Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung

Bundesamt für Sicherheit in der Informationstechnik

Version 3.2 vom 09.01.2003

Godesberger Allee 185-189, 53175 Bonn

Telefon: 0228/9582-0 - Telefax: 0228/9582-405

1 Einleitung 7

2 Überblick 8

2.1 Aufbau der PKI und ihre Schnittstellen 8
2.1.1 Zertifizierungshierarchie 8
2.1.2 Verzeichnisdienst 9

2.2 Kosten 9

2.3 Anwendungsbereich 10

2.4 Personelle Unterstützung 10
2.4.1 Organisationsstruktur 10
2.4.2 Ansprechstelle der Wurzelzertifizierungsstelle 10

3 Allgemeine Bestimmungen 11

3.1 Verpflichtungen der Wurzelzertifizierungsstelle 11

3.2 Verpflichtungen der Zertifizierungsstelle 11

3.3 Verpflichtungen der Endanwender 12

3.4 Vertraulichkeit 12

3.5 Gültigkeitsdauer 12

4 Identifizierung und Authentisierung 13

4.1 Erstmalige Registrierung 13
4.1.1 Identifizierung und Authentisierung einer natürlichen Person 13
4.1.2 Identifizierung und Authentisierung einer juristischen Person 13
4.1.3 Identifizierung und Authentisierung bei Gruppenzertifikaten 14
4.1.4 Anforderungen an die Namensvergabe 14
4.1.5 Eindeutigkeit des Namens von Zertifizierungsstellen 14
4.1.6 Namensraumvergabe der PCA der Verwaltung 14
4.1.7 Anforderungen an die Vergabe von Gruppenzertifikaten 14
4.1.8 Methoden zum Nachweis des Besitzes des geheimen Schlüssels 14

4.2 Regelmäßiges Wiederausstellen 15

4.3 Wiederausstellen nach Sperrung 15

4.4 Sperrantrag 15

5 Geheimhaltungsgrad bei Verschlüsselung 16

6 Ablauforganisation 17

6.1 Zertifikatsantrag 17

6.2 Ausstellung des Zertifikats 17

6.3 Akzeptanz des Zertifikats 18

6.4 Sperrung von Zertifikaten 18

6.4.1 Sperrgründe 18
6.4.2 Zeitdauer zwischen Sperrantrag und Sperrung 18
6.4.3 Ausstellung von Sperrlisten 18
6.4.4 Bekanntgabe von Sperrungen 19
6.4.5 Kompromittierung des geheimen Schlüssels 19
6.4.6 Suspendierung 19

6.5 Beweissicherung und Protokollierung 19

6.6 Schlüsselwechselmanagement 19

6.7 Kompromittierung und Wiederherstellung 20

6.8 Einstellen des Betriebs 20

7 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen für Zertifizierungsstellen 21

7.1 Infrastrukturelle Maßnahmen 21

7.2 Organisatorische Maßnahmen 21

7.3 Personelle Maßnahmen 21

8 Technische Sicherheitsmaßnahmen für Zertifizierungsstellen 22

8.1 Schlüsselgenerierung und -installation 22

8.1.1 Schlüsselgenerierung 22
8.1.2 Übergabe der öffentlichen Schlüssel und Zertifikaten 22
8.1.3 Akzeptanz von Zertifikaten 22
8.1.4 Kryptoalgorithmen, Schlüssellänge, Parametergenerierung 22
8.1.5 Schlüsselnutzung 23

8.2 Schutz des geheimen Schlüssels 23

8.2.1 Schlüsselteilung 23
8.2.2 Key Escrow 23
8.2.3 Backup des privaten Schlüssels 23

8.2.4 Archivierung des privaten Schlüssels 23
8.2.5 Schlüsselinstallation und Aktivierung 23
8.2.6 Schlüsselvernichtung 23

8.3 Weitere Aspekte des Schlüsselmanagements 24
8.3.1 Archivierung öffentlicher Schlüssel 24
8.3.2 Nutzungsdauer für öffentliche und private Schlüssel 24

8.4 Aktivierungsdaten 24

9 Profile für Zertifikate und Sperrlisten (CRLs) 25

10 Änderung und Anerkennung dieser Policy (BSI) .. 26

10.1 Policy Object Identifier 26

10.2 Änderungsmanagement 26

10.3 Anerkennung 26

11 Glossar 27

12 Literaturverzeichnis 31

Änderungshistorie

Version	Datum	Status, Änderungen	Autoren
1.21	17.04.2001	Freigegebene Version	BSI
2.0	03.06.2002	Einfügen der Funktionalität Gruppenzertifikate: • Gruppen • Funktionen • Automatisierte Prozesse Migration zu ISIS-MTT	Andreas Schmidt (Ref I 1.3)
2.1	14.06.2002	Änderungen aufgrund Anmerkungen seitens des BMI	Andreas Schmidt (Ref I 1.3)
3.0	25.11.2002	Freigabe der Erweiterung für SSL u. Änderungen aufgrund: • SSL-Studie (Jörg Völker, Hans-Joachim Knobloch) • Policy-Anpassung (Dörte Neundorf, H-J. Knobloch) • BSI-interne Kommentierung	Andreas Schmidt (Ref I 1.3, BSI)
3.1	10.12.2002	Einfügen der Anmerkungen von Hrn. Zenkert, LfStad in Bayern und von Herrn Jeß, Finanzbehörde Hamburg aufgrund der Abstimmung dieser Policy mit der AG KS des KoopA ADV	Andreas Schmidt (Ref I 1.3, BSI)
3.2	09.01.2003	Einfügen der Anmerkung des BMI (Dr. Schiel, Dr. Rosenhauer) zu Abschnitt 3.5 - Gültigkeitsdauer	Andreas Schmidt (Ref I 1.3, BSI)

1 Einleitung

Mit dem Aufbau einer Wurzelzertifizierungsstelle stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Zertifizierungsstellen aus dem Bereich der öffentlichen Verwaltung (Bund, Länder, Kommunen) Dienstleistungen für eine zertifikatsbasierte Schlüsselinfrastruktur (PKI) bundesweit zur Verfügung.

Darüber hinaus wird angestrebt, die PKI der Verwaltung (PKI-1-VERWALTUNG) in die Bridge-CA der deutschen Wirtschaft zu integrieren. Bei einer derartigen Einbindung würde die Wurzelzertifizierungsstelle, nachfolgend PCA der Verwaltung (PCA-1-VERWALTUNG) genannt, den Nutzerkreis der öffentlichen Verwaltung repräsentieren, wohingegen sich Unternehmen mit ihrer eigenen PKI direkt oder über Dienstleister der Bridge-CA anschließen könnten.

Für die PKI ist die Einschätzung der Vertrauenswürdigkeit der ausgestellten Zertifikate von entscheidender Bedeutung. Die dazu notwendigen Sicherheitsleitlinien (Policy) werden in diesem Dokument beschrieben. Der Aufbau dieses Dokuments lehnt sich dabei an die Empfehlungen des RFC 2527 [12] an, womit es inhaltlich sowohl Elemente einer Policy, als auch des mehr technisch-organisatorisch orientierten Certificate Practice Statements (CPS) vereinigt.

Um der Wurzelzertifizierungsstelle eine größtmögliche Flexibilität einzuräumen, stellen die teilnehmenden Zertifizierungsstellen die Einhaltung dieser Anforderungen über vertragliche Vereinbarungen sicher. Darüber hinausreichenden Regelungen können die Zertifizierungsstellen nach eigenem Ermessen festlegen.

In der jetzigen Ausbaustufe spezifiziert diese Policy in Verbindung mit einem entsprechenden Zertifikatsprofil Leitlinien für die Nutzung der Dienste Verschlüsselung, Authentisierung und fortgeschrittener elektronischer Signaturen im Sinne der durch das Signaturgesetz (SigG) vorgenommenen Umsetzung der EG-Richtlinie.

Die PKI erfüllt mit den erstellten Zertifikaten die Anforderungen an die Sicherheit der Verschlüsselung der Schutzklasse I des Schutzklassenmodells der KBSt (BMI). Es wird damit die Voraussetzung geschaffen, beim Einsatz geeigneter kryptographischer Produkte den Schutz bis zum mittleren Schutzbedarf zu realisieren. Für den Behördenbereich umfasst der mittlere Schutzbedarf den VS-Grad VS-NfD und bestimmte personenbezogene Daten. Werden bestimmte Randbedingungen beachtet, können auch Gruppenzertifikate (für Personengruppen, Funktionen und automatisierte IT-Prozesse) bis zum VS-Grad VS-NfD eingesetzt werden (siehe Abschnitt 4.1.7 und 5).

2 Überblick

2.1 Aufbau der PKI und ihre Schnittstellen

Die PKI basiert auf der MailTrusT-Spezifikation des TeleTrusT Deutschland e.V. in der Version 2 (MTTv2) [1]. Damit wird die Interoperabilität zu international verbreiteten Standards wie X.509, PKIX, S/MIME und LDAP [4] ermöglicht. Gemäß [2] wird die Migration zu ISIS-MTT angestrebt mit dem Ziel der Interoperabilität eines breiten Spektrums getesteter Produkte auf Basis des ISIS-MTT Standards [3].

Die konkret umgesetzten Formate und Protokolle für die Wurzelzertifizierungsstelle sind durch die technischen Grundlagen [5] bereits weitergehend spezifiziert. Das Dokument enthält daneben auch Hinweise und Vorgaben für die Zertifizierungsstellen.

2.1.1 Zertifizierungshierarchie

Die Architektur der PKI der Verwaltung ist in der folgenden Abbildung dargestellt. Die Wurzelzertifizierungsstelle erstellt als oberste Zertifizierungsstelle der Hierarchie ein selbstsigniertes Wurzelzertifikat und signiert die Zertifikate der angeschlossenen Zertifizierungsstellen.

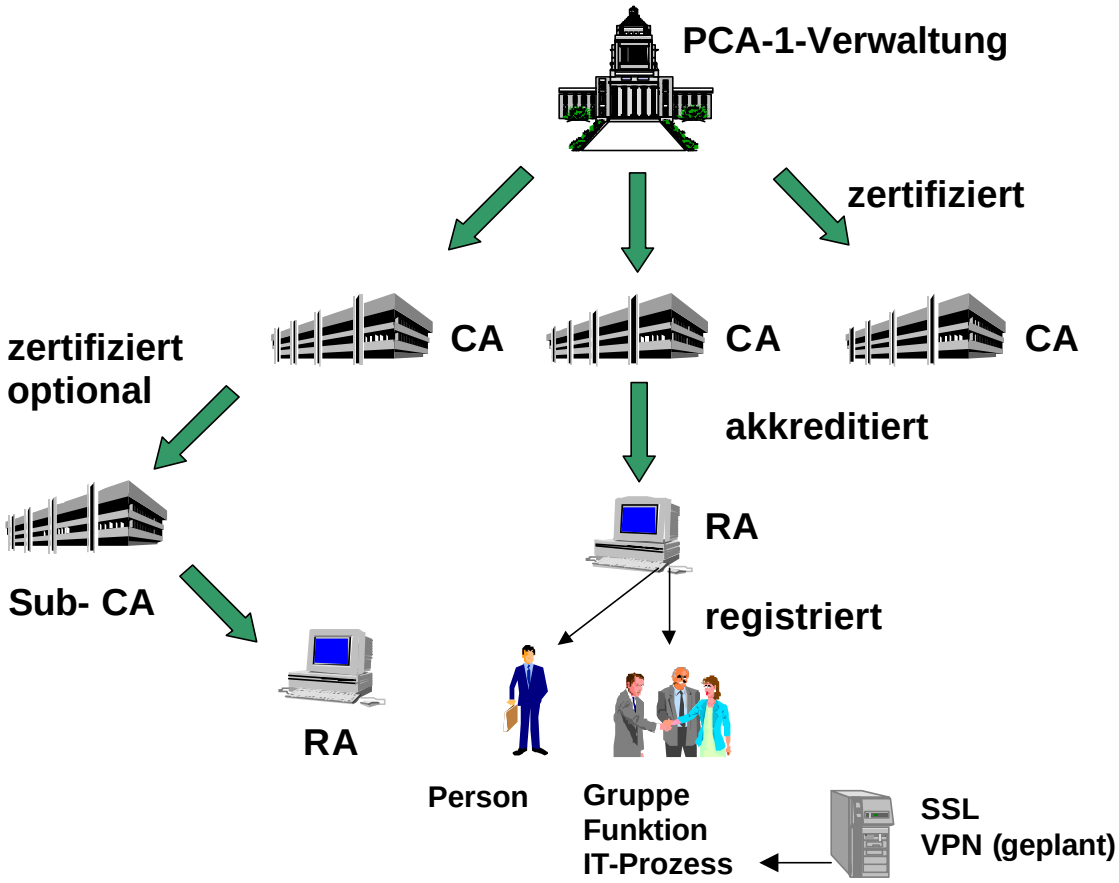
Die von der Wurzelzertifizierungsstelle zertifizierten Zertifizierungsstellen („Certification Authority“ – „CA“) bilden die zweite Stufe der PKI-Hierarchie. Die Endanwender wiederum werden durch die ihnen zugeordnete Zertifizierungsstelle eingebunden und bilden die unterste Stufe der Zertifizierungshierarchie.

Teilnehmer sind Personen, Personengruppen, Funktionen oder Dienste (IT-Prozesse), die im Rahmen der PKI-1-Verwaltung Schlüssel und Zertifikate erhalten oder aus dem Verzeichnisdienst PKI-Informationen von CAs oder Teilnehmern abrufen. Endanwender sind natürliche oder juristische Personen, die Teilnehmer und Inhaber eines Zertifikates der PKI-1-Verwaltung sind. Für natürliche Personen werden Pseudonyme zugelassen.

Ob die jeweilige Zertifizierungsstelle Teilaufgaben, wie z. B. Schlüsselerzeugung oder Identifizierung von Teilnehmern lokalen Registrierungsstellen (Local Registration Authority: LRA), überträgt, wird von der jeweiligen Zertifizierungsstelle in Einvernehmen mit der betroffenen Institution geregelt.

Darüber hinaus steht es jeder Zertifizierungsstelle frei, weitere nachgeordneten Zertifizierungsstellen (SubCA) zu zertifizieren. Um eine praktikable Architektur mit überprüfbaren Sicherheitsleitlinien zu gewährleisten, wird eine maximal fünfstufige PKI-Hierarchie vorgegeben. Sollten besondere Umstände gegen diese Beschränkung sprechen, so ist dies bei der Antragstellung zu begründen und die Genehmigung der PCA der Verwaltung einzuholen.

Die Kopplung zweier unabhängiger Zertifizierungsinfrastrukturen über eine Über-Kreuzzertifizierung ist prinzipiell möglich, erübrigt sich jedoch nach Anschluss der PCA der Verwaltung an die Bridge-CA. Unterhalb der PCA der Verwaltung darf keine derartige Kopplung erfolgen.



2.1.2 Verzeichnisdienst

Die Wurzelzertifizierungsstelle stellt die von ihr ausgestellten Zertifikate und Sperrlisten in den öffentlich zugänglichen Teil des X.500-Verzeichnisses des IVBB (Informationsverbund Berlin-Bonn) ein. Die Verfügbarkeit dieses Verzeichnisses erfüllt die hohen Verfügbarkeitsanforderungen des IVBB. Detailliertere Informationen über Aufbau und Zugriff sind dem Verzeichnisdienstkonzept der PCA der Verwaltung zu entnehmen.

2.2 Kosten

Es gilt die BSI-Kostenverordnung.

2.3 Anwendungsbereich

Die Wurzelzertifizierungsstelle erstellt auf Antrag Zertifikate für alle Zertifizierungsstellen, die den vertraglichen Verpflichtungen einschließlich der Selbsterklärung und dieser Policy nachkommen. Zertifikate können von Zertifizierungsstellen als personenbezogene Zertifikate oder als Gruppenzertifikate ausgestellt werden. Gruppenzertifikate können ausgestellt werden für:

- Personengruppen (z.B. Projektgruppe PKI)
- Funktionen (z.B. Poststelle; Funktion, die durch einen Mitarbeiter ausgefüllt wird)
- Automatisierte IT-Prozesse (z. B. elektron. Stempel, Serverprozesse mit Signatur, SSL-Server).

Der Anwendungsbereich der Zertifikate der PKI der Verwaltung erstreckt sich im Rahmen dieser Policy auf die Verschlüsselung und Authentisierung sowie die fortgeschrittene elektronische Signatur im Sinne der durch das Signaturgesetz (SigG) vorgenommenen Umsetzung der EG-Richtlinie.

2.4 Personelle Unterstützung

2.4.1 Organisationsstruktur

Die Wurzelzertifizierungsstelle wird durch das Bundesamt für Sicherheit in der Informationstechnik in Abstimmung mit dem Bundesministerium des Innern betrieben.

2.4.2 Ansprechstelle der Wurzelzertifizierungsstelle

Bundesamt für Sicherheit in der Informationstechnik
PCA-1-VERWALTUNG
Referat I 1.3
Godesberger Allee 185-189

53175 Bonn

Tel.: 0228 99 9582-0

Fax.: 0228 99 9582-405

e-mail: v-pki@bsi.bund.de

3 Allgemeine Bestimmungen

3.1 Verpflichtungen der Wurzelzertifizierungsstelle

Die Wurzelzertifizierungsstelle übernimmt folgende Verpflichtungen:

- Erzeugung eines kryptographisch geeigneten Schlüsselpaares in einer gesicherten Umgebung
- Erzeugung ihres selbstsignierten Zertifikats
- Integere und authentische Veröffentlichung:
  - ihres Zertifikats einschließlich des dazugehörigen Fingerabdrucks,
  - der von ihr ausgestellten Zertifikate,
  - von Sperrlisten der Zertifizierungsstellen,
- Einhaltung dieser Policy und
- Bereitstellung eines Sperrdienstes.

3.2 Verpflichtungen der Zertifizierungsstelle

(1) Die Zertifizierungsstelle vereinbart mit der PCA der Verwaltung einen innerhalb der gesamten PKI eindeutigen Namen und stellt sicher, dass die vereinbarten Namensbestandteile in ihrem Zuständigkeitsbereich gemäß [6] verwendet werden.

(2) Mit Vertragsabschluss verpflichtet sich die Zertifizierungsstelle zur Einhaltung und Erfüllung der in den Sicherheitsleitlinien der Wurzelzertifizierungsstelle und der in der Selbsterklärung gestellten Anforderungen.

(3) Sobald die Zertifizierungsstelle erkennt, dass sie die in den Sicherheitsleitlinien der Wurzelzertifizierungsstelle und/oder der Selbsterklärung gestellten Anforderungen nicht mehr erfüllt, ist sie verpflichtet, dies der PCA der Verwaltung unverzüglich schriftlich mitzuteilen.

(4) Erkennt die PCA der Verwaltung, dass die in den Sicherheitsleitlinien der Wurzelzertifizierungsstelle und/oder der Selbsterklärung aufgestellten Anforderungen von der Zertifizierungsstelle nicht mehr erfüllt werden, wird sie die Zertifizierungsstelle hierüber schriftlich informieren und zur Stellungnahme auffordern. Die Stellungnahme der Zertifizierungsstelle muss innerhalb von zwei Wochen nach Zugang der Aufforderung schriftlich erfolgen.

(5) Die Zertifizierungsstelle ist auf Verlangen der PCA der Verwaltung verpflichtet, Aufzeichnungen und Unterlagen, auch soweit sie in elektronischer Form vorliegen, zur Prüfung vorzulegen und auf Verlangen der PCA der Verwaltung die bei der Antragsstellung unterzeichnete Selbsterklärung zu erneuern. Liegt die er-

neuerte Selbsterklärung der PCA der Verwaltung nicht innerhalb von zwei Wochen vor, ist die PCA der Verwaltung berechtigt, das CA-Zertifikat mit sofortiger Wirkung zu sperren.

(6) Die Zertifizierungsstelle erklärt ihr Einverständnis mit der Veröffentlichung ihrer Zertifikate durch die PCA der Verwaltung.

(7) Die Weitergabe geheimer Schlüssel, PINs oder Kopien geheimer Schlüssel ist grundsätzlich verboten. Die Weitergabe von privaten Schlüsseln, deren öffentlicher Schlüssel zu einem Gruppenzertifikat gehört, ist abweichend hiervon in [7] geregelt. Die Endanwender werden von der Zertifizierungsstelle verpflichtet, alle Kopien des geheimen Schlüssel durch eine genügend lange PIN oder andere Maßnahmen des Zugriffschutz vor Zugriff Dritter zu schützen. Werden zur Speicherung von geheimen Schlüssel Web-Browser verwendet, so sind die Hinweise zum Schutz in [13] zu beachten. Beim Einsatz von Zertifikaten in Verbindung mit dem SSL-Protokoll sind die Regelungen in [13] zu beachten. Weitergehende Verpflichtungen (z.B. Einschränkungen der zulässigen Zertifikatsweitergabe) der Endanwender werden ggf. von der zuständigen Zertifizierungsstelle vorgenommen.

3.3 Verpflichtungen der Endanwender

Die Verpflichtung der Endanwender zur Einhaltung der in Abschnitt 3.2 genannten Regelungen erfolgt durch die Zertifizierungsstellen. Siehe hierzu Abschnitt 3.2.

3.4 Vertraulichkeit

Die Vertraulichkeit der der PCA vorgelegten Dokumente wird sichergestellt.

3.5 Gültigkeitsdauer

Das Zertifikat der Wurzelzertifizierungsstelle ist 5 Jahre gültig.

Zertifikate der Zertifizierungsstellen sind für maximal 4 Jahre gültig.

Endanwenderzertifikate einschließlich der Gruppenzertifikate sind für maximal 3 Jahre gültig. Hiervon abweichend sind SSL-Serverzertifikate maximal 1 Jahr gültig.

Eine Re-Zertifizierung[1] ist grundsätzlich nicht zulässig, insbesondere darf die Verwendungsdauer der Schlüssel die o.g. maximale Gültigkeitsdauer nicht überschreiten.

[1] Re-Zertifizierung bedeutet im Rahmen dieser PKI die erneute Verwendung von Schlüsselmaterial in Verbindung mit einem neuen Zertifikat.

4 Identifizierung und Authentisierung

Alle in der PKI der Verwaltung ausgestellten Zertifikate entsprechen in der Regel einer Vertrauensstufe. Diese bezieht sich auf die grundsätzliche Art der Überprüfung der Inhalte und der Identitätsfeststellung.

Für die Vertrauensstufe in der PKI der Verwaltung ist damit die Verbindlichkeit der durch die Zertifikate gemachten Aussagen bedeutsam. Der Zuordnung des Zertifikats zum Zertifikatsinhaber bzw. zum Schlüsselverantwortlichen bei Gruppenzertifikaten kommt somit entscheidende Bedeutung zu.

In der PKI der Verwaltung sind daher folgende Anforderungen für die Identifizierung der Zertifikatsinhaber bindend vorgeschrieben:

4.1 Erstmalige Registrierung

Für die erstmalige Ausstellung eines Zertifizierungsstellen-Zertifikats gelten besondere Regelungen, dargelegt in diesem Abschnitt. Bei der Ausstellung weiterer Zertifikate für bereits registrierte Zertifikatsinhaber gelten vereinfachte Verfahren, dargestellt in 4.2.

4.1.1 Identifizierung und Authentisierung einer natürlichen Person

Personen, die ein Zertifikat beantragen, werden durch persönliches Erscheinen identifiziert und anhand eines gültigen amtlichen Ausweises authentisiert. Dies gilt auch, wenn es sich um ein Zertifikat mit Pseudonym handelt.

4.1.2 Identifizierung und Authentisierung einer juristischen Person

Juristische Personen, die ein Zertifikat beantragen, werden durch persönliches Erscheinen mindestens einer sie vertretenden Person identifiziert. Diese Person muss sich, wie unter 4.1.1 dargestellt, authentisieren. Zusätzlich ist durch sie nachzuweisen:

- ihre Vertretungsvollmacht zur Beantragung eines Zertifikates für die juristische Person,
- den Nachweis der Existenz der juristischen Person durch Handelsregisterauszug oder vergleichbare Dokumente und
- die Erklärung, dass gegenwärtig kein Insolvenzverfahren gegen die juristische Person eröffnet worden ist oder dessen Eröffnung beantragt worden ist.

4.1.3 Identifizierung und Authentisierung bei Gruppenzertifikaten

Für jedes Gruppenzertifikat ist eine natürliche Person als Schlüsselverantwortlicher zu benennen. Diese Person muss gemäß Abschnitt 4.1 ein entsprechendes Zertifikat beantragen und die in 4.1.1 geforderten Identitäts- und Authentisierungsnachweise erbringen. Die Person muss die Berechtigung zur Beantragung des Gruppenschlüssels nachweisen. Der Schlüsselverantwortliche nimmt die entsprechenden Schlüssel und Zertifikate in Empfang und verpflichtet sich gegenüber der Zertifizierungsstelle zur Einhaltung der Regelungen für Gruppenzertifikate [7].

Wird die Verantwortung an einen neuen Schlüsselverantwortlichen übergeben, muss dieser ebenfalls die in 4.1.1 geforderten Nachweise erbringen und sich gegenüber der Zertifizierungsstelle zur Einhaltung der Regelungen für Gruppenzertifikate [7] verpflichten.

4.1.4 Anforderungen an die Namensvergabe

Für die PKI der Verwaltung sind die Namensregeln und -formate aus [6] verbindlich. Die konkret umgesetzten Formate für Zertifikate und Sperrlisten sind durch die technischen Grundlagen für die Wurzelzertifizierungsstelle [5] spezifiziert. Das Dokument enthält daneben auch Hinweise und Vorgaben für die Zertifizierungsstellen.

4.1.5 Eindeutigkeit des Namens von Zertifizierungsstellen

Für die Eindeutigkeit der verwendeten Namen für Zertifizierungsstellen tragen die ausstellenden Zertifizierungsstellen die Verantwortung.

4.1.6 Namensraumvergabe der PCA der Verwaltung

Der Namensraum, für den die Zertifizierungsstelle Zertifikate ausstellt, wird der Wurzelzertifizierungsstelle zur Prüfung und Freigabe vorgelegt. Nicht benutzte Namensräume werden bei der Wurzelzertifizierungsstelle abgemeldet.

4.1.7 Anforderungen an die Vergabe von Gruppenzertifikaten

Siehe hierzu die Regelungen für Gruppenzertifikate gemäß [7].

4.1.8 Methoden zum Nachweis des Besitzes des geheimen Schlüssels

Die antragstellende Zertifizierungsstelle muss der Wurzelzertifizierungsstelle nachweisen, dass sie im Besitz des geheimen Schlüssels ist, der zu ihrem öffentlichen Schlüssel korrespondiert.

Dies geschieht durch die elektronische Signatur über ihre Zertifikatsanforderung.

4.2 Regelmäßiges Wiederausstellen

Folgezertifikate müssen entweder wie bei der erstmaligen Registrierung oder als digital signierter Verlängerungsantrag beantragt werden.

4.3 Wiederausstellen nach Sperrung

Nach einer Sperrung des Zertifikats einer Zertifizierungsstelle ist wie bei einer erstmaligen Registrierung vorzugehen, d. h. es ist ein neues Zertifikat zu beantragen.

4.4 Sperrantrag

Sperren eines Zertifikates einer Zertifizierungsstelle kann mittels verschiedener Verfahren zu Übermittlung des Sperrantrages erfolgen. Die Wurzelzertifizierungsstelle nimmt Sperranträge der Zertifizierungsstellen per

- Telefon unter Nennung eines vereinbarten Passwortes,
- Telefax mit Sperrpasswort,
- Briefpost oder
- signierter E-Mail

entgegen. Vor der Sperrung erfolgt durch die Wurzelzertifizierungsstelle eine fernmündliche Rücksprache. Dazu sind der PCA der Verwaltung die Liste der Rufnummern der autorisierten Ansprechpartner zu übergeben.

Die Zertifizierungsstellen stellen sicher, dass die benutzten Passwörter nur dem autorisierten Personenkreis bekannt sind.

5 Geheimhaltungsgrad bei Verschlüsselung

Die Sicherheit der Verschlüsselung ist unter anderem von den eingesetzten Algorithmen, Zertifikaten und Produkten abhängig. Die Sicherheit der Verschlüsselung bei Gruppenzertifikaten ist unter anderem von organisatorischen und technischen Randbedingungen abhängig.

Die Vertrauensstufen der Zertifikate hinsichtlich der Verschlüsselung von Informationen sind wie folgt gegliedert:

- Persönliche Zertifikate:
  - Schutzklasse I
  - VS-Grad VS-NfD (diese Sicherheitsleitlinie ist für VS-NfD ausgelegt. Die Zulassung des zugrundeliegenden IT-Systems für VS-NfD verbleibt im Rahmen eines Zulassungsverfahrens noch zu erteilen.)
- Gruppenzertifikate:
  - Schutzklasse I
  - VS-NfD - sofern zur Verarbeitung von VS des Grades VS-NfD die Anzahl der ausgegebenen Gruppenzertifikate (für eine Gruppe, Funktion oder automatisierten IT-Prozess) auf 30 begrenzt ist und der Grundsatz "Kenntnis nur, wenn nötig" beachtet wird und sofern die Zertifizierungsstellen sicherstellen, dass die maximale Gruppengröße[2] von den Kommunikationsteilnehmern elektronisch abgefragt werden kann. Dies kann auch dadurch umgesetzt werden, dass die maximale Gruppengröße und ggf. die Eignung der Gruppenzertifikate für VS-NfD im *CommonName* des Zertifikats dokumentiert wird (die Zulassung des zugrundeliegenden IT-Systems für VS-NfD verbleibt im Rahmen eines Zulassungsverfahrens noch zu erteilen).

[2] Es wird empfohlen, bei Festlegung der maximalen Gruppengröße zukünftige Erweiterungen zu berücksichtigen.

6 Ablauforganisation

6.1 Zertifikatsantrag

Zertifizierungsstellen beantragen ihr Zertifikat bei der Wurzelzertifizierungsstelle.

Die Ausstellung eines Zertifikats für Zertifizierungsstellen ist schriftlich zu beantragen. Dem Antrag sind beizufügen:

(1) die aktuell geltenden Sicherheitsleitlinien der Zertifizierungsstelle,

(2) die Selbsterklärung der Zertifizierungsstelle,

(3) ein aktueller Handelsregisterauszug oder vergleichbare Dokumente,

(4) die Erklärung, dass gegenwärtig kein Insolvenzverfahren gegen den Antragsteller eröffnet worden ist oder dessen Eröffnung beantragt worden ist.

Auf Verlangen sind technische Dokumentationen und Betriebskonzepte vorzulegen.

Die Vorlage eines Sicherheitskonzepts ist nicht zwingend vorgeschrieben. Dessen ungeachtet ist von der beantragenden Zertifizierungsstelle ein Sicherheitskonzept zu erstellen, welches die konkrete Umsetzung des Schutzbedarfs der verarbeiteten Information in Sicherheitsmaßnahmen regelt. Die für den operativen Betrieb notwendigen Sicherheitsmaßnahmen sollten zusätzlich in einem Betriebskonzept dargelegt werden.

6.2 Ausstellung des Zertifikats

Die Wurzelzertifizierungsstelle erzeugt im Rahmen ihrer Verpflichtungen nach Vorliegen eines vollständigen und geprüften Antrags und nach erfolgter Identifizierung Zertifikate für Zertifizierungsstellen. Dazu muss ein signierter Zertifikats-Antrag (Certificate-Request) [1] der beantragenden Zertifizierungsstelle der Wurzelzertifizierungsstelle persönlich überbracht werden.

Die Wurzelzertifizierungsstelle prüft den signierten Zertifikats-Antrag mit dem vorgelegten öffentlichen Signatur-Schlüssel. Hiermit wird sichergestellt, dass der vorgelegte Signatur-Schlüssel mit den Signaturerstellungsdaten korrespondiert.

Mit dem Ausstellen des Zertifizierungsstellen-Zertifikats durch die Wurzelzertifizierungsstelle bestätigt die PCA der Verwaltung die Zuordnung des Zertifikats zu dem Antragsteller.

Die Wurzelzertifizierungsstelle behält sich vor, bei dem Wechsel des Zertifikats der Wurzelzertifizierungsstelle neue Zertifikate für die Zertifizierungsstelle auszustellen.

6.3 Akzeptanz des Zertifikats

Die Wurzelzertifizierungsstelle übergibt das Zertifikat dem Antragsteller in einer Zertifikats-Antwort (Certificate-Reply) [5].

Die Zertifizierungsstelle ist verpflichtet, das für sie ausgestellte Zertifikat nach Erhalt auf Richtigkeit der Angaben und funktionale Korrektheit zu überprüfen und die Akzeptanz der Wurzelzertifizierungsstelle schriftlich mitzuteilen. Anschließend wird das Zertifikat im X.500 Verzeichnis des IVBB veröffentlicht.

Ist die Prüfung nicht erfolgreich oder bleibt die Bestätigung innerhalb von 5 Arbeitstagen aus, so wird das Zertifikat gesperrt.

6.4 Sperrung von Zertifikaten

6.4.1 Sperrgründe

Ein Zertifizierungsstellen-Zertifikat muss aus folgenden Gründen gesperrt werden:

(1) Nach dem Wirksamwerden der Kündigung des Vertrages durch eine der Vertragsparteien wird das entsprechende Zertifikat gesperrt.
(2) Die Zertifizierungsstelle beantragt die Sperrung ihres Zertifikates. Sie kann die Sperrung jederzeit ohne Angabe von Gründen vornehmen lassen.
(3) Der geheime Signaturerstellungsschlüssel ist nicht mehr verfügbar oder kompromittiert.

Ein Zertifikat kann aus folgenden Gründen gesperrt werden:

(1) Das Zertifizierungsstellen-Zertifikat enthält Angaben, die nicht mehr korrekt sind.
(2) Erhebliche Schwächen eines verwendeten Kryptoalgorithmus samt zugehöriger Schlüssel werden bekannt.
(3) Erhebliche Schwächen der eingesetzten Hard- und Software werden bekannt.
(4) Die Zertifizierungsstelle kommt ihren vertraglichen Verpflichtungen in wesentlichen Punkten nicht nach.

6.4.2 Zeitdauer zwischen Sperrantrag und Sperrung

Die Wurzelzertifizierungsstelle sperrt bei Vorliegen eines gültigen Sperrantrags das Zertifikat einer Zertifizierungsstelle unmittelbar, jedoch spätestens am nächsten Arbeitstag der Wurzelzertifizierungsstelle.

6.4.3 Ausstellung von Sperrlisten

Die Wurzelzertifizierungsstelle stellt spätestens nach Ablauf einer Arbeitswoche turnusgemäß eine aktuelle Sperrliste aus.

Darüber hinaus wird nach der Sperrung eines Zertifikats unmittelbar eine neue Sperrliste ausgestellt.

6.4.4 Bekanntgabe von Sperrungen

Die aktuelle Sperrliste wird von der Wurzelzertifizierungsstelle unmittelbar dem Verzeichnisbetreiber übermittelt und innerhalb von 24 Stunden dort eingestellt.

Die Wurzelzertifizierungsstelle stellt keinen Online-Zertifikatsstatus für Zertifikate der Zertifizierungsstellen zur Verfügung.

Aus wichtigem Grund kann die Wurzelzertifizierungsstelle die Sperrung einer Zertifizierungsstelle im Bundesanzeiger oder in anderen Medien bekannt geben.

6.4.5 Kompromittierung des geheimen Schlüssels

Bei Kompromittierung eines geheimen Schlüssels ist das zugeordnete Zertifikat unverzüglich zu sperren. Wurde der geheime Schlüssel der Wurzelzertifizierungsstelle kompromittiert, müssen alle ausgegebenen Zertifizierungsstellen-Zertifikate und das eigene Zertifikat gesperrt werden.

Analoge Regelungen gelten im Kompromittierungsfall für alle Zertifizierungsstellen der PKI.

6.4.6 Suspendierung

Die Suspendierung von Zertifikaten ist in der gesamten PKI der Verwaltung nicht vorgesehen.

6.5 Beweissicherung und Protokollierung

Die Wurzelzertifizierungsstelle legt im Betriebskonzept [12] fest, welche Daten und Ereignisse in welchen Abständen von wem aufgezeichnet werden. Darüber hinaus wird geregelt, wie lange die Datensicherungen und Protokolldaten aufbewahrt, bzw. archiviert werden und wer darauf zugreifen kann.

6.6 Schlüsselwechselmanagement

Aufgrund der Nutzungsdauer des Wurzelzertifizierungsstellen-Schlüssels von maximal fünf Jahren ergibt sich die Notwendigkeit eines regelmäßigen Schlüsselwechsels. Dieser erfolgt grundsätzlich im jährlichen Rhythmus. Mit dem Wechsel des Schlüssels der Wurzelzertifizierungsinstanz wird der Fingerabdruck des neuen Wurzelzertifikats über einen sicheren Kanal, unter anderem im Bundesanzeiger, veröffentlicht.

Es wird somit mehrere gültige Wurzelzertifikate geben.

Bei Wechsel des Schlüssels der Zertifizierungsstelle wird ein neues Zertifizierungsstellen-Zertifikat von der Wurzelzertifizierungsstelle ausgestellt. Es kann somit mehrere gültige Zertifizierungsstellen-Zertifikate geben.

6.7 Kompromittierung und Wiederherstellung

Für Notfälle und Katastrophen ist von der Wurzelzertifizierungsstelle und den Zertifizierungsstellen ein Konzept zu erstellen und zu pflegen, welches die Wiederherstellung des ordnungsgemäßen Betriebes innerhalb einer angemessenen Frist sicherstellt. Insbesondere sind die Kompromittierung des geheimen Schlüssels, das Bekannt werden von Schwachstellen in den verwendeten kryptographischen Verfahren und die Nichtverfügbarkeit der Sperrlisten als Notfall betrachtet.

6.8 Einstellen des Betriebs

Die Absicht, den Betrieb einer Zertifizierungsstelle oder der Wurzelzertifizierungsstelle einzustellen, ist anzukündigen. Grundsätzlich gelten hierfür folgende Modalitäten:

- Die Wurzelzertifizierungsstelle kann den Betrieb mit einer Ankündigungsfrist von 12 Monaten zum Ende des Kalenderjahres einstellen.
- Die Zertifizierungsstelle kann den Betrieb mit einer Ankündigungsfrist von drei Monaten ohne Angabe von Gründen einstellen.
- Die Ankündigung muss schriftlich erfolgen und ist zu veröffentlichen.
- Das Einstellen des Betriebs wird vertraglich zwischen Wurzelzertifizierungsstelle und den von ihr zertifizierten Zertifizierungsstellen geregelt.

Mit Einstellung des Betriebes werden alle noch gültigen Zertifizierungsstelle-Zertifikate dieser gesperrt. Nach erfolgter Ankündigung werden Zertifikate für Zertifizierungsstellen nur noch mit einer Gültigkeitsdauer bis zum Zeitpunkt des Betriebsendes ausgestellt.

Bei Einstellung des Betriebs der Wurzelzertifizierungsstelle werden alle noch gültigen Wurzelzertifikate gesperrt.

7 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen für Zertifizierungsstellen

Von jeder Zertifizierungsstelle sind alle erforderlichen Sicherheitsmaßnahmen nach dem IT-Grundschutzhandbuch [10] umzusetzen und in einem Sicherheitskonzept zu dokumentieren. Die Wurzelzertifizierungsstelle setzt entsprechende Maßnahmen, welche in [8] dokumentiert sind und mindestens dem Niveau des IT-Grundschutzhandbuchs [10] entsprechen, um.

Die nachfolgenden Ausführungen beziehen sich auf den Betrieb der Wurzelzertifizierungsstelle. Analoge Regelungen sind von den jeweiligen Zertifizierungsstellen zu treffen.

7.1 Infrastrukturelle Maßnahmen

Die infrastrukturellen Maßnahmen der PCA sind im Sicherheitskonzept der Wurzelzertifizierungsstelle [8] niedergelegt.

7.2 Organisatorische Maßnahmen

Die organisatorischen Maßnahmen der PCA sind im Sicherheitskonzept der Wurzelzertifizierungsstelle [8] niedergelegt und werden im Sinne eines Rollenkonzepts durch das Betriebskonzept der Wurzelzertifizierungsstelle [11] oder auf andere Weise umgesetzt[11].

7.3 Personelle Maßnahmen

Für jede Rolle muss ein Anforderungsprofil existieren. Jeder Mitarbeiter muss nachweislich die Voraussetzungen hinsichtlich Ausbildung, Qualifikation, Erfahrung und Zuverlässigkeit erfüllen.

8 Technische Sicherheitsmaßnahmen für Zertifizierungsstellen

Alle technischen Sicherheitsmaßnahmen sind im Sicherheitskonzept darzulegen. Die Maßnahmen sollten mindestens dem Niveau des IT-Grundschutzhandbuchs [10] entsprechen. Die nachfolgenden Angaben beziehen sich jeweils auf die PCA der Verwaltung.

8.1 Schlüsselgenerierung und -installation

8.1.1 Schlüsselgenerierung

Die Wurzelzertifizierungsstelle erzeugt kryptographisch hinreichend sichere Signaturschlüssel in einem von einer allgemein anerkannten Evaluierungsstelle geprüften Hardwaremodul. Das Modul ist so konstruiert, dass unberechtigte Zugriffe und Manipulationen erkannt und weitestgehend verhindert werden. Das Schlüsselgenerierungssystem ist ausschließlich nach dem Vier-Augen-Prinzip zu bedienen.

Die Zertifizierungsstellen verpflichten sich vertraglich, die Schlüsselgenerierung nach dem aktuellen Stand der Technik sicherzustellen.

8.1.2 Übergabe der öffentlichen Schlüssel und Zertifikaten

Die öffentlichen Schlüssel der Zertifizierungsstelle werden der Wurzelzertifizierungsstelle in dem festgelegten Format [5] persönlich übergeben.

Die öffentlichen Schlüssel der Wurzelzertifizierungsstelle werden der Zertifizierungsstelle in Form selbstsignierter Zertifikate übergeben.

8.1.3 Akzeptanz von Zertifikaten

Die Zertifizierungsstelle muss neben der Authentizität des übermittelten Wurzelzertifikats dessen Integrität anhand des veröffentlichten Fingerabdrucks überprüfen.

Die Zertifizierungsstelle muss die Akzeptanz des Zertifikats nach erfolgreicher Prüfung (vgl. 6.3) bestätigen. Hierauf werden die Zertifikate in das Verzeichnis der Wurzelzertifizierungsstelle eingestellt.

8.1.4 Kryptoalgorithmen, Schlüssellänge, Parametergenerierung

Die aktuellen Empfehlungen des BSI – „Geeignete Kryptoalgorithmen gemäß §17 (2) SigV“ - sind innerhalb der PKI verbindlich.

8.1.5 Schlüsselnutzung

Der private Schlüssel der Wurzelzertifizierungsstelle wird ausschließlich zum Signieren des eigenen öffentlichen Schlüssels, der Schlüssel der Zertifizierungsstellen und der Sperrliste verwendet.

8.2 Schutz des geheimen Schlüssels

Die geheimen Signaturschlüssel der Wurzelzertifizierungsstelle werden in einem Modul nach 8.1.1 aufbewahrt. Der Zugriff wird über ein Vier-Augen-Prinzip, welches mittels zweier passwortgeschützter Smartcards realisiert ist, gesichert.

8.2.1 Schlüsselteilung

Ist seitens der Wurzelzertifizierungsstelle nicht vorgesehen.

8.2.2 Key Escrow

Ist seitens der Wurzelzertifizierungsstelle nicht vorgesehen.

8.2.3 Backup des privaten Schlüssels

Die Signaturschlüssel der Wurzelzertifizierungsstelle sind über ein Backupverfahren unter Einhaltung des Vier-Augen-Prinzips wiederherstellbar [11]. Die Schlüssel werden auf Smartcards gespeichert. Letztere sind wiederum über Sicherungsschlüssel geschützt, die auf mehrere Smartcards verteilt sind.

8.2.4 Archivierung des privaten Schlüssels

Die Archivierung des privaten Schlüssels der Wurzelzertifizierungsstelle bis zum Ablauf der Gültigkeit des Zertifikats wird, wie im Backupkonzept beschrieben, realisiert.

8.2.5 Schlüsselinstallation und Aktivierung

Nach der Generierung der Signaturschlüssel der Wurzelzertifizierungsstelle im kryptographischen Modul kann die Zertifizierungseinheit auf die Schlüssel unter Einhaltung des Vier-Augen-Prinzips zugreifen.

8.2.6 Schlüsselvernichtung

Nach Ablauf der Gültigkeit oder nach Sperrung des zugeordneten Zertifikats werden die privaten Schlüssel zuverlässig vernichtet [11].

8.3 Weitere Aspekte des Schlüsselmanagements

8.3.1 Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel der Wurzelzertifizierungsstelle müssen spätestens nach Ablauf des Gültigkeitszeitraums archiviert werden. Dies gilt auch für die von der Wurzelzertifizierungsstelle ausgestellten Zertifikate und Sperrlisten.

8.3.2 Nutzungsdauer für öffentliche und private Schlüssel

Die Nutzungsdauer des Schlüsselpaars stimmt mit der Nutzungsdauer des dazugehörigen Zertifikats überein. Eine Re-Zertifizierung von Schlüsselmaterial, das Zertifizierungsstellen gehört, ist nicht vorgesehen.

8.4 Aktivierungsdaten

Das Schlüsselgenerierungssystem ist ausschließlich unter Beachtung des Vier-Augen-Prinzips zu bedienen. Die Schlüsselgenerierung wird durch Benutzeranmeldung am Kryptomodul unter Verwendung von Token und durch Aktivierung des Generierungssystems initiiert.

9 Profile für Zertifikate und Sperrlisten (CRLs)

Die Festlegung der Profile für die Wurzel- und Zertifizierungsstellenzertifikate sind Gegenstand der Spezifikation „Technische Grundlagen, Formate und Protokolle“ [5]. In diesem Dokument werden auch Regelungen hinsichtlich der Verwendung von Zertifikatserweiterungen mitsamt den zugeordneten Kritikalitäten getroffen.

Analog regelt das Dokument [5] auch die Profile der Sperrlisten der Wurzelzertifizierungsstelle und der Zertifizierungsstellen einschließlich der Sperrlistenerweiterungen.

Alle relevanten Regelungen bezüglich der Vergabe von Namen ist im Namenskonzept [6] geregelt.

10 Änderung und Anerkennung dieser Policy (BSI)

10.1 Policy Object Identifier

Der Policy Object Identifier (Bezeichner) für diese Policy lautet: 1.3.6.1.4.1.7924.1.1

10.2 Änderungsmanagement

Der Betreiber der Wurzelzertifizierungsstelle ist verantwortlich für die Fortschreibung dieser Policy. Änderungen und entsprechende Umsetzungen unterliegen einem geregelten Verfahren.

Die Wurzelzertifizierungsstelle entscheidet, ob bei Änderungen der Policy ein neuer Policy-Identifier verwendet wird. Dies wird insbesondere dann der Fall sein, wenn die Policy erhebliche Änderungen gegenüber der vorangegangenen aufweist.

Falls andere Sicherheitsleitlinien auf gleicher Ebene im Zuge einer Über-Kreuzzertifizierung mit externen Wurzelzertifizierungsstellen anerkannt werden, wird dies explizit bekannt gegeben.

10.3 Anerkennung

Die Wurzelzertifizierungsstelle verpflichtet sich zur Anerkennung dieser Policy. Die Anerkennung dieser Policy seitens der Zertifizierungsstellen ist Vertragsbestandteil.

11 Glossar

Authentisierung
Prüfung der behaupteten Identität eines Zertifikatinhabers

Certificate Revocation List
→ Sperrliste, die Sperrinformationen über Teilnehmer-Zertifikate (und ggf. PCA / CA-Zertifikate) enthält.

E-Mail
Elektronische Nachricht, die in der Regel aus einem Mail-Body und/oder einem oder mehreren Anhängen besteht. Mail-Body und/oder Anhänge können auch fehlen.

Endanwender
Natürliche oder juristische Person, die → Teilnehmer und Inhaber eines Zertifikates der PKI ist.

Fingerabdruck
Kryptographisch sicherer Hashwert eines Datenobjekts, mit Hilfe dessen die Unverfälschtheit des Datenobjekts per Augenschein überprüft werden kann. Fingerabdrücke werden im Rahmen der PKI insbesondere für die Überprüfung von Wurzel-Zertifikaten genutzt.

Geheimer Schlüssel
Geheimer oder privater Anteil des Schlüsselpaares. Mit diesem Schlüssel können elektronische Signaturen erzeugt und die mit dem dazugehörenden → öffentlichen Schlüssel verschlüsselten Texte entschlüsselt werden.

Geheimer Signaturschlüssel
Geheimer Anteil des Schlüsselpaares zur Erstellung und Prüfung einer elektronischen Signatur. Dieser Schlüssel wird zur Erstellung der elektronischen Signatur eingesetzt. Die Signaturen können nur mit dem dazugehörenden öffentlichen Schlüssel verifiziert werden.

Gültigkeit
Die Aussage "ein → Zertifikat ist gültig" entspricht dem Gültigkeitsmodell, das in [1] beschrieben ist.

Lokale Registrierungsstelle
Stelle in einer Institution, die die organisatorische Schnittstelle zwischen → Endanwender und PKI bildet. Hauptaufgabe ist die sichere Identifizierung der Antragssteller im Rahmen der Registrierung, Zertifizierung und ggf. Sperrung.

Öffentlicher Schlüssel
Öffentlicher Anteil des Schlüsselpaares zur Verschlüsselung bzw. Prüfung

von elektronischen Signaturen. Die mit diesem Schlüssel verschlüsselten Daten können nur mit dem dazugehörenden geheimen Schlüssel entschlüsselt werden.

Öffentlicher Signatur-Schlüssel

Öffentlicher Anteil des Schlüsselpaares zur Erstellung und Prüfung einer elektronischen Signatur. Mit dem Verifikationsschlüssel können die mit dem dazugehörenden geheimen Signaturschlüssel erzeugten Signaturen verifiziert werden.

Policy

hier: Richtlinien für das Ausstellen, Sperren, Erneuern und Anwenden von Zertifikaten durch eine Zertifizierungsstelle (CA).

Public Key Infrastruktur

Auf einem asymmetrischen Schlüsselsystem basierende Infrastruktur, die die geforderten Sicherheitsdienste (Sicherstellung der Integrität, Vertraulichkeit und Authentizität) ermöglicht.

Zu einer Public Key Infrastruktur im Sinne dieses Dokumentes gehören sowohl zentrale Komponenten (z. B. CA-/RA-Komponenten) als auch dezentrale Komponenten (z. B. Plugins und Client-Komponenten).

Die Public Key Infrastruktur umfasst außerdem sowohl technische als auch organisatorische Aspekte.

Schlüsselverantwortlicher

→ Endanwender, der durch die für den Einsatz der Gruppenzertifikate verantwortlichen Stelle zu benennen ist. Diese Stelle wird hier als → "Vollmacht gebende Stelle" bezeichnet.

Signaturzertifikat

Zuordnung des → öffentlichen Signaturschlüssels zu einer Person über die Nennung des Namens im → Zertifikat. Eine vertrauenswürdige → Zertifizierungsstelle, die zuvor die Identität des Schlüsselinhabers überprüft hat, bestätigt diese Zuordnung durch ihre Signatur.

Signaturalgorithmus

Algorithmus, mit dem die Signatur erzeugt wird.

Sperrliste

Von einer → Zertifizierungsstelle signierte Liste gesperrter → Zertifikate.

SSL

Secure Socket Layer, Protokoll zur Absicherung von Internet-Verbindungen, das Zertifikate zur Authentiserung von Server und Client (optional) nutzt.

Sub-CA

untergeordnete Zertifizierungsstelle, deren Zertifikat wieder durch eine → Zertifizierungsstelle ausgestellt worden ist.

Teilnehmer

Teilnehmer sind Personen, Personengruppen, Funktionen oder Dienste (IT-Prozesse), die im Rahmen der PKI-1-Verwaltung Schlüssel und → Zertifikate erhalten oder aus dem Verzeichnisdienst PKI-Informationen von → Zertifizierungsstellen oder Teilnehmern abrufen.

Verschlüsselungszertifikat

Zuordnung des → öffentlichen Verschlüsselungsschlüssels zu einer Person über die Nennung des Namens im → Zertifikat.

Vollmacht gebende Stelle (für Gruppenzertifikate)

Die Stelle, die dem → Schlüsselverantwortlichen die Berechtigung zur Wahrnehmung seiner Funktion als Schlüsselverantwortlicher des Gruppenschlüssels erteilt.

Wurzel-Prüfmaterial

Vertrauenswürdig übermittelte Information, anhand derer die Authentizität eines Zertifikats sicher überprüft werden kann (z. B. → Fingerprint des → Wurzel-Zertifikats).

Wurzel-Zertifikat

Das Wurzel-Zertifikat beinhaltet den öffentlichen Schlüssel der → Wurzel-Zertifizierungsstelle und ist mit dem zugehörigen geheimen Schlüssel signiert (selbstsigniert).

Wurzelzertifizierungsstelle

Oberste Vertrauensinstanz einer PKI.

Zertifikat

In einem digitalen Zertifikat wird ein öffentlicher Schlüssel einer Person zugeordnet. Das Zertifikat enthält den Namen der Person, die im Besitz des dazugehörigen geheimen Schlüssels ist. In der Regel wird ein Zertifikat von einer vertrauenswürdigen → Zertifizierungsstelle, die zuvor die Identität dieser Person überprüft hat, digital signiert. Man unterscheidet → Signaturzertifikate und → Verschlüsselungszertifikate.

Zertifizierungsstelle

Stelle, die Zertifikate der PKI und → Sperrlisten (CRLs) ausstellt. Gegebenenfalls werden auch CA-Zertifikate für untergeordnete CAs (kurz: → Sub-CAs) und die entsprechenden Sperrlisten ausgestellt. Eine Zertifizierungsstelle stellt darüber hinaus in der Regel weitere Dienste zur Verfügung, wie z. B. den Registrierungs- und einen Verzeichnisdienst.

12 Literaturverzeichnis

[1] J. Biester, F. Bauspiess, D. Fox, MailTrust Version 2, Austauschformat, 16. März 1999

J. Biester F. Bauspiess, D. Fox, MailTrust Version 2, Profile für Zertifikate und Sperrlisten, 16. März 1999

[2] Beschluss der Bundesregierung zur Sicherheit im elektronischen Rechts- und Geschäftsverkehr mit der Bundesverwaltung, 16. Januar 2002

[3] T7 e.V. und TeleTrust e.V., ISIS-MTT Specification

[4] B. Ramsdell, S/MIME Version 3, Certificate Handling, Juni 1999
B. Ramsdell, S/MIME Version 3, Message Specification, Juni 1999

[5] Zertifizierungsinfrastruktur für die PKI-1-VERWALTUNG, Technische Grundlagen der Wurzelzertifizierungsstelle, Formate und Protokolle nach MTTv2 (in der aktuellen Version)

[6] Zertifizierungsinfrastruktur für die PKI-1-Verwaltung, Namensregeln und -formate (in der aktuellen Version)

[7] BSI, Regelungen für Gruppenzertifikate (in der aktuellen Version)

[8] Referenz gelöscht.

[9] Sicherheitskonzept, VERWALTUNGS-PKI (in der aktuellen Version)

[10] IT-Grundschutzhandbuch (in der aktuellen Version), Bundesanzeigerverlag

[11] PCA-1-VERWALTUNG, Betriebshandbuch Wurzelzertifizierungsstelle (in der aktuellen Version)

[12] S. Chokhani, RFC2527: Certificate Policy and Certification Practices Framework, März 1999

[13] BSI, Regelungen für die Anwendung von SSL (in der aktuellen Version)