei **muss** sicher gestellt sein, dass die eindeutige Verbindung von Zertifikatsnehmer und dem im Zertifikat durch den öffentlichen Schlüssel dokumentierten privaten Schlüssel besteht.

4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats

Eine Benachrichtigung des Zertifikatsnehmers über die Bereitstellung wird schriftlich durchgeführt. Das Medium E-Mail ist zulässig.

4.4 Zertifikatsannahme

Die Annahme des Nutzerzertifikates erfolgt persönlich durch den Nutzer in der Registrierungsstelle oder durch einen ähnlich sicheren Übergabeprozess.

4.4.1 Verhalten für eine Zertifikatsannahme

Die Ausgabestelle **muss** anhand dokumentierter Prozesse die sichere Übergabe und Bedingungen beschreiben, die zu einer Annahme des Zertifikates führen.

4.4.2 Veröffentlichung des Zertifikats durch die CA Gesicherte Verteilung durch das Trust Center

Die Veröffentlichung der Zertifikate erfolgt entsprechend dem Verzeichnisdienstkonzept mit deren Generierung in regelmäßigen Abständen nach einer Plausibilitätsprüfung. Die Zeitabstände werden festgelegt.

Sollen die Zertifikate nicht generell veröffentlicht werden, so **muss** mindestens eine Validierung anhand der Sperrliste/CRL möglich sein. Die CA-Zertifikate **müssen** veröffentlicht sein.

4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats

Eine persönliche Benachrichtigung ist nicht vorgesehen.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

Generell gilt hierzu sinngemäß das VEDIS-Dokument „Umgang mit Schlüsselmaterial“

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Das vom Marktteilnehmer für die einzelnen Einsatzfälle vorgesehene Speichermedium **muss** als Träger für Nutzerzertifikate und Schlüssel eingesetzt werden. Dies können z. B. Disketten/Softtoken/USB-Token, SmartCards oder Hardwaresicherheitsmodule sein.

Der private Schlüssel des PKI-Teilnehmers **darf nur** für Anwendungen benutzt werden, die in Übereinstimmung mit den im Endnutzerzertifikat angegebenen Nutzungsarten stehen. Die folgenden Nutzungsarten sind vorgesehen:

- Authentifizierung von Benutzer- oder Anwendungsdaten und technischen Systemen (Nutzungsart digital signature)
- Entschlüsselung von Benutzer- oder Anwendungsdaten oder von symmetrischen Schlüsseln, welche in dem sogenannten Hybridverfahren für die Verschlüsselung solcher Daten dienen (Nutzungsarten dataEncryption bzw. KeyEncryption)
- Kennzeichnung der Verbindlichkeit (Nutzungsart non-repudiation) einer elektronischen Signatur durch den Zertifikatsnehmer.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Der öffentliche Schlüssel des PKI-Nutzers **muss** für alle Anwendungen benutzt werden, die in Übereinstimmung mit den im Endnutzerzertifikat angegebenen Nutzungsarten stehen. Die folgenden grundlegenden Nutzungsarten sind vorgesehen:

- Überprüfung der Authentifizierung von Benutzer- oder Anwendungsdaten (Nutzungsart digital signature)
- Verschlüsselung von Benutzer- oder Anwendungsdaten oder von symmetrischen Schlüsseln, welche in dem sogenannten Hybridverfahren für die Verschlüsselung solcher Daten dienen (Nutzungsarten dataEncryption bzw. KeyEncryption)
- Überprüfung der Verbindlichkeit (Nutzungsart non-repudiation) einer elektronischen Signatur durch den Zertifikatsnehmer.

Hinweis: Nach einer internationalen Normungsübereinkunft wird bei der Interpretation der Key-Usage-Bits der Begriff „NonRepudiation“ durch den Begriff „ContentCommitment“ ersetzt und damit zukünftig Missverständnisse bei der Key-Usage DigitalSignature und NonRepudiation vermieden.

4.6 Zertifikatserneuerung

4.6.1 Bedingungen für eine Zertifikatserneuerung

Eine Zertifikatserneuerung unter Beibehaltung des asymmetrischen Schlüsselpaares **darf nur** dann erfolgen, wenn die bisher eindeutige Verbindung von Zertifikatsnehmer und privaten Schlüssel sichergestellt bleibt.

Die Registrierungsstelle **muss** im Rahmen seiner Sicherheitsrichtlinie die Bedingungen für eine Zertifikatserneuerung dokumentieren.

4.6.2 Wer darf eine Zertifikatserneuerung beantragen

Eine Zertifikatserneuerung kann durch den Zertifikatsinhaber bei Nutzerzertifikaten beantragt werden.

4.6.3 Bearbeitungsprozess eines Antrages auf Zertifikatserneuerung

Die Bearbeitung eines Antrages auf Zertifikatserneuerung **muss** ein vollständig dokumentierter Prozess sein, der die Anforderungen der Identifizierung nach 2.3.2 erfüllt.

Grundsätzlich ist wie in 4.2.2 die Reihenfolge

- Beantragung
- Registrierung
- Zertifizierung
- Zertifikatsveröffentlichung

einzuhalten. Ein nicht vollständiger Prozessschritt verhindert die weiteren Schritte. Ein „Nachreichen“ ist nicht möglich.

Im Gegensatz zu 4.2.2 sind mittels eines gültigen Zertifikats und abgesicherten Anwendungen Self Service Prozesse möglich, da die zweifelsfreie Identifizierung elektronisch vorgenommen werden kann.

4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Die Benachrichtigung des Zertifikatsnehmers folgt entsprechend dokumentierter Prozesse.
Wie in 4.3.2

4.6.5 Verhalten für die Annahme einer Zertifikatserneuerung

Die Ausgabestelle beschreibt den Prozess für die sichere Zertifikatsübergabe und Bedingungen, die zu einer Annahme des Zertifikates durch den Teilnehmer führen.

4.6.6 Veröffentlichung der Zertifikatserneuerung durch die CA

Ein erneuertes CA-Zertifikat **muss** gegenüber den Kommunikationspartnern unverzüglich veröffentlicht werden.

Endnutzerzertifikate **sollten** gegenüber den Kommunikationspartnern in einem Verzeichnisdienst unverzüglich veröffentlicht werden.

4.6.7 Benachrichtigung anderer PKI-Teilnehmer über die Erneuerung des Zertifikates

Keine weiteren Ausführungen

4.7 Zertifizierung nach Schlüsselerneuerung

4.7.1 Bedingungen der Zertifizierung nach Schlüsselerneuerungen

Die Zertifizierungsstelle **muss** Bedingungen beschreiben, unter welchen Umständen ein neu erzeugtes Schlüsselpaar zusammen mit den bisherigen Zertifikatsdaten zertifiziert wird.
Mögliche Voraussetzungen sind:

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

4.7.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen

Analog 4.6.2

4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Für den Zertifikatsinhaber analog 4.6.3

Zusätzlich **müssen** zwischen RA und CA die Prozessschritte analog Erstantrag eingehalten werden, da wieder Schlüsselgenerierung, Aufspielen auf Personal Security Environments (PSE), Transportsicherung erforderlich sind.

4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Zertifikatsnutzer, deren Erneuerungsprozess durch das Erreichen der Grenze der Lebensdauer ansteht (z. B. 80%), werden schriftlich über die von den Registrierungsstellen geplante Erneuerung informiert. Das Medium E-Mail ist zulässig.

4.7.5 Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen

Die Ausgabestelle beschreibt den Prozess für die sichere Zertifikatsübergabe und Bedingungen, die zu einer Annahme des Zertifikates durch den Teilnehmer führen.

Aufgrund der Neugenerierung der Schlüsselpaare muss im Prinzip auf Seiten der Services (RA, CA, Chipkartenmanagement, etc.) der technische Prozess, wie in Kapitel 4.4.1. beschrieben, durchlaufen werden. Allerdings können auf Seiten der Endbenutzer Registrierung und Belehrungsmaßnahmen entfallen.

4.7.6 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA

Ein erneuertes CA-Zertifikat **muss** unverzüglich veröffentlicht werden.

Endnutzerzertifikate **sollten** in einem Verzeichnisdienst veröffentlicht werden.

4.7.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Keine weiteren Ausführungen

4.8 Zertifikatsänderung

4.8.1 Bedingungen für eine Zertifikatsänderung

Keine Bedingungen; technisch bedeutet dies ein neues Zertifikat

4.8.2 Wer darf eine Zertifikatsänderung beantragen

Wird vom jeweiligen Unternehmen ausgestaltet

4.8.3 Bearbeitung eines Antrages auf Zertifikatsänderung

Wird vom jeweiligen Unternehmen ausgestaltet

4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikates

Wird vom jeweiligen Unternehmen ausgestaltet

4.8.5 Verhalten für die Annahme einer Zertifikatsänderung

Unter den übergeordneten Aspekten analoge Prozesse wie in 4.4

4.8.6 Veröffentlichung der Zertifikatsänderung durch den CA

Ein geändertes CA-Zertifikat **muss** gegenüber den Mitgliedern am Verfahren unverzüglich veröffentlicht werden. Endnutzerzertifikate **sollten** veröffentlicht werden.

Unter den übergeordneten Aspekten analoge Prozesse wie in 4.4

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

Die Änderung eines CA-Zertifikates **muss** gegenüber den Mitgliedern am Verfahren unverzüglich angezeigt werden.

Unter den übergeordneten Aspekten analoge Prozesse wie in 4.4

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Bedingungen für eine Sperrung

Die Zertifizierungsstelle **muss** Bedingungen beschreiben, unter welchen Umständen eine Zertifikatssperrung durchgeführt wird. Eine Sperrung **muss** erfolgen, wenn:

- eine Kompromittierung des Schlüssels vorliegt,
- die eindeutige Zuordnung des Zertifikats zu seinem Zertifikat nicht mehr gegeben ist,

- die eindeutige Verbindung zwischen Zertifikat und Schlüssel nicht mehr gegeben ist.

Folgende Gründe führen z. B. zu einer Sperrung des Nutzerzertifikates:

- Beendigung eines Beschäftigungsverhältnisses
- Freistellungen / Beurlaubungen (z. B. Wehrdienst)
- Namensänderung, z. B. durch Heirat oder Umorganisation (DN-Änderung)
- Zweckentfremdung des privaten Schlüssels
- genereller Verdacht auf Kompromittierung oder Zweckentfremdung
- Festgestellte Kompromittierung oder Zweckentfremdung
- es wird ein Träger mit Schlüsselmaterial (Token) gefunden
- Sperrung eines übergeordneten Zertifikates
- Beschädigung / Verlust des Trägers mit Schlüsselmaterial

4.9.2 Wer kann eine Sperrung beantragen

Eine Sperrung eines Nutzerzertifikates kann z. B. durch folgende Personen veranlasst werden:

- den Mitarbeiter selbst
- den disziplinarischen Vorgesetzten des Mitarbeiters
- einen leitenden Mitarbeiter der Personalabteilung (Nutzerzertifikate)
- einen Mitarbeiter der zentralen Sicherheitsdienste
- einen Mitarbeiter der Registrierungsstelle
- einen Mitarbeiter der Zertifizierungsstelle

4.9.3 Verfahren für einen Sperrantrag

Sowohl die Registrierungsstelle, als auch die Zertifizierungsstelle **müssen** das Verfahren für die Sperrung eines Zertifikates dokumentieren.

4.9.4 Fristen für einen Sperrantrag

Die Zertifizierungsstelle **muss** Fristen für einen Sperrantrag gegenüber dem Zertifikatsnehmer dokumentieren.

4.9.5 Zeitspanne für die Bearbeitung des Sperrantrags durch die CA

Die Zeitdauer zwischen Erhalt eines Sperrantrags bei der zuständigen Registrierungsstelle und dem Wirksamwerden der Sperrung mit der Veröffentlichung der CRL mit dem gesperrten Zertifikat hat schnellstmöglich zu erfolgen (Latenzzeit im Service Level Agreement (SLA) definieren).

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Die verfügbaren Methoden zum Prüfen von Sperrinformationen **müssen** den Konformitätskriterien von VEDIS entsprechen.

Es erfolgt durch den autorisierten Mitarbeiter eine Prüfung auf das Vorliegen von Sperrgründen (siehe Aufzählung 4.9.1)

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten (CP)

Die Frequenz der Veröffentlichung von Sperrlisten **muss** von der Zertifizierungsstelle dokumentiert werden. Dabei **soll** eine zeitnahe Verfügbarkeit von aktuellen Sperrinformationen gewährleistet sein.

Die Zeitspanne zur Bereitstellung einer neuen CRL erfolgt schnellstmöglich.

4.9.8 Maximale Latenzzeit für Sperrlisten (CP)

Die maximale Latenzzeit für Sperrlisten **muss** von der Zertifizierungsstelle dokumentiert sein. Empfohlen wird 24 Stunden.

4.9.9 Online-Verfügbarkeit von Sperrinformationen (CP)

Die Zertifizierungsstelle **muss** Sperrinformationen online zur Verfügung stellen. Diese können per OCSP zur Verfügung stehen. Dies **muss** über eine im Zertifikat hinterlegte HTTP- oder LDAP-Adresse geschehen. Es **sollten** beide Wege (HTTP und LDAP) zur Verfügung stehen. Die Verfügbarkeit dieser Online-Dienstleistung **muss** dokumentiert werden.

4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen (CP)

Der Teilnehmer **muss** Informationen für den Zugriff auf seine Sperrinformationen angeben. Diese **müssen** die Internet-Adresse und Protokollinformationen für den Zugriff enthalten. Weiterhin **sollen** Informationen über die Verfügbarkeit sowie anzuwendende Richtlinien im Falle der Nicht-Verfügbarkeit angegeben werden.

Online-Prüfung von Sperrinformationen ist auch für externe Zertifikatsnutzer unter der URL http://xxx.yyy.zzz/pki/crl bzw. ldap://xxx.yyy.zzz möglich. Eine Online-Prüfung über einen eigenen OCSP-Responder ist noch nicht vorgesehen.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen (CP)

Sperrinformationen können auch durch eine Positiv-Auskunft gegeben werden. Dabei sind alle derzeit in Verzeichnisdiensten bereitgestellten Zertifikate gültig. Gesperrte Zertifikate werden aus den Verzeichnisdiensten zeitnah entfernt.

Es **sollten** allerdings zunächst keine Delta-CRL verwendet werden, da sie noch nicht allgemein unterstützt werden.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Die Veröffentlichung von Sperrinformationen nach einer Sperrung bei einer Kompromittierung des privaten Schlüssels **muss** unter Berücksichtigung der o. g. Fristen durchgeführt werden.

4.9.13 Bedingungen für eine Suspendierung

Eine Suspendierung ist nur bei nachgewiesenen unkritischen Vorgängen, also keinem Verdacht auf Korrumpierung des Schlüsselmaterials oder Missbrauch des Tokens, vorgesehen. Ansonsten **muss** eine Revozierung vollzogen werden.

4.9.14 Wer kann eine Suspendierung beantragen

Wie 4.9.2

4.9.15 Verfahren für Anträge auf Suspendierung

Wie 4.9.3.

4.9.16 Begrenzungen für die Dauer von Suspendierungen

Innerhalb eines angemessenen Zeitraums kann die Suspendierung auf Antrag aufgehoben werden. Anschließend **muss** eine Revozierung erfolgen.

4.10 Statusabfragedienst für Zertifikate (CP)

Manuelle Statusabfragen benutzen LDAP oder HTTP.
Ein automatisierter Dienst benutzt LDAP oder später OCSP.

4.10.1 Funktionsweise des Statusabfragedienstes

Ein Online-Statusabfragedienst ist in der ersten Ausbaustufe nicht vorgesehen.

4.10.2 Verfügbarkeit des Statusabfragedienstes (CP)

Die Verfügbarkeit des Statusabfragedienstes **muss** dokumentiert werden. Dabei soll eine zeitnahe Verfügbarkeit von aktuellen Statusinformationen gewährleistet sein.

4.10.3 Optionale Leistungen

Zunächst keine Aussagen

4.11 Kündigung durch den Zertifikatsnehmer

Organisatorische Veränderungen, die eine Nutzung von Zertifikaten nicht mehr sinnvoll möglich machen, sind im Gliederungspunkt 4.9.1 beschrieben und **müssen** zur Sperrung der Zertifikate führen.

4.12 Schlüsselhinterlegung und –wiederherstellung

Ein Key Escrow (notarielle Hinterlegung) ist in Deutschland nicht vorgesehen. Key Recovery (Hinterlegung im eigenen Haus) **darf nicht** für Signaturschlüssel und Authentisierungsschlüssel praktiziert werden. Ein Key Recovery für Verschlüsselungsschlüssel ist zulässig.

Im Fall einer Schlüsselhinterlegung **muss** der Zertifizierungsdiensteanbieter die Prozesse der Schlüsselhinterlegung dokumentieren. Diese **müssen** der eigenen Sicherheits-Policy und dem aktuellen Stand der Technik entsprechen.

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel

Keine Aussagen im CP

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Keine Aussagen im CP

5 Nicht-technische Sicherheitsmaßnahmen (CP)

Es erfolgt Orientierung am aktuellen Stand der Technik (z. B. IT-Grundschutzhandbuch oder ISO 17799:2005). Eine Orientierungshilfe zu einzelnen Punkten in diesem Abschnitt bieten die Empfehlungen im VDEW „Konzept für IT-Sicherheit“ (VDEW Material M-14 2004).

Im CP des Teilnehmers müssen zumindest die Anforderungen zu den folgenden Abschnitten publiziert werden:

- Abschnitt 5.6 Schlüsselwechsel beim Zertifikatsdiensteanbieter (CSP)
- Abschnitt 5.7 Kompromittierung des privaten Schlüssels des Zertifikatsdiensteanbieters (CSP)
- Abschnitt 5.8 Schließung eines Zertifikatsdiensteanbieters (CSP) oder einer Registrierungsstelle

5.1 Bauliche Sicherheitsmaßnahmen

Die zentralen Komponenten der Public Key Infrastructure **müssen** aufgrund ihrer Bedeutung für die Unternehmenskommunikation im besonderen Maße gegen Ausfälle und Angriffe geschützt werden.

5.1.1 Lage und Gebäude

In den internen Dokumenten (CPS) wird sichergestellt, dass die räumliche Lage dokumentiert wird und Veränderungen zeitnah eingepflegt werden.

5.1.2 Zugang

Siehe bauliche Sicherheitsmaßnahmen

5.1.3 Strom, Heizung und Klimaanlage

Durch geeignete Maßnahmen (z. B. USV) ist sichergestellt, dass durch Beeinträchtigungen in diesem Bereich keine Transaktionen, z. B. zwischen RA und CA, verloren gehen können.

5.1.4 Wassergefährdung

Siehe bauliche Sicherheitsmaßnahmen

5.1.5 Brandschutz

Siehe bauliche Sicherheitsmaßnahmen

5.1.6 Lager und Archiv

Die Archivierung der Dokumente und Logginglisten **sollte** gemäß Anforderungen an die Archivierung von Personaldokumenten erfolgen. Ein schreibender Zugriff **muss** nachträglich ausgeschlossen werden. Die Archivierung des Schlüsselmaterials (Verschlüsselungsschlüssel) erfolgt in einer Form, die es nur autorisierten Personen, z. B. nach dem 4-Augen-Prinzip ermöglicht, auf Antrag ein Key Recovery vorzunehmen.

5.1.7 Müllbeseitigung

Die Beseitigung vertraulicher Unterlagen erfolgt unter Aufsicht autorisierter Mitarbeiter.

5.1.8 Disaster Backup

Maßnahmen zur Unterrichtung und Schadensbehebung, falls bei der CA eine Kompromittierung der Sicherheit oder ein Schadensfall eingetreten ist, **müssen** revisionssicher dokumentiert werden.

5.2 Verfahrensvorschriften

Im Betrieb **muss** ein Rollenkonzept realisiert werden. Für das Rollenkonzept **muss** eine detaillierte Dokumentation vorliegen, die bei begründetem Interesse durch eine Schiedsstelle in den relevanten Teilen eingesehen werden kann.

Rollenkonzept

Das Rollenkonzept **muss** zwischen operativen Rollen, administrativen Rollen und Querschnittsrollen unterscheiden. Die im Rollenkonzept definierten Rollenausschlüsse **müssen** sicherstellen, dass einzelne Mitarbeiter unbemerkt keine Veränderungen an den Anlagen des Trustcenters oder anderer sicherheitskritischer Komponenten der PKI vornehmen können und keine Zertifikate, Schlüsselmaterial oder PIN/Sperrkennwort einsehen, erstellen oder manipulieren können.

5.2.1 Rollenkonzept

Keine weiteren Aussagen im CP

5.2.2 Mehraugenprinzip

Sollte gewährleistet sein

5.2.3 Identifikation und Authentifizierung für einzelne Rollen

Keine Aussagen im CP

5.2.4 Rollenausschlüsse

Keine Aussagen im CP

5.3 Personalkontrolle

Sollte gewährleistet sein

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

Sollte gewährleistet sein

5.3.2 Methoden zur Überprüfung der Rahmenbedingungen

Sollte gewährleistet sein

5.3.3 Anforderungen an Schulungen

Keine Vorgaben

5.3.4 Häufigkeit von Schulungen und Belehrungen

Sollte ausreichend gewährleistet sein

5.3.5 Häufigkeit und Folge von Job-Rotation

Unternehmensintern zu regeln

5.3.6 Maßnahmen bei unerlaubten Handlungen

Unzuverlässige Mitarbeiter, gemäß Kriterien der Personalabteilung, **dürfen nicht** mehr in sicherheitskritischen Bereichen eingesetzt werden.

5.3.7 Anforderungen an freie Mitarbeiter

Unzuverlässige freie Mitarbeiter, gemäß Kriterien der Personalabteilung, **dürfen nicht** mehr in sicherheitskritischen Bereichen eingesetzt werden.

5.3.8 Dokumente, die dem Personal zur Verfügung gestellt werden müssen

Keine Aussagen im CP

5.4 Überwachungsmaßnahmen

Keine Aussagen im CP

5.4.1 Arten von aufgezeichneten Ereignissen

Alle Transaktionen zwischen CA, RA und Directory mit Ergebnissen von Plausibilitätskontrollen auf Satzebene **müssen** in Logging-Protokollen aufgezeichnet werden.

5.4.2 Häufigkeit der Bearbeitung der Aufzeichnungen

Der Auditor **sollte** regelmäßig den technisch einwandfreien Betrieb kontrollieren.

5.4.3 Aufbewahrungszeit von Aufzeichnungen

10 Jahre

5.4.4 Sicherung der Aufzeichnungen

Die Sicherung **sollte** mindestens gemäß handelsrechtlicher und steuerrechtlicher Anforderungen erfolgen.

5.4.5 Datensicherung der Aufzeichnungen

Die Sicherung **sollte** mindestens gemäß handelsrechtlicher und steuerrechtlicher Anforderungen erfolgen.

5.4.6 Speicherung der Aufzeichnungen (intern / extern)

Die Sicherung **sollte** mindestens gemäß handelsrechtlicher und steuerrechtlicher Anforderungen erfolgen.

5.4.7 Benachrichtigung der Ereignisauslöser

Alle Prozessbeteiligte **müssen** zu jeder Zeit den einwandfreien Betrieb technisch und organisatorisch überwachen und sicherstellen.

Die Überprüfung des Auditors auf technisch einwandfreien Betrieb löst spätestens bei Unregelmäßigkeiten technische Überprüfungen aus, deren Ergebnis dokumentiert werden **muss**.

5.4.8 Verwundbarkeitsabschätzungen

Die PKI gehört zur unternehmenskritischen Infrastruktur und **muss** entsprechend ganz oder in Teilen durch die jeweils Verantwortlichen behandelt werden.

5.5 Archivierung von Aufzeichnungen

Die Sicherung **sollte** mindestens gemäß handelsrechtlicher und steuerrechtlicher Anforderungen erfolgen.

5.5.1 Arten von archivierten Aufzeichnungen

Es **muss** insbesondere eine Archivierung des Beantragungsformulars erfolgen, einschließlich der Ausgabeprotokolle der Zertifikate und Schlüssel über den Gültigkeitszeitraum des Zertifikats plus Verjährungsfrist, mindestens aber gemäß handelsrechtlicher Vorgaben.

5.5.2 Aufbewahrungsfristen für archivierte Daten

Mindestens 10 Jahre (siehe 5.5.1)

5.5.3 Sicherung des Archivs

Die Sicherung **sollte** mindestens gemäß handelsrechtlicher und steuerrechtlicher Anforderungen erfolgen.

5.5.4 Datensicherung des Archivs

Die Sicherung **sollte** mindestens gemäß handelsrechtlicher und steuerrechtlicher Anforderungen erfolgen.

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

Die Sicherung **sollte** mindestens gemäß handelsrechtlicher und steuerrechtlicher Anforderungen erfolgen.

5.5.6 Archivierung (intern / extern)

Muss gewährleistet sein; Umsetzungsdetails können unternehmensintern geregelt werden.

5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen

Muss gewährleistet sein; Umsetzungsdetails können unternehmensintern geregelt werden.

5.6 Schlüsselwechsel beim CSP (CP)

Der Schlüsselwechsel beim Zertifizierungsdiensteanbieter **muss** anhand dokumentierter Prozesse erfolgen, die sich an der Sicherheits-Policy für Infrastruktur-Schlüssel der entsprechenden Partei orientieren.

5.7 Kompromittierung und Geschäftsweiterführung beim CSP (CP)

Der Zertifizierungsdiensteanbieter **muss** Prozesse im Fall einer Kompromittierung oder eines Desasters dokumentieren, die sich an die Sicherheits-Policy für Infrastruktur-Schlüssel der entsprechenden Partei orientiert.

5.7.1 Behandlung von Vorfällen und Kompromittierungen

Vorfälle sind durch den Zertifizierungsdiensteanbieter zu bewerten und entsprechend der Dokumentation zu behandeln.

5.7.2 Rechnerressourcen-, Software- und/oder Datenkompromittierung

Vorfälle sind durch den Zertifizierungsdiensteanbieter zu bewerten und entsprechend der Dokumentation zu behandeln.

5.7.3 Kompromittierung des privaten Schlüssels des CSP (CP)

Dieser Fall **muss** zur Sperrung aller Zertifikate, die von dieser CA ausgegeben wurden, führen.
Die Sperrung **muss** unverzüglich unternehmensintern und extern veröffentlicht werden.
Es stellt praktisch den größten anzunehmenden Unfall dar.

5.7.4 Möglichkeiten zur Geschäftsweiterführung nach einer Kompromittierung

Offen und abhängig vom Schadensfall

5.8 Schließung eines CSP oder einer Registrierungsstelle (CP)

Die Schließung einer Zertifizierungsstelle (Certificate Service Provider, CSP) bzw. einer Registrierungsstelle **muss** ein dokumentierter Prozess sein. Der Teilnehmer **muss** die Beendigung seiner Zertifizierungsdienstleistungen den anderen Teilnehmern am Verfahren rechtzeitig anzeigen.

Schließung des CSP: Der Auftraggeber **muss** vertraglich sicherstellen, dass in diesem Fall der Betrieb ggf. unter anderer Aufsicht solange weitergeführt werden kann, bis ein geordneter Übergang auf alternative Lösungen ohne weitreichende Beeinträchtigung des Geschäftsbetriebs gewährleistet wird.

Perspektivwechsel Marktteilnehmer CP:

Schließung einer RA in der Betriebsverantwortung eines Unternehmensbereiches / Mehrheitsbeteiligung ist dem Bereich anzuzeigen, der als Issuer für die Zertifikate verantwortlich ist (z. B. CIO–Bereich). Bei Schließung einer Registrierungsstelle werden die Zertifikate von Mitarbeitern dieser Registrierungsstelle gesperrt bzw. die damit verbundenen Rechte eingeschränkt.

6 Technische Sicherheitsmaßnahmen

Hauptziel: Schutz kryptographischer Schlüssel, vor allem im Bereich Trustcenter, und deren Aktivierungsdaten (PIN, Passwörter) bei ihrer Erstellung, Speicherung, Transport und Nutzung; betrifft den Life Cycle von Schlüsseln und Zertifikaten und alle Instanzen (CA und Repositories, RA und End-Entities).

In die Spezifikation sind auch die Sicherheitskontrollen von Entwicklungsumgebungen oder die Entwicklungsmethodik für vertrauenswürdige Software mit einzubeziehen.

Unternehmensintern zu regeln.

Die technischen Sicherheitsmaßnahmen **müssen** im Rahmen der Sicherheits-Policy der Zertifizierungsstelle erfolgen und orientieren sich am aktuellen Stand der Technik.

Im CP des Teilnehmers **müssen** die Anforderungen zu den folgenden Abschnitten angegeben werden:

- Abschnitt 6.1 Erzeugung und Installation von Schlüsselpaaren
- Abschnitt 6.2.4 Sicherung privater Schlüssel
- Abschnitt 6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

Unternehmensintern zu regeln.

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Das PSE wird **persönlich** an den Nutzer ausgegeben. Der Empfang ist zu quittieren.

6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

Die Lieferung öffentlicher Schlüssel erfolgt als Datei.

6.1.4 Lieferung öffentlicher Schlüssel des CSP an Zertifikatsnutzer

Die Lieferung öffentlicher Schlüssel erfolgt als Datei.

6.1.5 Schlüssellängen (CP)

Die Schlüssellängen **müssen** dem aktuellen Stand der Technik und Kryptographie entsprechen.

Hinweis: Für die Wahl der Schlüssellängen in Relation zur Laufzeit wird als Anhaltspunkt auf das Dokument „Geeignete Algorithmen zur Erfüllung der Anforderungen des Signaturgesetzes…“ (http://www.bsi.de/esig/basics/techbas/krypto/index.htm) hingewiesen.

6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle (CP)

Unternehmensintern zu regeln.

Diese Parameter **müssen** VEDIS-Konformitätsvorgaben gemäß dem Dokument „Technische PKI-Interoperabilität“ entsprechen.

6.1.7 Schlüsselverwendungen (CP)

Die Schlüsselverwendung **muss** auf

- Digital Signature

und/oder

- Encryption

gesetzt sein.

Weitere Verwendungen können den einzelnen Teilnehmern überlassen werden.
Der Zertifizierungsdiensteanbieter soll die Schlüsselverwendung angeben.

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

Unternehmensintern zu regeln.

Der Zertifizierungsdiensteanbieter **muss** die ordnungsgemäße Sicherung des privaten Schlüssels gewährleisten und definiert die Anforderungen an kryptographische Module im Rahmen seiner Sicherheits-Policy und orientiert sich an dem aktuellen Stand der Technik.

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

Die verwendeten kryptographischen Module **müssen** anerkannte Standards verwenden.

6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m)

Unternehmensintern zu regeln.

6.2.3 Hinterlegung privater Schlüssel

Unternehmensintern zu regeln.

Die Hinterlegung des privaten Signaturschlüssels eines Teilnehmers der Zertifizierungsstelle **ist nicht** zulässig.

6.2.4 Sicherung privater Schlüssel

Unternehmensintern zu regeln.

Für RA, Repository, etc. gemäß spezieller Verhaltensregeln für diese Mitarbeitergruppe.

Für End-User gemäß Unternehmensrichtlinien

6.2.5 Archivierung privater Schlüssel

Eine Archivierung von Schlüsseln der Zertifizierungsstellen erfolgt nicht.

Während des Vorpersonalisierungsprozesses für Nutzer wird die Archivierung des privaten Verschlüsselungsschlüssels in der Zertifizierungsstelle durchgeführt.

Prozessbeschreibung:

Nach der Generierung des öffentlichen und privaten Schlüssels mit dem Zertifikat in der Zertifizierungsstelle wird ein PKCS#12 File zur Verfügung gestellt. In den Sicherheitsrichtlinien der Zertifizierungsstelle ist die Schlüsselarchivierung aktiviert. Anschließend erfolgt der Export des PKCS#12 Files durch Mitarbeiter der Registrierungsstelle auf den Mitarbeiter-Token. Nach einem erfolgreichen Abschluss des Vorganges wird das PKCS#12 File automatisch in der Zertifizierungsstelle gelöscht und befindet sich nur noch im gesicherten Archiv der Zertifizierungsstelle.

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Die technischen Sicherheitsmaßnahmen **müssen** im Rahmen der Sicherheits-Policy der Zertifizierungsstelle erfolgen und orientieren sich am aktuellen Stand der Technik.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Die technischen Sicherheitsmaßnahmen **müssen** im Rahmen der Sicherheits-Policy der Zertifizierungsstelle erfolgen und orientieren sich am aktuellen Stand der Technik.

6.2.8 Aktivierung privater Schlüssel

Die Aktivierung des Signaturschlüssels erfolgt mit einer 4-8-stelligen PIN. Der Zugriff auf das Personal Security Environment wird dem Benutzer signalisiert.

Für Massensignaturen muss nicht jedes Mal die PIN eingegeben werden.

6.2.9 Deaktivierung privater Schlüssel

Eine Deaktivierung erfolgt automatisch nach einer definierten Zeitspanne und zum Sitzungsende.

6.2.10 Zerstörung privater Schlüssel

Nicht relevant

6.2.11 Beurteilung kryptographischer Module

Nicht relevant

6.3 Andere Aspekte des Managements von Schlüsselpaaren

Nicht relevant

6.3.1 Archivierung öffentlicher Schlüssel

Nicht relevant

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren (CP)

Die Zertifikate und Schlüsselpaare **sollten** einer periodischen Vergrößerung der Schlüssellängen unterliegen, um das Sicherheitsniveau ausreichend zu erhalten.

Es gelten die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

6.4 Aktivierungsdaten

Die Zertifizierungsstelle **muss** geeignete Prozesse zur sicheren Übermittlung von Aktivierungsdaten definieren.

Festlegungen, synchron zu Regelungen beim Mitarbeiterausweis, sind sinnvoll.

6.4.1 Aktivierungsdaten

Muss ausführlich unternehmensintern geregelt werden.

6.4.2 Schutz von Aktivierungsdaten

Muss unternehmensintern geregelt werden.

6.4.3 Andere Aspekte von Aktivierungsdaten

Keine Vorgaben

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Alle IT-Komponenten der PKI unterliegen den Sicherheitsanforderungen der existierenden IT-Sicherheitsrichtlinien.

6.5.2 Beurteilung von Computersicherheit

Die Beurteilung **sollte** im Rahmen von internen Audits erfolgen.

6.6 Technische Maßnahmen während des Life Cycles

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

Die Beurteilung **sollte** im Rahmen von internen Audits erfolgen.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Alle IT-Komponenten der PKI unterliegen den Sicherheitsanforderungen der existierenden IT-Sicherheitsrichtlinien.

6.6.3 Sicherheitsmaßnahmen während des Life Cycles

entfällt

6.7 Sicherheitsmaßnahmen für Netze

Alle IT-Komponenten der PKI **müssen** den Sicherheitsanforderungen der existierenden IT-Sicherheitsrichtlinien unterliegen.

6.8 Zeitstempel

Die Archivierung erfolgt gemäß prinzipieller Anforderungen des Signaturgesetzes §17 an die Langzeitarchivierung digital signierter Dokumente. Dabei muss der Zeitstempeldienst nicht zwingend qualifizierte Zeitstempel erzeugen.

7 Profile von Zertifikaten, Sperrlisten und OCSP (CP)

7.1 Zertifikatsprofile

7.1.1 Versionsnummern (CP)

Zertifikate **müssen** konform zum Standard X.509 v3 (Type 0x2) sein.

7.1.2 Zertifikatserweiterungen (CP)

Die Zertifizierungsstelle **muss** die Zertifikatserweiterungen definieren.

Folgende Zertifikatserweiterungen **müssen** kritisch sein:

KeyUsage,

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

Für die KeyUsage und BasicConstraints (von CA-Zertifikaten) **müssen** die Vorgaben der ISIS-MTT-Profilierung eingehalten werden (siehe [ISIS/MTT] ISIS/MTT Version 1.1, Part 1. Table 12: KeyUsage)

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

Die E-Mail-Adresse **soll** im Zertifikat enthalten sein, entweder

- im SubjectAltName (rfc822Name, bevorzugt) oder
- innerhalb des DN (E=)

7.1.3 Algorithmen OID

Keine Bedingungen, aber Orientierung an den BSI-Empfehlungen bzw. der Bundesnetzagentur-Verordnung wird empfohlen.

7.1.4 Namensformate (CP)

Die CA **muss** Namensformate dokumentieren. Grundsätzlich sollen Konformitätskriterien beachtet werden. Darüber hinaus gelten die folgenden Anforderungen.

- Im DistinguishedName (DN) **muss** der CommonName (CN) angegeben werden.
- Der DN im End Entity Zertifikat **muss** innerhalb der ausgebenden CA eindeutig sein.
- Nicht personengebundene Zertifikate **müssen** zu erkennen sein (im DN oder anderswo).

7.1.5 Namensbeschränkungen

Keine Bedingungen

7.1.6 OID der Zertifikatsrichtlinien

Keine Bedingungen

Es wird **empfohlen**, die OID dieser CP als nicht kritische Erweiterung in das Attribut „certificatePolicies“ einzutragen.

7.1.7 Nutzung der Erweiterung „Policy Constraints“

Keine Bedingungen

7.1.8 Syntax und Semantik von „Policy Qualifiers“

Keine Bedingungen

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung Zertifikatsrichtlinie

Keine Bedingungen

7.2 Sperrlistenprofile (CP)

Eine CRL **muss** Version, Signature, Issuer Name, Date Issued, Issue Date for Next Update, Revoked Certificates enthalten.

Der Sperrlistengrund wird nicht extern veröffentlicht.

7.2.1 Versionsnummer(n) (CP)

Es **müssen** Sperrlisten der Version 1 oder einer höheren Version verwendet werden.

Aus Interoperabilitätssicht **sollten** jedoch Sperrlisten mit Version 2 (Typ 0x1) eingesetzt werden.

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

Keine Bedingungen

7.3 Profile des Statusabfragedienstes (OCSP) (CP)

Entfällt zunächst

7.3.1 Versionsnummer(n) (CP)

Entfällt zunächst

7.3.2 OCSP Erweiterungen (CP)

Stellt die Zertifizierungsstelle eine OCSP-Statusprüfung zur Verfügung, **müssen** diese Erweiterungen auch dokumentiert werden.

8 Überprüfungen und andere Bewertungen

8.1 Häufigkeit und Bedingungen für Überprüfungen

Bilateral zwischen den beteiligten Unternehmen zu regeln.

8.2 Identität/Qualifikation des Prüfers

Bilateral zwischen den beteiligten Unternehmen zu regeln.

8.3 Stellung des Prüfers zum Bewertungsgegenstand

Bilateral zwischen den beteiligten Unternehmen zu regeln.

8.4 Durch Überprüfungen abgedeckte Themen

Bilateral zwischen den beteiligten Unternehmen zu regeln.

8.5 Reaktionen auf Unzulänglichkeiten

Bilateral zwischen den beteiligten Unternehmen zu regeln.

9 Andere finanzielle und rechtliche Angelegenheiten

Im CP des Teilnehmers **sollten** zumindest zu den folgenden Abschnitten Anforderungen publiziert werden:

- Abschnitt 9.4 Datenschutz von Personendaten
- Abschnitt 9.10 Gültigkeitsdauer und Beendigung
- Abschnitt 9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern
- Abschnitt 9.14 Zugrunde liegendes Recht
- Abschnitt 9.16.3 Salvatorische Klausel

9.1 Preise

9.1.1 Preise für Zertifikate oder Zertifikatserneuerungen

9.1.2 Preise für den Zugriff auf Zertifikate

9.1.3 Preise für Sperrungen oder Statusinformationen

9.1.4 Preise für andere Dienstleistungen

9.1.5 Regeln für Kostenrückerstattungen

9.2 Finanzielle Zuständigkeiten

9.2.1 Versicherungsdeckung

9.2.2 Andere Posten

9.2.3 Versicherung oder Gewährleistung für Endnutzer

Der Issuer versichert, dass die über die PKI bereitgestellte Infrastruktur geeignet ist, Echtheit der Herkunft und Unversehrtheit des Inhaltes zu gewährleisten.

Hinweis: Damit ist die Infrastruktur, insbesondere zum elektronischen Austausch von Rechnungsdaten per Electronic Data Interchange gemäß §14 Absatz 3 Umsatzsteuergesetz und ähnlicher formgebundener Dokumente geeignet. Entsprechende Endnutzer bedürfen dazu eines bilateralen EDI-Vertrages gemäß Anforderungen der EG-Empfehlung 94/820/EG unter Bezug auf das vorliegende CP.

9.3 Vertraulichkeitsgrad von Geschäftsdaten

Das Mitglied am Verfahren versichert, dass ihm zugängliche Daten (z. B. CPS-Dokumente anderer Teilnehmer) auf Wunsch vertraulich behandelt werden.

Die PKI definiert weder, was vertrauliche Daten sind, noch stellt sie bestimmte Anforderungen an die Handhabung solcher Daten. Dies ist ggf. in anderen Policy-Dokumenten geregelt. Sie stellt „lediglich“ eine Infrastruktur bereit, über die vertrauliche Daten sicher ausgetauscht werden können. Regelungen zur Definition und zum Umgang mit vertraulichen Business-Daten sind jeweils bilateral zwischen den jeweiligen Partnern zu treffen.

9.3.1 Definition von vertraulichen Informationen

Vertrauliche Informationen sind Informationen, die lediglich im Rahmen des Verfahrens zugänglich gemacht werden und nicht für eine breite Öffentlichkeit bestimmt sind.

Das CPS, das die Anforderungen des vorliegenden CP abdeckt und das vertraulich behandelt wird, regelt betriebliche und technische Anforderungen innerhalb der PKI für die jeweilige Einheit.

9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören

Perspektivwechsel:

Das CP des Mitglieds am Verfahren (z. B. Marktteilnehmer) stellt eine Untermenge an Aussagen aus dem CPS dar, die öffentlich gemacht werden können.

9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen

Perspektivwechsel:

Auf Vorschlag des zuständigen Bereichs des Mitglieds am Verfahren (z. B. Marktteilnehmer) werden anlassbezogen CPS und CP überarbeitet.

9.4 Datenschutz von Personendaten

Die Teilnehmer gewährleisten den Datenschutz gemäß gesetzlicher Vorgaben des Datenschutzgesetzes.

Die Teilnehmer am Verfahren stellen Zertifikatsinformationen und weitere Personendaten auf ihre eigene Verantwortung in externe (LDAP-)Verzeichnisse.

Der externe Verzeichnisdienst unterstützt nur vollqualifizierte Anfragen über eine vollständige und eindeutige E-Mail-Adresse.

9.4.1 Datenschutzkonzept

Muss ausführlich unternehmensintern geregelt werden.

9.4.2 Als persönlich behandelte Daten

Muss ausführlich unternehmensintern geregelt werden.

9.4.3 Daten, die nicht als persönlich behandelt werden

Muss ausführlich unternehmensintern geregelt werden.

9.4.4 Zuständigkeiten für den Datenschutz

Muss ausführlich unternehmensintern geregelt werden.

9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten

Im Rahmen der betrieblichen Mitbestimmung wird möglichst gewährleistet, dass Zertifikatsinformationen extern veröffentlicht werden dürfen. Mindestens **müssen** Sperrlisten veröffentlicht werden können.

9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften

möglich

9.4.7 Andere Bedingungen für Auskünfte

Auskunft an Dritte erfolgt lediglich im Rahmen der externen Verzeichnisdienste und ihrer technischen Zugriffsmöglichkeiten.

Das CP wird im Internet unter xxx.yyy.zzz veröffentlicht. Es wird nach bestem Wissen und Gewissen erstellt und regelmäßig gepflegt. Eine Garantie auf Richtigkeit muss nicht abgegeben werden.

9.5 Geistiges Eigentumsrecht

ggf. bilateral zu regeln

9.6 Zusicherungen und Garantien

Alle Beteiligte sichern eine gleichbleibend hohe Güte in Datenqualität, Organisation und technischen Diensten zu.

9.6.1 Zusicherungen und Garantien der CA

Bilateral zwischen den beteiligten Unternehmen zu regeln.

9.6.2 Zusicherungen und Garantien der RA

Der RA ist bewusst, dass der Registrierungsprozess und insbesondere die zweifelsfreie Identifikation des Zertifikatsnehmers von entscheidender Bedeutung ist und deshalb größtmöglicher Sorgfalt unterliegen muss.

9.6.3 Zusicherungen und Garantien der Zertifikatsnehmer

Durch arbeitsrechtlich verbindliche Vereinbarungen und Anweisungen wird Bedeutung und Tragweite im Umgang mit kryptographischen Schlüsseln verdeutlicht. Dies gilt insbesondere für die elektronische Signatur und das Identity Management.

9.6.4 Zusicherungen und Garantien der Zertifikatsnutzer

Zertifikate werden nur zum Zwecke der Sicherheitsverfahren genutzt und können zu diesem Zwecke über die Infrastruktur auch dezentral gespeichert werden. Weitere fremde Zwecke, wie das Sammeln von E-Mail-Adressen, werden durch die Zertifikatsnutzer ausgeschlossen.

9.6.5 Zusicherungen und Garantien anderer PKI-Teilnehmer

entfällt

9.7 Haftungsausschlüsse

Bilateral zwischen den beteiligten Unternehmen zu regeln.

9.8 Haftungsbeschränkungen

Bilateral zwischen den beteiligten Unternehmen zu regeln.

9.9 Schadensersatz

Bilateral zwischen den beteiligten Unternehmen zu regeln.

9.10 Gültigkeitsdauer und Beendigung

Dieses CP gilt solange, bis es durch ein anderes ersetzt wird.

9.10.1 Gültigkeitsdauer

9.10.2 Beendigung

9.10.3 Auswirkung der Beendigung und Weiterbestehen

9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern (CP)

Diese **müssen** prinzipiell dann offen gelegt werden, wenn sie Auswirkungen auf das allgemeine Sicherheitsniveau haben.

9.12 Ergänzungen

Nachträge zum CP werden schriftlich ergänzt oder bei elektronischer Abrufbarkeit so ergänzend hinterlegt werden, dass sie dem Abrufenden unmittelbar als Ergänzung offensichtlich werden.

9.12.1 Verfahren für Ergänzungen

gemäß 9.12.

9.12.2 Benachrichtigungsmechanismen und –fristen

gemäß 9.12.

9.12.3 Bedingungen für OID-Änderungen

Eine OID für das CP **sollte** vergeben werden und unterhalb der beantragten Unternehmens-OID liegen.

9.13 Bestimmungen zur Schlichtung von Streitfällen

Bilateral zwischen den beteiligten Unternehmen zu regeln.

9.14 Zugrunde liegendes Recht (CP)

Deutsche Gesetzgebung

9.15 Einhaltung geltenden Rechts

Wird gewährleistet

9.16 Sonstige Bestimmungen

Bilateral zwischen den beteiligten Unternehmen zu regeln.

Diese **müssen** prinzipiell dann offen gelegt werden, wenn sie Auswirkungen auf das allgemeine Sicherheitsniveau haben.

9.16.1 Vollständigkeitserklärung

Das vorliegende Dokument beschreibt aus Sicht des VDEW prinzipielle organisatorische und technische Regelungen, die zwingend einzuhalten sind, damit zwischen den Marktteilnehmern beim elektronischen Datenaustausch ein vergleichbares und garantiertes Sicherheitsniveau eingehalten werden kann.

9.16.2 Abgrenzungen

offen

9.16.3 Salvatorische Klausel

Vorschlag für bilaterale Verträge, unter Bezug auf ein CPS, das sich nach dieser CP orientiert: Sollten Bestimmungen dieser Policy unwirksam sein oder werden oder **sollte** sich in dem Vertrag eine Lücke herausstellen, so soll hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt werden. Anstelle der unwirksamen Bestimmungen oder zur Ausfüllung der Lücke sollen Regelungen gelten, die – soweit rechtlich möglich – dem am nächsten kommen, was die Vertragspartner gewollt haben oder nach dem Sinn und Zweck des Vertrages gewollt haben würden, sofern sie den Punkt bedacht hätten.

9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

Unternehmensintern zu regeln

9.16.5 Höhere Gewalt

offen

9.17 Andere Bestimmungen

offen

10 Anhang

10.1 Anhang 1: Wichtige Begriffe in einer Public Key Infrastruktur

Asymmetrische Kryptographie	Ein mathematisches Verfahren zur Datenverschlüsselung, in dem zwei verschiedene mathematisch zusammengehörende Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet werden.
Authentifizierung/ Authentisierung	Die Authentifizierung (auch Authentifikation, engl. authentication) bezeichnet den Vorgang, die Identität einer Person oder eines Programms anhand eines bestimmten Merkmals zu überprüfen. Dies kann zum Beispiel mit einem Fingerabdruck, einem Passwort oder einem beliebigen anderen Berechtigungsnachweis geschehen. Nah verwandt mit der Authentifizierung ist die Authentisierung. Die Authentisierung ist das Nachweisen einer Identität, die Authentifizierung deren Überprüfung. Im Englischen wird zwischen den beiden Begriffen nicht unterschieden, das Wort authentication steht für beides. Ein Benutzer authentisiert sich zertifikatsbasiert gegenüber einer Anwendung mit seinem PSE, anstatt mit Kennung und Passwort. Die Anwendung überprüft (authentifiziert) die Gültigkeit des Zertifikats. Normungsgrundlage ist der RFC 3281. ISIS-MTT hat ein Profil vorgelegt. VEDIS nutzt nur die so genannte PUSH-Variante des Profils.
Besitzer, Schlüsselbesitzer	Der Besitzer eines Schlüssels ist der End-User, der über den privaten Schlüssel (in der Form des Personal Security Environments, PSE) verfügt und für dessen korrekten Einsatz verantwortlich ist. Bei einem persönlichen Schlüsselpaar ist der Eigentümer auch immer der Besitzer, weil es verboten ist, den persönlichen Schlüssel weiterzugeben.
Certification **A**uthority, CA „Trustcenter“	**C**ertification **A**uthority Instanz, die die Bindung eines Public Key an einen Benutzer in Form eines Zertifikates herstellt und

	mit der eigenen digitalen Signatur beglaubigt.
Chipkarte	Karte im Scheckkartenformat gemäß externem Zugriff über ISO 7816-Norm mit eingebettetem Mikrochip. Besitzt dieser Mikrochip einen programmierbaren Controller (CPU), so wird von einer SmartCard gesprochen. In einer PKI werden dann, wenn SmartCards als Trägermedium eingesetzt werden, praktisch ausschließlich hochsichere Chips mit Kryptocoprozessor eingesetzt.
Corporate Directory, Verzeichnisdienst	Das Corporate Directory ist das Verzeichnis, in dem unternehmensweit verfügbare Informationen der Angestellten eingetragen sind. Es dient auch dazu, Zertifikate zu veröffentlichen und unternehmensweit bereitzustellen bzw. durch geeignete Spiegelungsmechanismen ein Teil der Informationen (z. B. Name, Vorname, E-Mail und Zertifikat) auch extern bereitzustellen.
Digitale Signatur, heute elektronische Signatur	Eine elektronische Signatur stellt eine kryptographische Umformung von Daten dar, um diese vor unbemerkten Verfälschungen zu schützen (Schutz der Integrität). Mit digitaler Signatur wird meistens der Vorgang des digitalen Signierens assoziiert, der regional geltenden Gesetzen unterliegen kann. Die Bedeutung ist weiter gefasst, d. h. entspricht nicht dem Signaturgesetz.
Eigentümer, Schlüsseleigentümer	Der Eigentümer eines Schlüsselpaars ist der End-Benutzer, der für die korrekte Nutzung und Unversehrtheit des privaten Schlüssels verantwortlich ist. Der Eigentümer oder der Aussteller (CA) führt auch den Widerruf des Schlüsselpaars durch.
Fortgeschrittene Signatur (FS)	Im Gegensatz zu einer einfachen elektronischen Signatur (z. B. einkopierter Unterschriftszug) ist eine fortgeschrittene Signatur a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet b) ermöglicht die Identifizierung des Signaturschlüssel-Inhabers, c) ist mit Mitteln erzeugt worden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann und d) mit den Daten, auf die sie sich beziehen, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann. Der Vertrauensraum, in dem FS gültig sind, muss

	organisatorisch und technisch definiert werden. VEDIS strebt ein starkes organisatorisches Sicherheitsniveau an, um mit geringerem technischen und damit wirtschaftlichem Aufwand fortgeschrittene Signaturen akzeptieren zu können.
Hash-Algorithmen	Beim Hashen eines Dokumentes wird zunächst vom Dokument eine z. B. 160 Bit lange Zahl gebildet (Einwegfunktion). Es ist extrem unwahrscheinlich, dass zu verschiedenen Dokumenten ein gemeinsamer Hashwert existiert (kollisionsresistent). Der Hashwert wird anschließend mit dem privaten Signierschlüssel signiert, d. h. verschlüsselt, so dass er mit dem öffentlichen Schlüssel aus dem Zertifikat entschlüsselt werden kann. Die Validierung beim Dokumenten-Empfänger erfolgt dadurch, dass zunächst eigenständig der Hashwert über das Dokument gebildet wird. Anschließend wird dieser mit dem am Dokument mitübermittelten, mit Hilfe des öffentlichen Signierschlüssel des Signierers entschlüsselten Hashwerts verglichen. Stimmen beide Werte überein, wurde das Dokument nach der Signatur nicht verändert.
ISIS-MTT	Praktikable und eindeutig umsetzbare Profilierung der internationalen PKI-Normen Konformität kann mit dem Testbed überprüft werden. Deutschlandweit akzeptiert und international auf dem Vormarsch
Kettenmodell	Unter der Gültigkeitsregel des Kettenmodells ist eine Zertifikatskette technisch gültig, wenn unter anderem jedes Zertifikat der Kette innerhalb des Gültigkeitszeitraums des jeweiligen übergeordneten Zertifikats ausgestellt wurde. Nach § 19 Abs. 5 SigG bleibt die „Gültigkeit der ... qualifizierten Zertifikate ... von der Untersagung des Betriebes und der Einstellung der Tätigkeit sowie der Rücknahme und dem Widerruf einer Akkreditierung unberührt“. Damit wird nach deutschem Signaturgesetz das Kettenmodell als Validierungsmodell für elektronische Signaturen zugelassen. (siehe auch Schalenmodell)
Kryptoalgorithmus	Mathematisches Regelwerk, um kryptographische Operationen (z. B. Verschlüsseln, Hashen), ausgehend von elementaren mathematischen Funktionen (z. B. Verschieben, Multiplizieren, Restwert bilden) mit Hilfe von Schlüsseln und Parametern rekursiv zu vollziehen.

LDAP	Lightweight Directory Access Protocol LDAP ist ein TCP/IP-basiertes Directory-Zugangsprotokoll, das sich im Internet und in Intranets als Standardlösung für sichere Verzeichnisdienste etabliert hat.
LRA	Local Registration Authorities; Autorisierte, anwendernahe Stelle, welche die Identifizierung und Authentifizierung der User sicherstellt sowie das Schlüsselmaterial an die User übergeben und verwalten soll.
Nutzer, kryptographischer Verfahren in der PKI	• Person (auch: End-Benutzer): Angestellte/-er, Werkstudent/-in, Auszubildende/-er, Consultant (jeweils beim Unternehmen oder einem Geschäftspartner). • Organisation: Projektgruppe (innerhalb oder außerhalb des Unternehmens), Dienststelle, Geschäftspartner-Firma usw. • Verfahren: Dienst, Client, Server, Zertifizierungsstelle, LRA usw. • Einrichtung: Rechner, Router, Firewall usw. • Ein solcher Nutzer ist entweder Anwender eines Personal Security Environments (PSE) oder eines Zertifikats oder selbst Ziel einer Anwendung von Zertifikaten.
Öffentlicher Schlüssel, public key	Der öffentliche Schlüssel ist der für jedermann zugängliche Teil eines Schlüsselpaars, das in der asymmetrischen Kryptographie verwendet wird.
Personal Security Environment	PSE Summe des Schlüsselmaterials –insbesondere der privaten Schlüssel-, Zertifikate und weiterer Kontrollinformationen eines Users. Das Personal Security Environment (PSE) besteht hauptsächlich aus dem privaten Schlüssel und anderen Informationen, die dem Nutzer gehören, der allein Zugang zum privaten Schlüssel hat. Das PSE muss deshalb vor dem Zugriff durch Andere geschützt sein. SmartCards, Chipkarten und Disketten sind Datenträger, auf denen das PSE gespeichert wird.
Personalisierung	Zusammenführung von Personendaten zu Kartendaten
Persönlicher Schlüssel	Ein asymmetrisches Schlüsselpaar ist ein persönliches Schlüsselpaar, wenn Besitzer und Eigentümer des dazugehörenden Personal Security Environments nur ein und dieselbe Person sein dürfen und der Name dieser Person im

	Zertifikat beglaubigt ist.
Persönlicher Schlüssel. privater Schlüssel, private key	Der private Schlüssel ist der geheime Teil des Schlüsselpaars (eines persönlichen Schlüssels, eines Funktionsschlüssels), der in der asymmetrischen Kryptographie verwendet wird.
PIN, Personal Identity Number	Die PIN ist hier ein Passwort, mit dem ein End-Benutzer sich beim Zugriff auf das Personal Security Environment authentifiziert. Die PIN dient zum Vertraulichkeitsschutz des PSE, insbesondere des darin enthaltenen privaten Schlüssels.
Policy, PKI-	Ein Sicherheitskonzept besteht aus organisatorischen und technischen Maßnahmen und ist im Allgemeinen in einer Security-Policy niedergelegt. Die Public Key Infrastruktur wird in einer PKI-Policy niedergelegt und beschreibt das organisatorische Regelwerk, die technischen Komponenten sowie ihr Zusammenspiel. Die PKI-Policy ist das zentrale Dokument einer PKI schlechthin und definiert das Sicherheitslevel der PKI. Aussagen der PKI-Policy werden je nach Adressat oft auch in mehreren Policy-Dokumenten gemacht. Die Certificate Policy ist die oft vertragsrechtlich bindende Erklärung an Geschäftspartner. Das Certificate Practice Statement ist Umsetzungsvorgabe oder -Dokumentation. In Auftraggeber-Auftragnehmer-Beziehungen ist es Grundlage von SLA.
Private Key	Beim symmetrischen Verfahren spricht man von einem geheimen Schlüssel, den beide Kommunikationspartner besitzen. Beim asymmetrischen Verfahren hat jeder Teilnehmer einen öffentlichen Schlüssel (Public Key) und einen privaten Schlüssel. Mit dem privaten Schlüssel wird signiert und mit dem öffentlichen Schlüssel die Unterschrift geprüft (validiert). Mit dem privaten Schlüssel kann der Empfänger die mit dem öffentlichen Schlüssel des Empfängers verschlüsselte Nachricht wieder entschlüsseln siehe auch Public Key Kryptographie
Public Key Infrastructure	PKI PKI ist die Summe aller Instanzen und Verfahren, die zum Einsatz der Public Key Kryptographie notwendig sind. Sie werden im Allgemeinen in einer Policy beschrieben.

Public Key Kryptographie	Verschlüsselungsverfahren, bei dem 2 verschiedene Schlüssel zum Ver- und zum Entschlüsseln einer Nachricht verwendet werden (daher auch die Bezeichnung asymmetrische Kryptographie). In der praktischen Anwendung wird einer dieser Schlüssel mit den Identifikationsdaten des Inhabers veröffentlicht (= public key) und der andere dem Inhaber auf einem sicheren Weg (häufig auf einer SmartCard) übergeben oder gleich in der SmartCard generiert. Eine wichtige Anwendung der Public Key Kryptographie ist die elektronische Signatur, bei der ein Dokument mit dem private key signiert wird und bei der dann der Empfänger mit Hilfe des public key die Signatur überprüft.
Registration Authority	Registration Authority, auch Local Registration Authority (LRA) Stelle, an der die zweifelsfreie Identitätsfeststellung des Endanwenders und die Ausgabe von Schlüsselmaterial stattfindet.
Registrierung	Feststellung der Identität im Personalisierungsprozess in einer (L)RA und signierte Weitergabe der Daten über einen sicheren Kanal an das Trustcenter. Voraussetzung ist die Antragstellung. Dem Teilnehmer im Verfahren für digitale Signaturen wird dabei ein geeigneter, eindeutiger Name zugewiesen.
Qualifizierte Signatur	Nach §2 des Signaturgesetzes vom 22.5.2001 sind “qualifizierte elektronische Signaturen” elektronische Signaturen nach Nummer 2, die a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und b) mit einer sicheren Signaturerstellungseinheit erzeugt werden. Zur Ausgabe von qualifizierten Zertifikaten sind umfangreiche Anforderungen gemäß Signaturverordnung zu erfüllen. In Abgrenzung zu so genannten qualifizierten elektronischen Signaturen mit Anbieterakkreditierung (kurz: qualifiziert akkreditierte Signaturen) wird meist die Anzeigepflicht des ZDA und nicht die freiwillige Akkreditierung gemeint. Technisch bedeutet dies, dass nicht die Root-CA der Bundesnetzagentur oberste Wurzelinstanz in der Validierungskette ist, sondern diese angezeigte CA.

	Dadurch werden Abweichungen von internationalen Gegebenheiten vermieden, weil mit Redaktionsschluss dieses Dokumentes die Root-CA der Bundesnetzagentur als Hashalgorithmus RIPEMD und nicht den international üblichen SHA-1 und als Validierungsmodell das Kettenmodell und nicht das international übliche Schalenmodell verlangt. Zur Zeit bietet nur ein ZDA (neben akkreditierten) auch rein qualifizierte Zertifikate an. Im Behördenumfeld sind weitere Projekte in der Realisierung.
S/MIME	**S**ecure **M**ultipurpose **I**nternet **M**ail **E**xtensions Ermöglicht das sichere Versenden und den sicheren Empfang von E-Mails.
Schalenmodell	Unter der Gültigkeitsregel des Schalenmodells ist eine Zertifikatskette technisch gültig, wenn unter anderem jedes Zertifikat der Kette vom Gültigkeitszeitraum des übergeordneten Zertifikats vollständig eingeschlossen wird. Nach dem 1. Signatur Änderungsgesetz (beschlossen 12.11.2004) wird § 8 SigG dahingehend geändert, dass weitere Sperrgründe vertraglich vereinbart werden können. Damit wird ein modifiziertes Schalenmodell möglich.
Schlüssel, Schlüsselpaar	Ein zusammengehörendes Paar, bestehend aus einem privaten und einem öffentlichen Schlüssel, das zur Durchführung der asymmetrischen Kryptographie benötigt wird, wird hier als „Schlüsselpaar“ oder abkürzend als „Schlüssel“ bezeichnet.
Schlüsselmaterial	Die Zusammenfassung von persönlichem Schlüsselmaterial (Personal Security Environment) und dazugehörendem (öffentlichem) Schlüsselzertifikat.
Schlüsselsicherung (Key Backup)	„Schlüsselsicherung“ ist als Instanz in der Unternehmens-PKI-Organisation zuständig für die Sicherung privater Schlüssel, mit denen Entschlüsselungen vorgenommen werden sollen von Daten, deren unverschlüsseltes Original nicht verfügbar ist. Diese Komponente der PKI übernimmt, speichert und gibt Zugriff auf private Schlüssel bzw. ermöglicht die Anforderung auf die Wiederbeschaffung von Originaldaten (Data Recovery). Sie liegt nur im Einflussbereich des Unternehmens.
Schlüsselzertifikat	Ein Zertifikat ist eine Beglaubigung, die bestätigt, dass ein öffentlicher Schlüssel an Informationen, die Person, Organisation, Verfahren oder Einrichtung als Nutzer des zugehörigen privaten Schlüssels identifizieren, gebunden ist.

	Bei einem Zertifikat für einen persönlichen Schlüssel bestehen diese Informationen im wesentlichen aus den Identitätsdaten des Schlüsseleigentümers. Bei einem Zertifikat für einen Schlüssel ohne Personenbindung identifizieren die Informationen z. B. eine Dienststelle, eine Funktion, einen Server, ein IT-System, ein Verfahren, die berechtigt sind, den dazugehörigen Schlüssel einzusetzen. Kein Gegenstand der Ausarbeitung.
Security Policy	Verbindliches Dokument zur Beschreibung der Sicherheitspolitik eines Unternehmens. Mögliche Geschäftsrisiken werden bewertet und ggf. Maßnahmen festgelegt. Risiken sind sowohl unerwartete negative Ereignisse als auch unrealisierte geschäftliche Chancen. IT-Security ist Teil der Sicherheitspolitik; PKI-Policy ist Teil der Security Policy. Somit ergänzt dieses Dokument die Security Policy des Einzelunternehmens.
SmartCard	Kleinrechner im Scheckkartenformat. Sie besitzt einen Chip (auf einem Modul aufgebracht), der einen Prozessor, Datenspeicher (File System) und ein Betriebssystem enthält. Ein wesentlicher Aspekt des Betriebssystems ist der integrierte Zugriffsschutz auf Daten im File System. Erst nach Eingabe einer korrekten PIN oder durch eine Authentisierung kann z. B. der entsprechende Zugriffsstatus erreicht werden, so dass die in der jeweiligen Datei enthaltenen Daten an die Außenwelt abgegeben werden. Der Prozessor führt auch selbstständig kryptographische Rechenoperationen durch.
Sperrung (des Signatur-Zertifikats)	Vorgang, der dazu dient, bei der Überprüfung/Validierung der Signatur bei der CA oder replizierten Auskunftsdiensten das Zertifikat als ungültig zu erkennen (online). Die Sperrung kann der Teilnehmer oder sein Vertreter vornehmen lassen. Die kartenausgebende Instanz bzw. die CA als zertifikatsausstellende Instanz muss hier eine Vertreterfunktion haben. Die Sperrung muss den Zeitpunkt enthalten und darf nicht rückwirkend erfolgen. Es besteht Unterrichtungspflicht. SigG macht weitere Anforderungen an das Sperrmanagement.
Trust Center, Trustcenter	Instanz mit den möglichen Aufgaben Erzeugung von Schlüsselpaaren, sichere Aufbewahrung von Schlüsselmaterial, Ausstellen, Veröffentlichung und Rücknahme von Public Key-Zertifikaten, siehe auch

	Certification Authority, CA
Verifizieren, Verifikation, Validierung	Beim Verifizieren einer digitalen Signatur wird festgestellt, ob die signierten Daten unverfälscht sind und von der Person, Organisation, dem Verfahren oder der Einrichtung stammen, welche die digitale Signatur erstellt hat, siehe auch Hashwert.
Verschlüsselung	Die Verschlüsselung verhindert, dass unberechtigte Personen oder Dritte die elektronische Kommunikation verwerten können. Dabei werden mathematische Verfahren verwandt, welche die Daten in eine zwar lesbare, aber unverwertbare Form umwandeln (verschlüsseln). Die Rückumwandlung in die ursprüngliche Form (Entschlüsselung) ist nur autorisierten Personen, Organisationen, Verfahren oder Einrichtungen vorbehalten.
Widerruf, Revocation	Zertifikate können oder müssen in bestimmten Fällen durch die Eigentümer oder Besitzer oder Dritte, die nicht dem Unternehmen angehören, widerrufen werden, bevor ihre Gültigkeit abläuft. Mögliche Gründe, die einen Widerruf erzwingen, sind Offenlegung des Personal Security Environments (PSE), Diebstahl oder Verlust des PSE bzw. alle Fälle, in denen der Missbrauch eines PSE vermutet werden muss. Durch einen Widerruf wird der Gebrauch dieses Zertifikats und des zugehörigen PSE dauerhaft unterbunden; denn eine nachfolgende Aufhebung des Widerrufs ist nicht möglich.
Zertifikatsnutzer, Relying Party, Empfänger, Verifizierer, Validierer	Dies sind Personen, Organisationen, Verfahren oder Einrichtungen, die das Zertifikat bzw. den darin enthaltenen öffentlichen Schlüssel benutzen zum Verschlüsseln (vor dem Senden von Daten) oder Verifizieren (nach Empfang von signierten Daten).