Trustcenter der
Deutschen Rentenversicherung

Certificate Policy
für die qualifizierten Zertifikate
der
Deutschen Rentenversicherung Bund

Version 4.0

Stand 08.02.2011

Inhalt

1 Einleitung

1.1 Überblick

Die Träger der Deutschen Rentenversicherung betreiben nach § 138 SGB VI ein gemeinschaftliches Trustcenter zur Bereitstellung von Zertifizierungsdiensten nach dem deutschen Signaturgesetz (SigG). Die Deutsche Rentenversicherung Bund betreibt unter der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung einen Zertifizierungsdienst, der bei der Bundesnetzagentur nach dem SigG angezeigt ist.

Die Zertifizierungsstelle der Deutschen Rentenversicherung Bund gibt für die Mitarbeiter der Deutschen Rentenversicherung Bund Mitarbeiterchipkarten, die qualifizierte und fortgeschrittene Zertifikate enthalten, aus. Das vorliegende Dokument enthält die Zertifizierungsrichtlinie (Certificate Policy) für die qualifizierten Zertifikate gemäß SigG zum Zweck der Signaturerstellung und -prüfung. Daneben gibt es noch eine Zertifizierungsrichtlinie für fortgeschrittene Zertifikate zum Zweck der Verschlüsselung und Authentifizierung.

Der Begriff „Certificate Policy“ steht für die Gesamtheit der Regeln und Vorgaben, welche die Anwendbarkeit eines Zertifikatstyps festlegen. Die Zielsetzung einer Certificate Policy ist im RFC 3647, „Certificate Policy and Certification Practices Framework“, ausführlich dargestellt. Insbesondere sollte eine Certificate Policy darlegen,

- welche technischen und organisatorischen Anforderungen die bei der Ausstellung der Zertifikate eingesetzten Systeme und Prozesse erfüllen,
- welche Vorgaben für die Anwendung der Zertifikate sowie im Umgang mit den zugehörigen Schlüsseln und Signaturerstellungseinheiten (zum Beispiel Chipkarten) gelten,
- welche Bedeutung den Zertifikaten und ihrer Anwendung zukommt, das heißt welche Sicherheit, Beweiskraft, oder rechtliche Relevanz die mit ihnen erzeugten Kryptogramme bzw. Signaturen besitzen.

Die vorliegende Certificate Policy basiert auf dem Standard „TS 101 456 – Policy requirements for certification authorities issuing qualified certificates“ in der Version 1.2.1 des European Telecommunications Standards Institute (ETSI). Das Verhältnis der vorliegenden Certificate Policy zum genannten Standard wird in Abschnitt 2 erläutert.

1.2 Dokumentenidentifikation

Bezeichnung des Dokuments: Certificate Policy für die qualifizierten Zertifikate der Deutschen Rentenversicherung Bund, Version 4.0.

Der ASN.1 Object Identifier (OID) für dieses Dokument ist 1.3.6.1.4.1.22204.1.8.1.1.2.

Da die vorliegende Certificate Policy über den Standard hinaus gehende Regelungen enthält (siehe Abschnitt 2) wird der Object Identifier des Standards ETSI TS 101 456 nicht verwendet.

1.3 Teilnehmer und Instanzen

1.3.1 Zertifizierungsstellen

Die Deutsche Rentenversicherung Bund betreibt eine Zertifizierungsstelle für die Ausgabe von Mitarbeiterchipkarten. Die Zertifizierungsstelle der Deutschen Rentenversicherung Bund verwendet für die Erstellung der Zertifikate ein zentrales Zertifizierungssystem mit jeweils einer CA für qualifizierte und fortgeschrittene Zertifikate. Beide CAs sind von der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung zertifiziert.

Die Schlüssel, mit denen die beiden CAs der Wurzelzertifizierungsstelle (die eine für qualifizierte Zertifikate, die andere für fortgeschrittene Zertifikate) Zertifikate unterzeichnen, sind die grundlegenden „Vertrauensanker“ der Hierarchie. Über diese Schlüssel stellt jede Wurzelzertifizierungsstelle selbstsignierte Zertifikate aus.

1.3.2 Registrierungsstellen

Die Registrierung erfolgt durch die Zertifizierungsstelle der Deutschen Rentenversicherung Bund.

1.3.3 Zertifikatswerber (Subscriber)

Erwerber von Zertifikaten können Mitarbeiter der Deutschen Rentenversicherung Bund sein. Mitarbeiter in diesem Sinne sind auch externe Mitarbeiter, die für die Deutsche Rentenversicherung Bund tätig sind und für ihre Tätigkeit Mitarbeiterchipkarten und Zertifikate benötigen.

1.3.4 Zertifikatseigentümer (Subject)

Zertifikatsinhaber sind die Zertifikatswerber. Im Folgenden wird daher ausschließlich von Zertifikatsinhaber gesprochen.

1.3.5 Vertrauende Parteien

Durch die Anwendbarkeit der Zertifikate nach Kapitel 1.4 ist der Kreis der auf diese Zertifikate vertrauenden Parteien nicht eingeschränkt.

1.4 Anwendbarkeit der Zertifikate

Die von der Deutschen Rentenversicherung Bund ausgegebenen qualifizierten Zertifikate werden vom Zertifikatseigentümer im Rahmen seiner dienstlichen Tätigkeit verwendet. Außerdienstlich darf der Signaturschlüssel für die elektronische Kommunikation mit der öffentlichen Verwaltung genutzt werden. Im Einzelfall kann die Nutzung weiter eingeschränkt sein. Eine entsprechende Beschränkung ist im Zertifikat in der Extension „Restriction“ enthalten.

Der private Schlüssel der Signatur darf nur zur Erzeugung qualifizierter Signaturen verwendet werden. Für weitere Anwendungen wie Authentifizierung und Verschlüsselung wird separates Schlüsselmaterial auf die Smartcards aufgebracht (vgl. 2.1).

1.5 Verwaltung der Policy

1.5.1 Organisation für die Verwaltung dieses Dokuments

Für die Verwaltung dieses CP ist die Deutsche Rentenversicherung Bund zuständig.

1.5.2 Kontaktperson

Folgende Ansprechwege hinsichtlich des CP bestehen:

Deutsche Rentenversicherung Bund
Abteilung Organisation und IT-Services
Trustcenter der Deutschen Rentenversicherung
10704 Berlin

2 Verhältnis zu ETSI TS 101 456

Allgemein basiert die vorliegende Certificate Policy auf der in „TS 101 456 – Policy requirements for certification authorities issuing qualified certificates“ des European Telecommunications Standards Institute (ETSI) definierten „Qualified Certificate Policy for qualified certificates issued to the public, requiring use of secure signature-creation devices” (QCP public + SSCD). In diesem Abschnitt wird das Verhältnis der vorliegenden Certificate Policy zu QCP public + SSCD genau definiert.

Bemerkung: Da TS 101 456 zum Zeitpunkt der Erstellung der vorliegenden Certificate Policy nur in englischer Sprache vorliegt, wird im Anhang eine Übersetzung der relevanten Kapitel 6 und 7 von TS 101 456 gegeben.

2.1 Abweichungen von der QCP public + SSCD

Die Mitarbeiter der Deutschen Rentenversicherung Bund erhalten Mitarbeiterchipkarten mit qualifizierten Signaturzertifikaten zur Erledigung ihrer dienstlichen Aufgaben. Rechte und Pflichten sind in der Geschäftsordnung der Deutschen Rentenversicherung Bund geregelt, zu deren Beachtung die Mitarbeiter dienst- bzw. arbeitsrechtlich verpflichtet sind. Ein besonderes Vertragsverhältnis des Mitarbeiters zur Zertifizierungsstelle besteht nicht.

Unter anderem daraus ergeben sich die folgenden Abweichungen von der QCP public + SSCD.

2.1.1 Pflichten des Zertifikatswerbers (Abschnitt 6.2 TS 101 456)

Die Pflichten aus 6.2 a) sind Pflichten der Deutschen Rentenversicherung Bund.

2.1.2 Registrierung des Zertifikatseigentümers (Abschnitt 7.3.1 TS 101 456)

Den Forderungen aus 7.3.1 a), b) und f) wird im Rahmen des dienst- bzw. arbeitsrechtlichen Verhältnisses des Zertifikatswerbers zur Deutschen Rentenversicherung Bund entsprochen.

Die in 7.3.1 h) geforderten Einverständniserklärungen erfolgen, sofern sie nicht durch das dienst- bzw. arbeitsrechtliche Verhältnis obsolet sind, gemäß den Vorgaben und Forderungen des deutschen Signaturgesetzes. Insbesondere wird der Zertifikatseigentümer gemäß deutschem SigG unterrichtet und auf seine Sorgfaltspflichten im Umgang mit der qualifizierten Signatur hingewiesen.

2.1.3 Verbreitung der Nutzungsbedingungen (Abschnitt 7.3.4 TS 101 456)

Die Nutzungsbedingungen finden sich in dieser Policy sowie im Dokument „Certification Practice Statement der Zertifizierungsstelle der Deutschen Rentenversicherung Bund“.

2.1.4 Verwaltung und Betrieb der Zertifizierungsstelle (Abschnitt 7.4 TS 101 456)

Der gesamte Abschnitt 7.4 TS 101 456 kommt nicht zur Anwendung. Stattdessen gilt Folgendes:

Verwaltung und Betrieb der Zertifizierungsstelle finden auf der Grundlage eines Sicherheitskonzeptes statt, das den Anforderungen des deutschen Signaturgesetzes entspricht. Die Vorgaben des deutschen Signaturgesetzes zu Betrieb und Dokumentation werden eingehalten.

Das Personal erfüllt die Anforderungen des deutschen Signaturgesetzes.

Es werden vertrauenswürdige Systeme gemäß den Vorgaben des deutschen Signaturgesetzes und der Signaturverordnung verwendet.

2.1.5 Organisation (Abschnitt 7.5 TS 101 456)

Die Forderung 7.5 e) wird nach den Vorschriften des deutschen Signaturgesetzes eingehalten.

2.2 Über QCP public + SSCD hinausgehende Anforderungen

Die Zertifizierungsstelle der Deutschen Rentenversicherung Bund ist ein qualifizierter Zertifizierungsdiensteanbieter gemäß deutschem Signaturgesetz und hat ihre Betriebsaufnahme bei der zuständigen Behörde angezeigt.

Soweit das deutsche Signaturgesetz und die Signaturverordnung strengere Forderungen an den Betreiber der Zertifizierungsstelle als qualifiziertem Zertifizierungsdiensteanbieter stellen, werden diese strengeren Anforderungen erfüllt.

2.3 Nicht anwendbare Anforderungen aus QCP public + SSCD

2.3.1 Speicherung, Sicherung und Wiederherstellung der Schlüssel der Zertifizierungsstelle (Abschnitt 7.2.2 TS 101 456)

Die Forderungen 7.2.2 b) – d) sind nicht anwendbar, da die Schlüssel der Zertifizierungsstelle nicht aus den Geräten, in denen sie betrieben werden, exportiert werden können. Ein Backup dieser Schlüssel findet nicht statt.

2.3.2 Ausgabe sicherer Signaturerstellungseinheiten (Abschnitt 7.2.9 TS 101 456)

Die Forderung 7.2.9 c) ist nicht anwendbar.

Die Forderung 7.2.9 d) ist nicht anwendbar, da die sicheren Signaturerstellungseinheiten nicht mit Aktivierungsdaten, sondern mit Transport-PINs ausgegeben werden, die der Zertifikatsinhaber zur Vergabe eigener Aktivierungsdaten verwendet.

2.3.3 Zertifikatserneuerung, -modifizierung und Schlüsselerneuerung (Abschnitt 7.3.2 TS 101 456)

Die Forderungen 7.3.2 b) und c) sind nicht anwendbar.

2.3.4 Verbreitung von Zertifikaten (Abschnitt 7.3.5 TS 101 456)

Zertifikate werden überhaupt nicht öffentlich abrufbar gehalten (Forderung 7.3.5 b)). Forderung 7.3.5 e) wird nicht erfüllt.

2.3.5 Sperrung oder Suspendierung von Zertifikaten (Abschnitt 7.3.6 TS 101 456)

Bestätigungen zu Sperrmeldungen werden nicht eingeholt (Forderung 7.3.6 a)). Eine Suspendierung von Zertifikaten findet im Einklang mit dem SigG nicht statt.

Eine explizite Information des Zertifikatsinhabers über die erfolgreiche Sperrung findet in der Regel nicht statt (Forderung 7.3.6 e)).

Ab dem 23.01.2009 ist die Forderung 7.3.6 g) nicht mehr anwendbar. Ab diesem Zeitpunkt werden für die qualifizierte CA der Zertifizierungsstelle der Deutschen Rentenversicherung Bund keine Sperrlisten mehr herausgegeben. Die bis zum 23.01.2009 herausgegebenen Sperrlisten erfüllten die Forderung 7.3.6 g). Näheres dazu ist im Dokument „Certification Practice Statement der Zertifizierungsstelle der Deutschen Rentenversicherung“ beschrieben.

2.3.6 Aufbewahrung von Informationen zu Zertifikaten (Abschnitt 7.4.11 TS 101 456)

Die folgenden Forderungen aus Abschnitt 7.4.11 unter Registrierung i) in den ersten drei Aufzählungspunkten sind wegen § 8 Signaturverordnung in der Fassung vom 23.11.2011 nicht anwendbar:

- Typ des Dokuments (der Dokumente), das (die) der Antragsteller bei der Registrierung vorgelegt hat
- Datensatz mit eindeutigen Identifikationsnummern der Ausweisdokumente
- Speicherort von Kopien von Ausweisdokumenten

Anhang A – Teilübersetzung von ETSI TS 101 456

Die vorliegende Certificate Policy basiert auf der in dem Standard „TS 101 456 – Policy requirements for certification authorities issuing qualified certificates“ des European Telecommunications Standards Institute (ETSI) definierten QCP public + SSCD. Da dieser Standard zum Zeitpunkt der Erstellung der vorliegenden Certificate Policy nur in englischer Sprache vorliegt, wird in diesem Anhang eine Übersetzung der relevanten Kapitel 6 und 7 von TS 101 456 gegeben.

Hinweis: Die Zertifizierungsstelle hat sich um eine getreue Übersetzung bemüht. So wurden zum Beispiel (nach Meinung der Zertifizierungsstelle) fehlerhafte Verweise des Originals nicht korrigiert (Verweise auf nicht übersetzte Kapitel wurden dagegen mit dem Zusatz „von TS 101 456“ versehen). Es handelt sich jedoch nicht um eine von ETSI oder im rechtlichen Sinne anerkannte Übersetzung. Im Zweifel sind daher die Anforderungen der Übersetzung ausschlaggebend.

6 Pflichten und Haftung

Hinweis: Soweit nicht anders angegeben, ist dieser Absatz für beide in Absatz 5 von ETSI TS 101 456 identifizierten Certificate Policies – QCP public und QCP public + SSCD - anwendbar.

6.1 Pflichten der Zertifizierungsstelle

Die Zertifizierungsstelle muss sicherstellen, dass alle in Abschnitt 7 definierten Anforderungen an die Zertifizierungsstelle, soweit sie für die gewählte Qualified Certificate Policy anwendbar sind, umgesetzt werden.

Die Zertifizierungsstelle hat die Verantwortung für die Konformität ihrer Zertifizierungsdienste mit den in dieser Policy definierten Prozeduren, auch wenn die Funktionen durch Unterauftragnehmer realisiert werden.

Die Zertifizierungsstelle muss ihre Zertifizierungsdienste konform zu ihrem Certification Practice Statement (CPS) betreiben.

6.2 Pflichten des Zertifikatswerbers

Dem Zertifikatswerber müssen von der Zertifizierungsstelle im Rahmen der Vereinbarung (siehe Absatz 7.3.1 h)) die folgenden Pflichten auferlegt werden:

a) Korrekte und vollständige Daten werden von ihm an die Zertifizierungsstelle übermittelt, entsprechend den Anforderungen dieser Policy, insbesondere hinsichtlich der Registrierung.

b) Das Schlüsselpaar wird nur für elektronische Signaturen und unter Berücksichtigung aller anderen Einschränkungen verwendet, die dem Zertifikatswerber bekannt gegeben wurden (siehe Absatz 7.3.4).

c) Es wird mit angemessener Sorgfalt vorgegangen, um die nicht autorisierte Verwendung des privaten Schlüssels des Zertifikatseigentümers zu verhindern.

d) Wenn der Zertifikatswerber oder -eigentümer den Schlüssel des Zertifikatseigentümers generiert, gilt Folgendes:

   - Die Schlüssel des Zertifikatseigentümers werden mithilfe eines Algorithmus erzeugt, der für sichere elektronische Signaturen als geeignet anerkannt wird.
   - Länge und Algorithmus des Schlüssels werden für sichere elektronische Signaturen als geeignet anerkannt.

Hinweis 1: Derzeit wird vorgeschlagen, dass die Anerkennung der Algorithmen mit entsprechenden Schlüssellängen, die für sichere elektronische Signaturen geeignet sind, durch ein Gremium kryptographischer Gutachter unter dem in Artikel 9 der europäischen Signaturrichtlinie genannten Komitee erfolgt.

- Nach Bereitstellung an den Zertifikatseigentümer ist nur der Zertifikatseigentümer im Besitz des privaten Schlüssels.

e) Falls die Certificate Policy die Verwendung einer sicheren Signaturerstellungseinheit fordert (zum Beispiel QCP public + SSCD), wird das Zertifikat nur für elektronische Signaturen verwendet, die mit einem solchen Gerät erstellt wurden.

Hinweis 2: Der obige Punkt ist NICHT anwendbar für die Qualified Certificate Policy: QCP public.

f) Falls das Zertifikat unter der Certificate Policy QCP public + SSCD ausgestellt wird und die Schlüssel des Zertifikatseigentümers unter der Kontrolle des Zertifikatswerbers erzeugt werden, so werden die Schlüssel des Zertifikatseigentümers in der sicheren Signaturerstellungseinheit erzeugt, das zum Signieren verwendet wird.

Hinweis 3: Der obige Punkt ist NICHT anwendbar für die Qualified Certificate Policy: QCP public.

g) Er benachrichtigt die Zertifizierungsstelle möglichst umgehend, wenn vor Ende des im Zertifikat angegebenen Gültigkeitszeitraums eine der folgenden Situationen eintritt:

- Der private Schlüssel ist verloren gegangen, wurde gestohlen oder möglicherweise kompromittiert.
- Die Kontrolle über den privaten Schlüssel des Zertifikatseigentümers ging aufgrund der Kompromittierung von Aktivierungsdaten (beispielsweise des PIN-Codes) oder aus anderen Gründen verloren.
- Im Zertifikat enthaltene Daten sind nicht korrekt oder haben sich geändert.

h) Nach einer Kompromittierung wird die Nutzung des privaten Schlüssels sofort und dauerhaft eingestellt.

6.3 Informationen für vertrauende Parteien

Die allgemeinen Nutzungsbedingungen, die vertrauenden Parteien zugänglich gemacht werden (siehe 7.3.4), müssen einen Hinweis enthalten, dass einem Zertifikat nur dann zu vertrauen ist, wenn

a) seine Gültigkeit sowie eine potenzielle Suspendierung oder Sperrung durch aktuelle Informationen zum Sperrstatus geprüft wurde (siehe Absatz 7.3.4),

Hinweis 1: Abhängig von den Praktiken der Zertifizierungsstelle und den Mechanismen, mit denen Informationen über den Sperrstatus bereitgestellt werden, kann es Verzögerungen von bis zu einem Tag bis zur Verbreitung der Informationen zum Sperrstatus geben.

b) die im Zertifikat oder den Nutzungsbedingungen (entsprechend Absatz 7.3.4) angegebenen Nutzungsbeschränkungen beachtet wurden und

c) alle weiteren in Vereinbarungen oder an anderer Stelle angegebenen Vorsichtsmaßnahmen getroffen wurden.

Hinweis 2: Die in Artikel 6 der europäischen Signaturrichtlinie definierte Haftung der Zertifizierungsstellen, die qualifizierte Zertifikate für die Öffentlichkeit ausstellen, gilt für eine Partei, die „vernünftigerweise auf das Zertifikat vertraut“.

6.4 Haftung

Zertifizierungsstellen, die qualifizierte Zertifikate für die Öffentlichkeit ausstellen, sind gemäß Artikel 6 der europäischen Signaturrichtlinie haftbar.

7 Anforderungen an die Praktiken der Zertifizierungsstelle

Hinweis 1: Soweit nicht anders angegeben, ist dieser Absatz für beide Certificate Policies - QCP public und QCP public + SSCD - anwendbar.

Die Zertifizierungsstelle muss die folgenden Anforderungen durch geeignete Maßnahmen erfüllen.

Hinweis 2: Nach jedem Absatz wird ein Verweis auf die Artikel der europäischen Signaturrichtlinie, auf dem die entsprechende Anforderung basiert, angegeben.

Das vorliegende Dokument beschäftigt sich mit Zertifizierungsstellen, die qualifizierte Zertifikate ausstellen. Dies beinhaltet die Vorgaben für die funktionalen Teilbereiche Registrierung, Zertifikatserstellung, Verbreitung von Zertifikaten, Sperrmanagement und Bereitstellung von Statusinformationen. Dort, wo sich Anforderungen auf einen der genannten Teilbereiche beziehen, ist dieser jeweils direkt unter der entsprechenden Überschrift angegeben. Dort, wo kein Teilbereich oder „Allgemeine Anforderungen“ angegeben ist, gelten die Anforderungen für den gesamten Betrieb der Zertifizierungsstelle.

Diese Policy-Anforderungen implizieren keine Beschränkungen hinsichtlich der Rechnungsstellung für Zertifizierungsstellendienste.

Die Anforderungen sind als Sicherheitsziele formuliert, die – falls dies für das Vertrauen in die Erfüllung dieser Ziele erforderlich ist – von spezifischeren Anforderungen an die Maßnahmen zur Umsetzung dieser Ziele gefolgt werden. Jede Maßnahmenforderung wird durch einen Verweis auf die relevante Anforderung in der Signaturrichtlinie ergänzt.

Hinweis 3: Die genauen Maßnahmen, die zum Erreichen eines Zieles erforderlich sind, bilden ein Gleichgewicht aus dem Erreichen des erforderlichen Vertrauens und dem Minimieren der Einschränkungen der Techniken, die die Zertifizierungsstelle bei der Ausgabe von qualifizierten Zertifikaten anwenden darf. In Absatz 7.4 (Verwaltung und Betrieb der Zertifizierungsstelle) wird auf andere, allgemeinere Standards verwiesen, die als Quelle für detailliertere Maßnahmenanforderungen dienen können. Aufgrund dieser Faktoren kann sich die Genauigkeit dieser Anforderungen in den einzelnen Themen unterscheiden.

7.1 Certification Practice Statement

Die Zertifizierungsstelle muss sicherstellen, dass sie die für die Bereitstellung der Zertifizierungsdienste erforderliche Zuverlässigkeit (siehe Anhang II (a) der Signaturrichtlinie) nachweist.

Insbesondere gilt:

a) Die Zertifizierungsstelle muss die Praktiken und Prozeduren, mit denen sie die Anforderungen der Qualified Certificate Policy umsetzt, in einem Certification Practice Statement (CPS) darlegen.

Hinweis 1: Diese Vereinbarung stellt keine Anforderungen an die Struktur des Certification Practice Statement.

b) Das CPS der Zertifizierungsstelle muss die Pflichten aller externen Organisationen, die sie bei der Erbringung des Zertifizierungsdienstes unterstützen, inklusive der anwendbaren Richtlinien und Praktiken darlegen.

c) Die Zertifizierungsstelle muss Zertifikatswerbern und vertrauenden Parteien ihr CPS sowie weitere relevante Dokumentation, die zur Bewertung der Einhaltung der Qualified Certificate Policy notwendig ist, zugänglich machen.

Hinweis 2: Die Zertifizierungsstelle ist im Allgemeinen nicht verpflichtet, alle Details ihrer Praktiken öffentlich zu machen.

d) Die Zertifizierungsstelle muss allen Zertifikatswerbern und potenziellen vertrauenden Parteien die Geschäftsbedingungen bezüglich der Nutzung des Zertifikats (siehe Absatz 7.3.4) zugänglich machen.

e) Die Zertifizierungsstelle muss eine Stelle des oberen Managements, die die letzte Autorität zur Freigabe und Genehmigung des CPS besitzt, benennen.

f) Das gehobene Management der Zertifizierungsstelle hat die Verantwortung dafür, dass die im CPS dargelegten Praktiken korrekt umgesetzt werden.

g) Die Zertifizierungsstelle muss einen Prozess zur regelmäßigen Überprüfung der in dem CPS dargelegten Zertifizierungspraktiken (einschließlich der Verantwortlichkeiten zur Pflege des CPS) definieren.

h) Die Zertifizierungsstelle muss geplante Änderungen an den im CPS dargelegten Praktiken ohne Verzögerung bekannt geben und das geänderte CPS nach der Freigabe gemäß (e) (s. oben) wie in (c) gefordert unverzüglich zugänglich machen.

7.2 Public Key-Infrastruktur – Handhabung der Schlüssel

7.2.1 Generierung der Schlüssel der Zertifizierungsstelle

Zertifikatserstellung

Die Zertifizierungsstelle muss sicherstellen, dass ihre Schlüssel unter kontrollierten Umständen generiert werden (siehe Anhang II (g) und (f) der Signaturrichtlinie).

Insbesondere gilt:

a) Die Schlüssel der Zertifizierungsstelle müssen in einer physikalisch gesicherten Umgebung (siehe Absatz 7.4.4), durch Personal in vertrauenswürdigen Rollen (siehe Absatz 7.4.3) und unter Einhaltung des Vier-Augen-Prinzips generiert werden. Die Zahl der Personen, die hierzu autorisiert sind, muss so gering wie möglich gehalten werden und den Praktiken der Zertifizierungsstelle entsprechen.

b) Der Schlüssel der Zertifizierungsstelle wird in einem Gerät durchgeführt, das eine der folgenden Anforderungen erfüllt:

- Es erfüllt die Anforderungen von FIPS PUB 140-1 [2] Level 3 oder höher. -ODER-
- Es erfüllt die Anforderungen von CEN Workshop Agreement 14167-2 [4]. -ODER-
- Es ist ein vertrauenswürdiges System, das nach ISO/IEC 15408 [3] mit mindestens EAL 4 oder nach gleichwertigen Sicherheitskriterien geprüft wurde. Diese Prüfung muss nach Sicherheitsvorgaben oder einem Schutzprofil erfolgen, die die Anforderungen des vorliegenden Dokumentes erfüllen.

Hinweis 1: Die Bestimmungen in Absatz 7.2.2 (b) bis d)) gelten auch dann für die Schlüsselerzeugung, wenn diese auf einem anderen System erfolgt.

c) Die Schlüssel der Zertifizierungsstelle müssen mit einem Algorithmus generiert werden, der als für qualifizierte Zertifikate geeignet angesehen wird.

d) Die gewählte Länge der Schlüssel der Zertifizierungsstelle muss für die von der Zertifizierungsstelle ausgegebenen qualifizierten Zertifikate als geeignet angesehen werden.

Hinweis 2: Derzeit wird vorgeschlagen, dass die Anerkennung der Algorithmen mit entsprechenden Schlüssellängen, die für sichere elektronische Signaturen geeignet sind, durch ein Gremium kryptographischer Gutachter unter dem in Artikel 9 der europäischen Signaturrichtlinie genannten Komitee erfolgt.

7.2.2 Speicherung, Sicherung und Wiederherstellung der Schlüssel der Zertifizierungsstelle

Zertifikatserstellung

Die Zertifizierungsstelle muss sicherstellen, dass die Vertraulichkeit und Integrität ihrer privaten Schlüssel gewahrt bleibt (siehe Anhang II (g) und (f) der Signaturrichtlinie).

Insbesondere gilt:

a) Der private Signaturschlüssel der Zertifizierungsstelle muss in einem sicheren kryptografischen Gerät aufbewahrt und verwendet werden, das eine der folgenden Anforderungen erfüllt:

   - Es erfüllt die Anforderungen von FIPS PUB 140-1 [2] Level 3 oder höher. -ODER-
   - Es erfüllt die Anforderungen von CEN Workshop Agreement 14167-2 [4]. -ODER-
   - Es ist ein vertrauenswürdiges System, das nach ISO/IEC 15408 [3] mit mindestens EAL 4 oder nach gleichwertigen Sicherheitskriterien geprüft wurde. Diese Prüfung muss nach Sicherheitsvorgaben oder einem Schutzprofil erfolgen, die die Anforderungen des vorliegenden Dokumentes erfüllen, auf einer Risikoanalyse basiert und physikalische sowie andere nicht-technische Maßnahmen umfasst.

b) Außerhalb der Signaturerstellungseinheit (siehe a) oben) muss der private Signaturschlüssel der Zertifizierungsstelle mit einem Algorithmus und einer Schlüssellänge verschlüsselt werden, die nach gegenwärtigem Wissensstand Angriffen durch Kryptoanalyse bis nach Ablauf der Lebensdauer des verschlüsselten Schlüssels oder Schlüsselteils standhalten können.

c) Die Sicherung, Speicherung und Wiederherstellung des privaten Signaturschlüssels der Zertifizierungsstelle darf nur von Personal in vertrauenswürdigen Rollen unter Anwendung des Vier-Augen-Prinzips und in einer physikalisch gesicherten Umgebung (siehe Absatz 7.4.4) durchgeführt werden. Die Zahl der Personen, die hierzu autorisiert sind, muss so gering wie möglich gehalten werden und den Praktiken der Zertifizierungsstelle entsprechen.

d) Die Sicherungskopien der privaten Signaturschlüssel müssen denselben oder strengeren Sicherheitsmaßnahmen wie die derzeit verwendeten Schlüssel unterliegen.

e) Falls die Schlüssel in einem speziellen Hardwaremodul gespeichert und angewendet werden, muss durch Zugriffskontrollen sichergestellt sein, dass von außerhalb des Moduls nicht auf die Schlüssel zugegriffen werden kann.

7.2.3 Veröffentlichung der Schlüssel der Zertifizierungsstelle

Zertifikatserstellung und Zertifikatsverteilung

Die Zertifizierungsstelle muss sicherstellen, dass die Integrität und Authentizität des (öffentlichen) Signaturprüfungsschlüssels der Zertifizierungsstelle sowie der zugehörigen Parameter während der Verteilung an vertrauende Parteien gewährleistet bleiben (siehe Anhang II (g) und (f) der Signaturrichtlinie).

Insbesondere gilt:

a) Die (öffentlichen) Signaturprüfungsschlüssel der Zertifizierungsstelle werden vertrauenden Parteien in einer Art zugänglich gemacht, die ihre Integrität und die Authentizität ihrer Herkunft sicherstellt.

Hinweis: Öffentliche Schlüssel von Zertifizierungsstellen können beispielsweise in Zertifikaten, die sich selbst signieren, zusammen mit einer Erklärung verteilt werden, die besagt, dass der Schlüssel die Zertifizierungsstelle authentifiziert. Alternativ können die öffentlichen Schlüssel von einer anderen Zertifizierungsstelle ausgestellt werden. Sich selbst signierenden Zertifikaten kann ihre Herkunft von der Zertifizierungsstelle nicht eindeutig nachgewiesen werden. Um die Korrektheit solcher Zertifikate definitiv nachzuweisen, sind zusätzliche Maßnahmen, wie das Vergleichen des Fingerabdrucks des entsprechenden Zertifikats mit einer vertrauenswürdigen Quelle, erforderlich.

7.2.4 Treuhänderische Schlüsselhinterlegung

Die privaten Signaturschlüssel der Zertifizierungsstelle und der Zertifikatseigentümer dürfen nicht in einer Weise aufbewahrt werden, die eine Backup-Entschlüsselungsfunktion bietet, die es autorisierten Stellen unter bestimmten Bedingungen ermöglicht, mit Informationen, die eine oder mehrere Parteien bereitstellen, Daten zu entschlüsseln (im Allgemeinen als „treuhänderische Schlüsselhinterlegung“ bezeichnet) (siehe Anhang II (j) der Signaturrichtlinie).

7.2.5 Nutzung der Schlüssel der Zertifizierungsstelle

Die Zertifizierungsstelle muss sicherstellen, dass die privaten Signaturschlüssel der Zertifizierungsstelle nicht unangemessen verwendet werden.

Insbesondere gilt:

Zertifikatserstellung

a) Die zum Erstellen von Zertifikaten verwendeten Signaturschlüssel der Zertifizierungsstelle (siehe Absatz 7.3.3) bzw. die Zertifikate, die zur Ausgabe von Informationen zum Sperrstatus verwendet werden, dürfen zu keinem anderen Zweck verwendet werden.

b) Die Signaturschlüssel für Zertifikate dürfen nur in physikalisch sicheren Umgebungen verwendet werden.

7.2.6 Deaktivierung der Schlüssel der Zertifizierungsstelle

Die Zertifizierungsstelle muss sicherstellen, dass die privaten Signaturschlüssel der Zertifizierungsstelle nicht über das Ende ihrer Lebensdauer hinaus benutzt werden (siehe Anhang II (g) und (f) der Signaturrichtlinie).

Insbesondere gilt:

Zertifikatserstellung

a) Alle Kopien der privaten Signaturschlüssel der Zertifizierungsstelle müssen nach Ablauf ihrer Lebensdauer

   - so gelöscht werden, dass die privaten Schlüssel nicht wieder hergestellt werden können, oder
   - so verwahrt werden, dass eine erneute Verwendung ausgeschlossen wird.

7.2.7 Handhabung der kryptografischen Geräte

Die Zertifizierungsstelle hat die Sicherheit der kryptografischen Geräte während ihrer gesamten Lebensdauer sicherzustellen (siehe Anhang II (f) der Signaturrichtlinie).

Zertifikatserstellung

Insbesondere muss die Zertifizierungsstelle Folgendes sicherstellen:

a) Die zur Signierung von Zertifikaten verwendete kryptografische Hardware wurde während ihrer Lieferung nicht manipuliert.

b) Die zur Signierung von Zertifikaten oder Statusinformationen verwendete kryptografische Hardware wurde während der Lagerung nicht manipuliert.

c) Die Installation, Aktivierung, Sicherung und Wiederherstellung der privaten Signaturschlüssel der Zertifizierungsstelle in kryptografischer Hardware kann nur unter der gleichzeitigen Aufsicht von mindestens 2 vertrauenswürdigen Mitarbeitern durchgeführt werden.

d) Die zur Signierung von Zertifikaten oder Statusinformationen verwendete kryptografische Hardware funktioniert fehlerfrei.

e) Die privaten Signaturschlüssel, die auf der kryptografischen Hardware der Zertifizierungsstelle gespeichert sind, werden bei der Stilllegung des Gerätes gelöscht.

7.2.8 Verwaltung von Schlüsseln der Zertifikatseigentümer

Die Zertifizierungsstelle hat sicherzustellen, dass alle von ihr generierten Schlüssel der Zertifikatseigentümer in sicherer Weise erzeugt werden, und dass die Geheimhaltung der privaten Schlüssel gewährleistet ist (siehe Anhang II (f) und (j) der Signaturrichtlinie).

Zertifikatserstellung

Falls die Zertifizierungsstelle die Schlüssel der Zertifikatseigentümer generiert:

a) Die von der Zertifizierungsstelle generierten Schlüssel der Zertifikatseigentümer müssen mit einem Algorithmus erzeugt werden, der als für qualifizierte elektronische Signaturen geeignet angesehen wird.

b) Die Länge der von der Zertifizierungsstelle generierten Schlüssel der Zertifikatseigentümer und der Public Key-Algorithmus, mit dem sie eingesetzt werden können, müssen als für qualifizierte elektronische Signaturen geeignet angesehen werden.

Hinweis: Derzeit wird vorgeschlagen, dass die Anerkennung der Algorithmen mit entsprechenden Schlüssellängen, die für sichere elektronische Signaturen geeignet sind, durch ein Gremium kryptographischer Gutachter unter dem in Artikel 9 der europäischen Signaturrichtlinie genannten Komitee erfolgt.

c) Die von der Zertifizierungsstelle generierten Schlüssel der Zertifikatseigentümer werden vor ihrer Auslieferung an den Zertifikatswerber oder Zertifikatseigentümer auf sichere Weise generiert und gespeichert.

d) Die Schlüssel der Zertifikatseigentümer müssen auf eine Weise an den Zertifikatseigentümer ausgeliefert werden, so dass die Geheimhaltung der Schlüssel nicht kompromittiert wird und nach der Auslieferung nur der Zertifikatseigentümer Zugriff auf seinen privaten Schlüssel hat.

7.2.9 Ausgabe sicherer Signaturerstellungseinheiten

Hinweis 1: Dieser Absatz ist NICHT anwendbar für die Qualified Certificate Policy: QCP public.

Die Zertifizierungsstelle hat sicherzustellen, dass, sofern sie sichere Signaturerstellungseinheiten an die Zertifikatseigentümer ausgibt, die Ausgabe in sicherer Weise erfolgt (siehe Anhang III der Signaturrichtlinie).

Bereitstellung von Geräten für Zertifikatseigentümer

Gibt die Zertifizierungsstelle sichere Signaturerstellungseinheiten aus, gilt Folgendes:

a) Die Bereitstellung von Signaturerstellungseinheiten wird vom Dienstanbieter auf sichere Weise kontrolliert.

b) Die sicheren Signaturerstellungseinheiten werden auf sichere Weise gelagert und ausgeliefert.

c) Die Deaktivierung und Reaktivierung von Signaturerstellungseinheiten wird auf sichere Weise kontrolliert.

d) Wenn das sichere Benutzergerät mit Aktivierungsdaten (zum Beispiel einer PIN) versehen ist, müssen diese Aktivierungsdaten sicher erzeugt und getrennt vom Signaturerstellungsgerät ausgeliefert werden.

Hinweis 2: Die Trennung kann durch eine zeitlich versetzte Auslieferung oder eine Auslieferung über verschiedene Wege erreicht werden.

Hinweis 3: Die oben aufgeführten Anforderungen an die Bereitstellung von sicheren Signaturerstellungseinheiten können zum Beispiel durch die Verwendung eines geeigneten Schutzprofils, das in Übereinstimmung mit ISO/IEC 15408 definiert wurde, oder gleichwertigen Kriterien erfüllt werden.

7.3 Public Key-Infrastruktur – Lebenszyklus des Zertifikatsmanagements

7.3.1 Registrierung des Zertifikatseigentümers

Die Zertifizierungsstelle hat sicherzustellen, dass die Zertifikatseigentümer korrekt identifiziert und authentifiziert werden; und dass Zertifizierungsanträge vollständig, akkurat und ordnungsgemäß autorisiert sind (siehe Anhang II (d) der Signaturrichtlinie).

Insbesondere gilt:

Registrierung

Hinweis 1: Bei der Registrierung wird der Zertifikatseigentümer als Person mit spezifischen Attributen identifiziert. Diese Attribute können zum Beispiel eine Zuordnung zu einer Rolle innerhalb einer Organisation anzeigen.

a) Bevor die Zertifizierungsstelle in ein Vertragsverhältnis mit einem Zertifikatswerber eintritt, muss sie den Zertifikatswerber über die Geschäftsbedingungen bzgl. der Nutzung der Zertifikate wie in Absatz 7.3.4 angegeben informieren (siehe Anhang II (k) der Signaturrichtlinie).

b) Die Zertifizierungsstelle muss diese Informationen über ein dauerhaftes (das heißt in der Zeit beständiges) Kommunikationsmittel zur Verfügung stellen, dessen elektronische Übertragung zulässig ist und das in normal verständlicher Sprache geschrieben sein muss.

Hinweis 2: Eine Vorlage für eine Erklärung zur Public Key-Infrastruktur (PKI Disclosure Statement), welche als Grundlage einer solchen Mitteilung verwendet werden kann, wird in Anhang B von ETSI TS 102 042 bereitgestellt.

c) Der Dienstanbieter muss die Identität und, falls anwendbar, jegliche spezifische Attribute der Person, für die das Zertifikat ausgestellt wird, in geeigneter Weise und konform zu nationalem Recht verifizieren. Nachweise der Identität müssen entweder gegen die natürliche Person direkt oder indirekt in einer Weise, die gleichwertige Gewissheit zur körperlichen Anwesenheit bietet (siehe Hinweis 3), geprüft werden. Nachweise können entweder auf Papier oder elektronisch eingereicht werden.

Hinweis 3: Ein Beispiel für einen indirekten Nachweis einer natürlichen Person ist eine zur Registrierung vorgelegte Dokumentation, die im Rahmen einer Antragstellung erlangt wurde, die eine physikalische Anwesenheit erforderte.

Hinweis 4: Attributzertifikate sind außerhalb des Gültigkeitsbereiches des vorliegenden Dokumentes, da sie keinen öffentlichen Schlüssel enthalten

d) Falls der Zertifikatseigentümer eine natürliche Person ist, sind folgende Nachweise zu erbringen:

- vollständiger Name (einschließlich Nachname und aller Vornamen)
- Geburtstag und -ort, national anerkannte Identitätsnummer oder andere Merkmale, die – soweit möglich – dazu genutzt werden könnten, diese Person von einer anderen Person gleichen Namens zu unterscheiden.

Hinweis 5: Es wird empfohlen, die Ortsangabe gemäß der landesüblichen Konventionen für Geburtsregister zu machen.

Hinweis 6: Die Zertifizierungsstelle ist bezüglich der Genauigkeit „alle[r] Informationen in dem qualifizierten Zertifikat“ haftbar (siehe Artikel 6 der Signaturrichtlinie).

e) Falls der Zertifikatseigentümer eine Person ist, die in Verbindung mit einer juristischen Person oder einer anderen Organisation identifiziert wird, müssen folgende Nachweise erbracht werden:

- vollständiger Name (einschließlich Nachname und aller Vornamen) des Zertifikatseigentümers
- Geburtstag und -ort, Verweis auf ein national anerkanntes Ausweisdokument oder andere Merkmale des Zertifikatseigentümers, die – soweit möglich – dazu genutzt werden könnten, diese Person von einer anderen Person gleichen Namens zu unterscheiden.
- vollständiger Name und juristischer Status der verknüpften juristischen Person oder Organisation
- jegliche relevanten, existierenden Registrierungsinformationen (zum Beispiel Einträge des Handelsregisters) der verknüpften juristischen Person oder Organisation
- Nachweis, dass der Zertifikatseigentümer mit der angegebenen juristischen Person oder Organisation verknüpft ist.

f) Der Zertifikatswerber muss eine physikalische Adresse oder sonstige Merkmale hinterlassen, die angeben, wie er kontaktiert werden kann.

g) Die Zertifizierungsstelle muss alle zur Prüfung der Identität des Zertifikatseigentümers verwendeten Informationen, inklusive jeglicher Referenzen auf die zur Prüfung verwendeten Dokumente sowie zu jeglichen Beschränkungen ihrer Gültigkeit aufbewahren.

h) Die Zertifizierungsstelle bewahrt das unterschriebene Einverständnis des Zertifikatswerbers auf. Dies umfasst:

- Einverständnis zu den Pflichten des Zertifikatswerbers (siehe Absatz 6.2)

- Einverständnis zur Nutzung einer sicheren Signaturerstellungseinheit (falls von der Zertifizierungsstelle gefordert)

Hinweis 7: Der obige Punkt ist NICHT anwendbar für die Qualified Certificate Policy: QCP public

- Einverständnis dazu, dass die Zertifizierungsstelle die Informationen, die sie bei der Registrierung (siehe Absatz 7.4.11 h), i) j)), der Bereitstellung von Signaturerstellungseinheiten (siehe Absatz 7.4.11 m) und n)) oder einer späteren Sperrung erfasst (siehe Absatz 7.4.11 o)), aufbewahrt und im Fall einer Einstellung ihrer Dienste unter den Bedingungen dieser Policy an dritte Parteien weitergibt.
- Ob und unter welchen Bedingungen der Zertifikatswerber eine Veröffentlichung des Zertifikats verlangt und der Zertifikatseigentümer dieser zustimmt.
- Bestätigung, dass die im Zertifikat enthaltenen Informationen korrekt sind.

Hinweis 8: Der Zertifikatswerber kann unterschiedlichen Aspekten dieser Vereinbarung zu unterschiedlichen Zeitpunkten der Registrierung zustimmen. Beispielsweise kann die Bestätigung, dass die Informationen im Zertifikat korrekt sind, im Anschluss an andere Aspekte der Vereinbarung erfolgen.

Hinweis 9: Andere Parteien (zum Beispiel die zugeordnete juristische Person) können in die Erstellung des Einverständnisses involviert sein.

Hinweis 10: Diese Vereinbarung kann in elektronischer Form vorliegen.

i) Die oben genannten Unterlagen müssen für einen dem Zertifikatswerber angegebenen (siehe a) und b) oben) und für den Bedarf als Nachweis der Zertifizierung in Gerichtsprozessen notwendigen Zeitraum aufbewahrt werden.

j) Wird der Schlüssel der Zertifikatseigentümers nicht von der Zertifizierungsstelle generiert, muss der Prozess der Zertifikatsanfrage sicherstellen, dass der Zertifikatseigentümer im Besitz des privaten Schlüssels ist, der mit dem öffentlichen Schlüssel verknüpft ist, der zur Zertifizierung vorgelegt wird.

Hinweis 11: Um Gewissheit darüber zu erhalten, dass der private Schlüssel tatsächlich in einer sicheren Signaturerstellungseinheit befindet, kann die Zertifizierungsstelle durch den Prozess für die Beantragung eines Zertifikates auch sicherstellen, dass das Schlüsselpaar tatsächlich in der sicheren Signaturerstellungseinheit erzeugt wurde.

k) Die Zertifizierungsstelle muss sicherstellen, dass die geltenden nationalen Gesetze zum Datenschutz (einschließlich der Verwendung von Pseudonymen) während der Registrierung eingehalten werden.

7.3.2 Zertifikatserneuerung, -modifizierung und Schlüsselerneuerung

Die Zertifizierungsstelle muss sicherstellen, dass die Zertifizierungsanfragen für einen Zertifikatseigentümer, der bereits zuvor registriert war, vollständig, akkurat und entsprechend autorisiert sind. Dies gilt auch für Zertifikatserneuerungen, Schlüsselerneuerungen nach Sperrung oder vor Ablauf, und Modifizierung aufgrund von Änderungen an den Attributen des Zertifikatseigentümers (siehe Anhang II (g) der Signaturrichtlinie).

Hinweis: Der Zertifikatswerber kann, sofern die Zertifizierungsstelle diesen Dienst anbietet, die Erneuerung eines Zertifikats anfordern, wenn sich relevante Attribute im Zertifikat geändert haben oder wenn das Zertifikat in Kürze abläuft.

Insbesondere gilt:

Registrierung

a) Die Zertifizierungsstelle muss sicherstellen, dass die zur Identitäts- und Attributsprüfung verwendeten Informationen noch gültig sind.

b) Sollten sich die Geschäftsbedingungen der Zertifizierungsstelle geändert haben, ist dies dem Zertifikatswerber mitzuteilen und gemäß Absatz 7.3.1 a), b), und h) zu vereinbaren.

c) Sollten sich Informationen geändert haben, ist dies zu prüfen und festzuhalten und die Zustimmung des Zertifikatswerbers gemäß Absatz 7.3.1 c) bis g) einzuholen.

d) Die Zertifizierungsstelle erstellt unter Verwendung des zu einem früheren Zeitpunkt zertifizierten öffentlichen Schlüssels nur dann ein neues Zertifikat, wenn dessen kryptografische Sicherheit noch für die beabsichtigte Laufzeit des neuen Zertifikats ausreicht und es keine Anzeichen gibt, dass der private Schlüssel des Zertifikatseigentümers kompromittiert wurde.

7.3.3 Zertifikatserstellung

Die Zertifizierungsstelle hat sicherzustellen, dass sie Zertifikate auf eine sichere Weise ausstellt, die deren Authentizität erhält (siehe Anhang II (g) der Signaturrichtlinie).

Insbesondere gilt:

Zertifikatserstellung

a) Die Zertifikate müssen konform zu den Anhängen I und II (g) der Signaturrichtlinie erzeugt und ausgegeben werden.

Hinweis: Ein Standardformat für qualifizierte Zertifikate, das die Anforderungen von Anhang I der Signaturrichtlinie erfüllt, wird in TS 101 862 definiert.

b) Das Ausstellen des Zertifikats ist auf sichere Weise mit der verknüpften Registrierung, Zertifikatserneuerung oder Schlüsselerneuerung (einschließlich jedweder vom Zertifikatseigentümer erstellter Schlüssel) verbunden.

c) Wurde der Schlüssel des Zertifikatseigentümers von der Zertifizierungsstelle erstellt, gilt Folgendes:

- Das Ausstellen des Zertifikats ist auf sichere Weise mit dem Erstellen des Schlüsselpaars durch die Zertifizierungsstelle verknüpft.
- Der private Schlüssel (oder die sichere Signaturerstellungseinheit, siehe Absatz 7.2.9) wird auf sichere Weise an den registrierten Zertifikatseigentümer übermittelt.

d) Die Zertifizierungsstelle muss im Laufe der Zeit die Eindeutigkeit des dem Zertifikatseigentümer zugewiesenen eindeutigen Namens innerhalb der Domäne der Zertifizierungsstelle sicherstellen. (Das heißt über die Lebensdauer der Zertifizierungsstelle hinweg darf ein eindeutiger Name, der von ihr bereits einmal für ein Zertifikat verwendet wurde, in keinem Fall einer anderen Entität erneut zugewiesen werden).

e) Die Vertraulichkeit und Integrität der Registrierungsdaten ist zu schützen, insbesondere dann, wenn sie mit dem Zertifikatswerber/-eigentümer oder zwischen verteilten Systemkomponenten der Zertifizierungsstelle ausgetauscht werden.

f) Sollten externe Registrierungsdienstanbieter eingesetzt werden, hat die Zertifizierungsstelle sicherzustellen, dass die Registrierungsdaten mit anerkannten Registrierungsdienstanbietern ausgetauscht werden, deren Identität authentifiziert ist.

7.3.4 Verbreitung der Nutzungsbedingungen

Die Zertifizierungsstelle muss sicherstellen, dass die Nutzungsbedingungen den Zertifikatswerbern und vertrauenden Parteien zur Verfügung stehen (siehe Anhang II (k) der Signaturrichtlinie).

Insbesondere gilt:

a) Die Zertifizierungsstelle stellt den Zertifikatswerbern und vertrauenden Parteien die Nutzungsbedingungen bezüglich der Nutzung des Zertifikats einschließlich Anhang II (g) der Signaturrichtlinie zur Verfügung:

   - Die angewandte Qualified Certificate Policy (QCP), einschließlich einer klaren Aussage darüber, ob die Policy für öffentliche Zertifikate gilt und ob die Policy die Verwendung einer sicheren Signaturerstellungseinheit erforderlich macht
   - Mögliche Nutzungsbeschränkungen
   - Pflichten des Zertifikatswerbers, wie sie in Absatz 6.2 beschrieben sind, einschließlich Informationen darüber, ob die CP die Verwendung einer sicheren Signaturerstellungseinheit erforderlich macht.
   - Informationen zur Validierung des Zertifikats, einschließlich der Anforderungen zur Überprüfung des Sperrstatus des Zertifikats, sodass vertrauende Parteien dem Zertifikat vertrauen können (siehe Absatz 6.3).
   - Haftungseinschränkungen einschließlich der Verwendungszwecke, für die die Zertifizierungsstelle eine Haftung übernimmt (oder ausschließt).
   - Zeitraum, über den Registrierungsinformationen aufbewahrt werden (siehe Absatz 7.3.1).
   - Zeitraum, über den die Zertifizierungsstelle Ereignisprotokolle aufbewahrt (siehe Absatz 7.4.11).
   - Prozeduren bei Klagen und zur Beilegung von Rechtsstreitigkeiten
   - Anwendbares Recht
   - Ob die Zertifizierungsstelle hinsichtlich ihrer Konformität zu der definierten Qualified Certification Policy zertifiziert wurde, und gegebenenfalls über welches Schema

b) Die vorstehend unter a) aufgeführten Informationen müssen über ein dauerhaftes (das heißt in der Zeit beständiges) Kommunikationsmittel zur Verfügung stehen, dessen elektronische Übertragung zulässig ist und das in normal verständlicher Sprache geschrieben sein muss.

Hinweis: Eine Vorlage für eine Erklärung zur Public Key-Infrastruktur (PKI Disclosure Statement), welche als Grundlage einer solchen Mitteilung verwendet werden kann, wird in Anhang B bereitgestellt. Alternativ dazu kann dies auch als Teil der Nutzungsvereinbarung mit Zertifikatswerbern/vertrauenden Parteien bereitgestellt werden. Diese Nutzungsbedingungen können in einem Certification Practice Statement (CPS) enthalten sein, vorausgesetzt, sie sind für den Leser deutlich als solche zu erkennen.

7.3.5 Verbreitung von Zertifikaten

Die Zertifizierungsstelle muss sicherstellen, dass Zertifikate entsprechend der Erfordernisse den Zertifikatswerbern, Zertifikatseigentümern und vertrauenden Parteien zur Verfügung stehen (siehe Anhang II (l) der Signaturrichtlinie).

Insbesondere gilt:

Verbreitung von Zertifikaten

a) Bei der Erstellung wird das vollständige und korrekte Zertifikat dem Zertifikatswerber oder -eigentümer, für den das Zertifikat ausgestellt wird, zur Verfügung gestellt.

b) Zertifikate werden nur dann zum Abruf freigegeben, wenn der jeweilige Zertifikatseigentümer sein Einverständnis gegeben hat.

c) Die Zertifizierungsstelle stellt den vertrauenden Parteien die Nutzungsbedingungen bezüglich der Nutzung des Zertifikats zur Verfügung (siehe Absatz 7.3.4).

d) Die für ein bestimmtes Zertifikat geltenden Nutzungsbedingungen müssen ohne weiteres erkennbar sein.

e) Die Informationen unter b) und c) müssen rund um die Uhr und an allen Tagen der Woche verfügbar sein. Bei Systemausfall, Service oder bei Eintritt anderer Faktoren, die nicht von der Zertifizierungsstelle kontrolliert werden können, bemüht sich die Zertifizierungsstelle darum, sicherzustellen, dass dieser Informationsservice nicht länger als eine bestimmte, im Certification Practice Statement festgesetzte Dauer außer Betrieb bleibt.

f) Die unter b) und c) angegebenen Informationen müssen öffentlich und international frei verfügbar sein.

7.3.6 Sperrung oder Suspendierung von Zertifikaten

Die Zertifizierungsstelle muss sicherstellen, dass Zertifikate in einem angemessenen Zeitraum und auf der Basis von autorisierten und validierten Anfragen zur Sperrung von Zertifikaten gesperrt werden (siehe Anhang II (b) der Signaturrichtlinie).

Insbesondere gilt:

Sperrmanagement

a) Die Zertifizierungsstelle dokumentiert als Teil des Certification Practice Statement (siehe Absatz 7.1) die Prozeduren für die Sperrung von Zertifikaten. Dabei sind folgende Informationen enthalten:

   - Wer ist zur Einreichung von Sperrmeldungen und -anfragen berechtigt.
   - Wie können diese eingereicht werden.
   - Welche Voraussetzungen gelten für die darauf folgende Bestätigung von Sperrmeldungen und -anfragen.

   Hinweis 1: Beispielsweise kann eine Bestätigung des Zertifikatswerbers erforderlich sein, wenn ein Dritter eine Kompromittierung meldet.

   - Ob und, wenn ja, aus welchen Gründen darf ein Zertifikat suspendiert werden.
   - Mechanismus für die Verbreitung der Informationen zum Sperrstatus
   - Maximaler Zeitraum zwischen Erhalt einer Sperranfrage oder -meldung und Änderung der Informationen zum Sperrstatus, die für sämtliche vertrauende Parteien verfügbar sein müssen. Die Höchstgrenze für diesen Zeitraum beträgt 1 Tag.

b) Anfragen und Meldungen, die sich auf die Sperrung beziehen (zum Beispiel aufgrund einer Kompromittierung des privaten Schlüssels des Zertifikatseigentümers, aufgrund des Ablebens des Zertifikatseigentümers oder aufgrund einer unerwarteten Beendigung einer Zertifikatswerber- oder Zertifikatseigentümervereinbarung oder der jeweiligen Geschäftsfunktionen oder aufgrund von Verletzung vertraglicher Verpflichtungen) werden bei Erhalt sofort bearbeitet.

c) Anfragen und Meldungen, die sich auf Sperrungen beziehen, werden authentifiziert und auf Herkunft aus einer autorisierten Quelle geprüft. Diese Arten von Meldungen und Anfragen werden bestätigt, wenn die von der Zertifizierungsstelle dargelegten Praktiken dies erfordern.

d) Der Sperrstatus eines Zertifikats kann während des Bestätigungsvorgangs für die Sperrung auf „suspendiert“ gesetzt werden. Die Zertifizierungsstelle muss sicherstellen, dass das Zertifikat sich nicht länger als für die Bestätigung des Status notwendig im Status der Suspendierung befindet.

Hinweis 2: Die Unterstützung von Suspendierungen von Zertifikaten ist optional.

e) Der Zertifikatseigentümer und gegebenenfalls der Zertifikatswerber eines gesperrten oder suspendierten Zertifikats werden über die Statusänderung des Zertifikats informiert.

f) Sobald ein Zertifikat definitiv gesperrt (also nicht suspendiert) ist, kann diese Sperrung nicht mehr aufgehoben werden.

g) Wenn Sperrlisten (CRLs, Certificate Revocation Lists), einschließlich aller Varianten (wie zum Beispiel Delta-CRLs) verwendet werden, werden diese mindestens täglich bereitgestellt und:

- Auf jeder Sperrliste ist ein Zeitpunkt für den nächsten geplanten Sperrlistenvorgang angegeben.
- Es darf vor dem angegebenen Zeitpunkt für den nächsten Sperrlistenvorgang eine neue Sperrliste veröffentlicht werden.
- Die Sperrliste wird von der Zertifizierungsstelle selbst oder von einer durch die Zertifizierungsstelle benannten Stelle signiert.

h) Das Sperrmanagement steht rund um die Uhr und an allen Tagen der Woche zur Verfügung. Bei Systemausfall, Service oder bei Eintritt anderer Faktoren, die nicht von der Zertifizierungsstelle kontrolliert werden können, bemüht sich die Zertifizierungsstelle darum, sicherzustellen, dass dieser Dienst nicht länger als eine bestimmte, im Certification Practice Statement festgesetzte Dauer außer Betrieb bleibt.

Sperrstatus

i) Die Informationen zum Sperrstatus stehen rund um die Uhr und an allen Tagen der Woche zur Verfügung. Bei Systemausfall, Service oder bei Eintritt anderer Faktoren, die nicht von der Zertifizierungsstelle kontrolliert werden können, bemüht sich die Zertifizierungsstelle darum, sicherzustellen, dass dieser Informationsservice nicht länger als eine bestimmte, im Certification Practice Statement festgesetzte Dauer außer Betrieb bleibt.

Hinweis 3: Informationen zum Sperrstatus können beispielsweise mithilfe eines Online-Service für den Zertifizierungsstatus oder über die Verteilung von Sperrlisten über ein Repository bereitgestellt werden.

j) Integrität und Authentizität der Statusinformationen werden geschützt.

k) Die Informationen zum Sperrstatus müssen öffentlich und international frei verfügbar sein.

7.4 Verwaltung und Betrieb der Zertifizierungsstelle

7.4.1 Sicherheitsmanagement

Die Zertifizierungsstelle stellt die Anwendung von adäquaten administrativen und Managementprozeduren, die den anerkannten Standards entsprechen, sicher (siehe Anhang II (2), 2. Teil, der Signaturrichtlinie).

Insbesondere gilt:

Allgemeine Anforderungen

a) Die Zertifizierungsstelle führt eine Risikoanalyse durch, um die Geschäftsrisiken zu evaluieren und die notwendigen Sicherheitsanforderungen und betrieblichen Prozeduren zu bestimmen.

b) Die Zertifizierungsstelle behält die Verantwortung für alle Aspekte der Bereitstellung von Zertifizierungsdiensten, auch wenn einige Aufgaben an Auftragnehmer delegiert werden. Die Verantwortlichkeiten von vertrauenden Parteien werden von der Zertifizierungsstelle genau definiert und es werden die entsprechenden Vereinbarungen getroffen, um eine Verpflichtung der vertrauenden Parteien zur Einrichtung der von der Zertifizierungsstelle geforderten Kontrollen zu gewährleisten. Die Zertifizierungsstelle ist für die Offenlegung der jeweiligen Praktiken aller Parteien zuständig.

c) Das Management der Zertifizierungsstelle stellt über ein auf angemessen hoher Ebene angesiedeltes Lenkungsgremium Anweisungen zur Informationssicherheit bereit. Dieses Lenkungsgremium ist für die Richtlinien zur Informationssicherheit der Zertifizierungsstelle und für die Sicherstellung der Veröffentlichung und Kommunikation dieser Richtlinien an alle davon betroffenen Mitarbeiter verantwortlich.

d) Diese für das Sicherheitsmanagement innerhalb der Zertifizierungsstelle wichtige Infrastruktur für die Informationssicherheit wird permanent aufrechterhalten. Jegliche Änderungen, die sich auf das bereitgestellte Sicherheits-Level auswirken, müssen durch das Managementforum der Zertifizierungsstelle genehmigt werden.

Hinweis 1: Weitere Informationen zum Informationssicherheits-Management, einschließlich der Infrastruktur für die Informationssicherheit, des Forums für das Management der Informationssicherheit und der Richtlinien zur Informationssicherheit, finden Sie im Standard ISO/IEC 17799. Alternativ dazu finden Sie andere Dokumente mit Informationen zum Thema in der Bibliografie.

e) Die Sicherheitskontrollen und Betriebsprozeduren für Vorrichtungen, Systeme und Informationsbestände der Zertifizierungsstelle, mit denen die Zertifizierungsdienste betrieben werden, müssen dokumentiert und eingerichtet sein und aufrechterhalten werden.

Hinweis 2: Es wird empfohlen, dass diese Dokumentation (allgemein als „Richtlinien zur Systemsicherheit“ bezeichnet) alle relevanten Ziele, Objekte und potenzielle Gefahren in Zusammenhang mit den bereitgestellten Diensten sowie die zur Vermeidung oder Einschränkung solcher Gefahren erforderlichen Sicherheitsvorkehrungen festlegt. Es wird ebenfalls empfohlen, dass die Dokumentation die Regeln, Anweisungen und Prozeduren dazu beschreibt, wie die spezifizierten Dienste und die damit verbundene Sicherheitsgewährleistung garantiert werden. Darüber hinaus sollte die Dokumentation Richtlinien für Zwischenfälle oder Systemausfälle enthalten.

f) Die Zertifizierungsstelle muss sicherstellen, dass die Informationssicherheit auch dann aufrechterhalten wird, wenn die Verantwortlichkeit für Aufgaben der Zertifizierungsstelle an eine andere Organisation oder Entität delegiert wurde.

7.4.2 Klassifikation und Verwaltung von Beständen

Die Zertifizierungsstelle muss sicherstellen, dass ihre Bestände und Informationen im angemessenen Maß geschützt werden (siehe Anhang II (e) der Signaturrichtlinie).

Insbesondere gilt:

Allgemeine Anforderungen

a) Die Zertifizierungsstelle pflegt ein Inventar aller Informationsbestände und weist den der Risikoanalyse entsprechenden Beständen eine Klassifikation für die Schutzanforderungen zu.

7.4.3 Personalsicherheit

Die Zertifizierungsstelle muss sicherstellen, dass Personal und Einstellungspraktiken die Vertrauenswürdigkeit der Arbeitsvorgänge der Zertifizierungsstelle stärken und unterstützen (siehe Anhang II (e), 1. Teil, der Signaturrichtlinie).

Insbesondere gilt:

Allgemeine Anforderungen

a) Die Zertifizierungsstelle beschäftigt Personal, das über das Fachwissen, die Erfahrung und die Qualifikationen verfügt, die für die angebotenen Dienste erforderlich und die jeweilige Tätigkeit angemessen sind.

Hinweis 1: Es wird empfohlen, dass das Personal der Zertifizierungsstelle die Anforderungen bezüglich „Fachwissen, Erfahrung und Qualifizierungen“ durch formale Ausbildung und Zeugnisse, tatsächliche Erfahrung oder eine Kombination davon erfüllt.

b) Die den in den Sicherheitsrichtlinien der Zertifizierungsstelle definierten Rollen und Verantwortlichkeiten bezüglich der Sicherheit werden in den Tätigkeitsbeschreibungen dokumentiert. Vertrauenswürdige Rollen, auf denen die Sicherheit der Arbeitsabläufe der Zertifizierungsstelle beruht, müssen dabei klar herausgestellt werden.

c) Die (temporären oder unbefristeten) Mitarbeiter einer Zertifizierungsstelle haben Tätigkeitsbeschreibungen, die vom Standpunkt der Trennung von Pflichten und des Prinzips der geringsten Berechtigung aus definiert sind und die die Sensibilität der Position auf der Basis von Pflichten und Zugriffsebenen, Screening des jeweiligen Hintergrunds, Schulung und Bewusstseinsbildung festlegen. Gegebenenfalls kann bei diesen Tätigkeitsbeschreibungen zwischen allgemeinen Funktionen und für die Zertifizierungsstelle spezifischen Funktionen unterschieden werden. Es wird empfohlen, dass die Tätigkeitsbeschreibungen eine Beschreibung der erforderlichen Fähigkeiten und Erfahrungen beinhalten.

d) Das Personal führt administrative und Managementprozeduren und -prozesse aus, die mit den Prozeduren der Zertifizierungsstelle zum Informationssicherheits-Management (siehe Absatz 7.4.1) im Einklang sind.

Hinweis 2: Weitere Informationen finden Sie im Standard ISO/IEC 17799.

Registrierung, Zertifikatserstellung, Bereitstellung von Geräten für Zertifikatseigentümer und Sperrmanagement

e) Auf Managerebene wird Personal eingestellt, das über Expertise im Bereich der elektronischen Signaturen und Vertrautheit mit Sicherheitsprozeduren verfügt. Letzteres gilt für Personal mit Verantwortung im Bereich der Sicherheit und Erfahrung in der Sicherheits- und Risikoanalyse.

f) Alle Mitarbeiter der Zertifizierungsstelle in vertrauenswürdigen Rollen müssen frei von Interessenkonflikten sein, die die Objektivität der Arbeitsvorgänge der Zertifizierungsstelle gefährden könnten.

g) Vertrauenswürdige Rollen schließen Rollen mit folgenden Verantwortlichkeiten ein:

- Security Officers (Sicherheitsbeauftragte): Die Sicherheitsbeauftragten haben die Gesamtverantwortung für die Verwaltung und Umsetzung von Sicherheitspraktiken. Darüber hinaus genehmigen Sie die Erstellung/Sperrung/Suspendierung von Zertifikaten.
- System Administrators (Systemadministratoren): Systemadministratoren sind dazu autorisiert, die vertrauenswürdigen Systeme der Zertifizierungsstelle für Registrierung, Zertifikatserstellung, Bereitstellung von Geräten für Zertifikatseigentümer und Sperrmanagement zu installieren, konfigurieren und zu pflegen.
- System Operators (Systemoperatoren): Systemoperatoren sind für den Betrieb der vertrauenswürdigen Systeme auf einer täglichen Basis zuständig. Sie sind dazu autorisiert, Systemsicherungen und -wiederherstellungen durchzuführen.
- System Auditors (Systemprüfer): Systemprüfer sind dazu autorisiert, Archive und Auditprotokolle der vertrauenswürdigen Systeme der Zertifizierungsstelle einzusehen und zu pflegen.

h) Das Personal der Zertifizierungsstelle wird vom für die Sicherheit verantwortlichen leitenden Management formal für vertrauenswürdige Rollen verpflichtet.

i) Die Zertifizierungsstelle darf niemanden, der/die bekanntermaßen für ein schweres Verbrechen oder eine andere Straftat, die seine/ihre Eignung für die Position betrifft, verurteilt wurde, für eine vertrauenswürdige Rolle oder eine Position im Management verpflichten. Das Personal hat keinen Zugang zu diesen vertrauenswürdigen Funktionen, bis die notwendigen Prüfungen abgeschlossen sind.

Hinweis 3: In manchen Ländern ist es der Zertifizierungsstelle eventuell nicht möglich, Informationen über in der Vergangenheit erfolgte Verurteilungen zu erhalten. Der Arbeitgeber kann jedoch den Mitarbeiter auffordern, diese Informationen beizutragen, und im Fall einer Weigerung die Bewerbung ablehnen.

7.4.4 Physikalische und Umgebungssicherheit

Die Zertifizierungsstelle muss sicherstellen, dass der physikalische Zugang zu kritischen Diensten kontrolliert wird und physikalische Risiken für ihre Bestände so gering wie möglich gehalten werden (siehe Anhang II (f) der Signaturrichtlinie).

Insbesondere gilt:

Allgemeine Anforderungen

a) Der physikalische Zugang zu Vorrichtungen für Dienste zur Erstellung von Zertifikaten, Bereitstellung von Geräten für Zertifikatseigentümer und Sperrmanagement ist auf entsprechend autorisierte Einzelpersonen beschränkt.

b) Zur Vermeidung von Verlust, Schäden oder Kompromittierung von Beständen und Geschäftsunterbrechungen werden Kontrollen eingerichtet.

c) Zur Vermeidung von Kompromittierung oder Diebstahl von Informationen und Informationsverarbeitungsvorrichtungen werden Kontrollen eingerichtet.

Zertifikatserstellung, Bereitstellung von Geräten für Zertifikatseigentümer und Sperrmanagement

d) Die Vorrichtungen für die Erstellung von Zertifikaten, die Bereitstellung von Geräten für Zertifikatseigentümer und das Sperrmanagement werden in einer Umgebung betrieben, die die Dienste physikalisch vor Kompromittierung durch unbefugten Zugriff auf Systeme oder Daten schützt.

e) Physikalischer Schutz wird durch die Schaffung von klar definierten, die Dienste zur Zertifikatserstellung, zur Bereitstellung von Geräten für Zertifikatseigentümer und für das Sperrmanagement umgebenden Sicherheitsbereichen (das heißt physikalischen Barrieren) erreicht. Jegliche Teile der Geschäftsräume, die mit anderen Unternehmen oder Organisationen gemeinsam genutzt werden, müssen außerhalb solcher Sicherheitsbereiche liegen.

f) Physikalische und Umgebungssicherheitskontrollen werden eingerichtet, um die Systemressourcen für die Unterbringung der Vorrichtung, die Systemressourcen selbst und die für die Unterstützung ihres Betriebs verwendeten Vorrichtungen zu schützen. Die Richtlinien der Zertifizierungsstelle zur physikalischen und Umgebungssicherheit für Systeme, die Dienste in Zusammenhang mit der Zertifikatserstellung, der Bereitstellung von Geräten für Zertifikatseigentümer und dem Sperrmanagement übernehmen, behandeln unter anderem folgende Themen: Kontrolle des physikalischen Zugangs, Schutz bei Naturkatastrophen, Feuerschutz, Ausfall von unterstützenden Systemen (wie etwa Netzstrom oder Telekommunikation), Zusammenbruch der Struktur, undichte Stellen in der Installation, Schutz gegen Diebstahl und Einbruch, Disaster Recovery und so weiter.

g) Es werden Kontrollen zum Schutz gegen das nicht autorisierte Entfernen von mit den Zertifizierungsdiensten verbundenen Vorrichtungen, Informationen, Medien und Software aus der Zertifizierungsstelle eingerichtet.

Hinweis 1: Weitere Informationen zur physikalischen und Umgebungssicherheit finden Sie im Standard ISO/IEC 17799.

Hinweis 2: Im selben Sicherheitsbereich können unter der Voraussetzung, dass der Zugang auf autorisiertes Personal beschränkt ist, andere Funktionen unterstützt werden.

7.4.5 Betriebsmanagement

Die Zertifizierungsstelle muss sicherstellen, dass die Systeme der Zertifizierungsstelle sicher und korrekt sind sowie mit einem Minimalrisiko eines Systemausfalls betrieben werden (siehe Anhang II (e) der Signaturrichtlinie).

Insbesondere gilt:

Allgemeine Anforderungen

a) Die Integrität der Systeme und Informationen der Zertifizierungsstelle wird gegen Viren, bösartige oder nicht autorisierte Softwareprogramme geschützt.

b) Durch Anwendung von Prozeduren zur Meldung von und Reaktion auf Zwischenfälle werden aus Sicherheitszwischenfällen und Fehlfunktionen resultierende Schäden auf ein Minimum reduziert.

c) Die in der Zertifizierungsstelle verwendeten Medien werden unter Einhaltung von Sicherheitsstandards behandelt, um sie vor Beschädigung, Diebstahl oder unbefugten Zugriff zu schützen.

Hinweis 1: Jeder Angehörige des Personals mit Management-Verantwortung ist für die Planung und effektive Umsetzung der Certificate Policy und damit verbundenen Praktiken entsprechend der im Certification Practice Statement dokumentierten Richtlinien zuständig.

d) Für alle vertrauenswürdigen und administrativen Rollen, die Einfluss auf die Bereitstellung von Zertifizierungsdiensten haben, werden Prozeduren erstellt und implementiert.

Behandlung und Sicherheit von Medien

e) Alle Medien werden unter Einhaltung von Sicherheitsstandards und in Übereinstimmung mit den Anforderungen des Schemas für die Klassifikation von Informationen behandelt (siehe Absatz 7.4.2). Medien mit sensiblen Daten werden, sofern sie nicht länger benötigt werden, unter Einhaltung von Sicherheitsstandards entsorgt.

Systemplanung

f) Die Kapazitätsanforderungen werden überwacht und es werden Projektionen für zukünftige Kapazitätsanforderungen durchgeführt, um die Verfügbarkeit der entsprechenden Verarbeitungsleistung und ausreichenden Speicherkapazitäten sicherzustellen.

Meldung von und Reaktion auf Zwischenfälle

g) Die Zertifizierungsstelle agiert rechtzeitig und koordiniert, um schnell auf Zwischenfälle reagieren zu können und so die Auswirkungen von Sicherheitsverstößen einzudämmen. Alle Zwischenfälle werden so bald wie möglich nach ihrem Eintreten gemeldet.

Zertifikatserstellung, Sperrmanagement

Operative Prozeduren und Verantwortlichkeiten

h) Die die Sicherheit betreffenden Arbeitsabläufe in der Zertifizierungsstelle werden von den normalen Arbeitsabläufen getrennt abgewickelt.

Hinweis 2: Zu den Verantwortlichkeiten der Security Operations der Zertifizierungsstelle gehören:

- Operative Prozeduren und Verantwortlichkeiten
- Planung und Annahme von sicheren Systemen
- Schutz gegen bösartige Software
- Organisation
- Netzwerkverwaltung
- Aktive Überwachung von Audit-Journals, Ereignisanalyse und Folgeaktivitäten
- Behandlung und Sicherheit von Medien
- Austausch von Daten und Software

Diese Verantwortlichkeiten werden von den Security Operations der Zertifizierungsstelle verwaltet, können aber durch nicht spezialisiertes Betriebspersonal (unter Aufsicht) entsprechend der dafür geltenden Sicherheitsrichtlinien, Rollen und Dokumente zu den Verantwortlichkeiten durchgeführt werden.

7.4.6 Verwaltung des Systemzugriffs

Die Zertifizierungsstelle muss sicherstellen, dass der Zugriff auf Systeme der Zertifizierungsstelle auf korrekt autorisierte Einzelpersonen beschränkt ist (siehe Anhang II (f) der Signaturrichtlinie).

Insbesondere gilt:

Allgemeine Anforderungen

a) Kontrollen (wie zum Beispiel Firewalls) werden eingerichtet, um die internen Netzwerkdomänen der Zertifizierungsstelle vor externen Netzwerkdomänen, auf die durch Außenstehende zugegriffen werden kann, zu schützen.

Hinweis 1: Es wird die Einrichtung von Firewalls empfohlen, um Protokolle und Zugriffe, die nicht für den Betrieb der Zertifizierungsstelle notwendig sind, zu unterbinden.

b) Sensible Daten werden geschützt, wenn sie über nicht sichere Netzwerke ausgetauscht werden.

Hinweis 2: Die sensiblen Daten schließen Registrierungsinformationen ein.

c) Die Zertifizierungsstelle stellt die effektive Administration des Zugriffs durch Benutzer (Bediener, Administratoren und alle Benutzer, die direkten Systemzugriff haben) sicher, um die Systemsicherheit aufrechtzuerhalten. Dazu gehört auch die Verwaltung und Überwachung von Benutzerkonten und die rechtzeitige Modifizierung oder Entziehung von Zugriffsrechten.

d) Die Zertifizierungsstelle muss sicherstellen, dass der Zugriff auf Informationen und Funktionen des Anwendungssystems in Übereinstimmung mit den Richtlinien zur Zugriffskontrolle eingeschränkt wird. Die Zertifizierungsstelle stellt außerdem genügend Computersicherheitskontrollen für die in den Praktiken der Zertifizierungsstelle definierten vertrauenswürdigen Rollen bereit, wobei auch die Trennung von Sicherheitsadministrator- und Bedienerfunktionen eingeschlossen ist. Insbesondere die Verwendung von Systemprogrammen ist eingeschränkt und unterliegt einer strengen Kontrolle.

e) Das Personal der Zertifizierungsstelle muss erfolgreich eine Auswahl und Authentifizierung durchlaufen, bevor es kritische, mit dem Zertifikatsmanagement verbundene Anwendungen ausführt.

f) Das Personal der Zertifizierungsstelle kann für seine Aktivitäten zur Verantwortung gezogen werden, zum Beispiel durch Aufbewahren von Ereignisprotokollen (siehe Absatz 7.4.11).

g) Sensible Daten werden durch wieder verwendete Speicherobjekte (zum Beispiel gelöschte Dateien), auf die nicht autorisierte Benutzer zugreifen können, geschützt.

Hinweis 3: Die sensiblen Daten schließen Registrierungsinformationen ein.

Zertifikatserstellung

h) Die Zertifizierungsstelle muss sicherstellen, dass lokale Netzwerkkomponenten (zum Beispiel Router) in einer physikalisch sicheren Umgebung aufbewahrt werden und ihre Konfigurationen regelmäßig auf die Erfüllung der durch die Zertifizierungsstelle spezifizierten Anforderungen überprüft werden.

i) Permanente Überwachung und Alarmvorrichtungen werden bereitgestellt, damit die Zertifizierungsstelle bei unbefugten Zugriffen auf ihre Ressourcen und/oder irregulären Zugriffsversuchen diese rechtzeitig erkennen, registrieren und darauf reagieren kann.

Hinweis 4: Hier können beispielsweise ein System zur Erkennung von Eindringlingen, eine Überwachung der Zugriffskontrolle und Alarmvorrichtungen zur Anwendung kommen.

Verbreitung

j) Eine Verbreitungsanwendung erzwingt bei Versuchen, Zertifikate hinzuzufügen, zu entfernen oder damit verknüpfte Informationen zu modifizieren, Zugriffskontrollen.

Sperrmanagement

k) Permanente Überwachung und Alarmvorrichtungen werden bereitgestellt, damit die Zertifizierungsstelle bei unbefugten Zugriffen auf ihre Ressourcen und/oder irregulären Zugriffsversuchen diese rechtzeitig erkennen, registrieren und darauf reagieren kann.

Hinweis 5: Hier können beispielsweise ein System zur Erkennung von Eindringlingen, eine Überwachung der Zugriffskontrolle und Alarmvorrichtungen zur Anwendung kommen.

Sperrstatus

l) Die Anwendung des Sperrstatus erzwingt bei Versuchen, die Informationen zum Sperrstatus zu modifizieren, Zugriffskontrollen.

7.4.7 Verteilung und Pflege vertrauenswürdiger Systeme

Die Zertifizierungsstelle verwendet vertrauenswürdige Systeme und Produkte, die gegen Modifizierungen geschützt sind (siehe Anhang II (f) der Signaturrichtlinie).

Hinweis 1: Die Anforderungen für vertrauenswürdige Systeme können zum Beispiel mithilfe von Systemen, die einem geeigneten Schutzprofil (oder -profilen) entsprechen und gemäß dem Standard ISO/IEC 15408 [3] oder einem entsprechenden Standard definiert wurden, erfüllt werden.

Hinweis 2: Es wird empfohlen, dass die für die Dienste der Zertifizierungsstelle (siehe Absatz 7.4.1) durchgeführte Risikoanalyse die kritischen Dienste, die vertrauenswürdige Systeme erfordern, herausarbeitet und die erforderlichen Sicherungsstufen festlegt.

Insbesondere gilt:

Allgemeine Anforderungen

a) Eine Analyse der Sicherheitsanforderungen wird im Stadium des Entwurfs und der Spezifikation von Anforderungen aller von der Zertifizierungsstelle oder im Auftrag der Zertifizierungsstelle durchgeführter Systementwicklungsprojekte durchgeführt, um sicherzustellen, dass die Sicherheit einen integralen Bestandteil von IT-Systemen darstellt.

b) Für jegliche Betriebssoftware gibt es für Versionen, Modifizierungen und Software-Fixes in Notfällen von Kontrollprozeduren für Änderungen.

7.4.8 Management der Geschäftskontinuität und Behandlung von Zwischenfällen

Die Zertifizierungsstelle muss sicherstellen, dass im Falle eines Systemausfalls (einschließlich Kompromittierung des privaten Schlüssels der Zertifizierungsstelle) der Betrieb so bald wie möglich wieder aufgenommen werden kann (siehe Anhang II (a) der Signaturrichtlinie).

Insbesondere gilt:

Allgemeine Anforderungen

Kompromittierung von Schlüsseln der Zertifizierungsstelle

a) Der Plan der Zertifizierungsstelle für die Sicherung der Geschäftskontinuität (oder der Disaster Recovery-Plan) behandelt die (mutmaßliche) Kompromittierung des privaten Signaturschlüssels der Zertifizierungsstelle wie ein Desaster.

Sperrstatus

b) Im Fall einer Kompromittierung unternimmt die Zertifizierungsstelle zumindest folgende Schritte:

   - Benachrichtigung aller Zertifikatswerber, Dritter und anderer Zertifizierungsstellen, mit denen die Zertifizierungsstelle durch vertragliche Vereinbarungen oder andere etablierten Beziehungen bezüglich der Kompromittierung verbunden ist.
   - Hinweis darauf, dass Zertifikate und Informationen zum Sperrstatus, die mithilfe dieses Schlüssels der Zertifizierungsstelle ausgegeben wurden, eventuell nicht mehr gültig sind.

Hinweis: Wenn eine Zertifizierungsstelle, mit der die kompromittierte Zertifizierungsstelle eine Vereinbarung hat, über die Kompromittierung informiert wird, ist die Sperrung aller Zertifikate, die jene andere Zertifizierungsstelle für die kompromittierte Zertifizierungsstelle ausgestellt hat, zu sperren.

7.4.9 Einstellung der Dienste der Zertifizierungsstelle

Die Zertifizierungsstelle muss sicherstellen, dass eventuelle Unterbrechungen für Zertifikatswerber und vertrauende Parteien durch die Einstellung der Dienste der Zertifizierungsstelle auf ein Minimum beschränkt werden. Sie stellt die weitere Pflege von Datensätzen, die für den Nachweis der Zertifizierung für Gerichtsverfahren erforderlich sind, sicher (siehe Anhang II (i) der Signaturrichtlinie).

Insbesondere gilt:

Allgemeine Anforderungen

a) Bevor die Zertifizierungsstelle ihre Dienste einstellt, müssen zumindest Folgendes durchgeführt werden:

   - Die Zertifizierungsstelle informiert alle Zertifikatswerber, vertrauende Parteien und andere Zertifizierungsstellen, mit denen die Zertifizierungsstelle durch vertragliche Vereinbarungen oder andere etablierten Beziehungen verbunden ist.

Hinweis: Dabei muss die Zertifizierungsstelle keine vorherige Beziehung zu den vertrauenden Parteien haben.

   - Die Zertifizierungsstelle beendet alle Autorisierungen für Auftragnehmer, die bei der Realisierung von Funktionen im Prozess der Ausstellung von Zertifikaten im Auftrag der Zertifizierungsstelle handeln.
   - Die Zertifizierungsstelle unternimmt die notwendigen Schritte, um die Pflichten der Pflege der Registrierungsinformationen (siehe Absatz 7.3.1) und der Ereignisprotokollarchive (siehe Absatz 7.4.11) für den jeweils den Zertifikatswerbern und vertrauenden Parteien gegenüber genannten Zeitraum zu transferieren.
   - Die Zertifizierungsstelle zerstört ihre privaten Schlüssel oder zieht sie aus dem Verkehr, wie in Absatz 7.2.6 definiert.

b) Die Zertifizierungsstelle hat eine Vereinbarung über die Übernahme Kosten für die Erfüllung dieser Mindestanforderungen für den Fall, dass die Zertifizierungsstelle

zahlungsunfähig wird oder aus anderen Gründen die Kosten nicht selbst decken kann.

c) Die Zertifizierungsstelle legt in ihren Praktiken die Maßnahmen dar, die im Fall der Beendigung des Dienstes ergriffen werden. Diese Darlegung beinhaltet Folgendes:

- Benachrichtigung der betroffenen Entitäten
- Weitergabe der eigenen Pflichten an andere
- Behandlung des Sperrstatus für noch nicht abgelaufene Zertifikate, die von der Zertifizierungsstelle ausgestellt wurden

7.4.10 Einhaltung gesetzlicher Anforderungen

Die Zertifizierungsstelle stellt die Einhaltung gesetzlicher Anforderungen sicher (siehe Artikel 8 der Signaturrichtlinie).

Insbesondere gilt:

Allgemeine Anforderungen

a) Wichtige Datensätze werden vor Verlust, Zerstörung und Fälschung geschützt. Manche Datensätze müssen möglicherweise sicher aufbewahrt werden, um einerseits die gesetzlichen Anforderungen zu erfüllen und andererseits wichtige Geschäftsaktivitäten zu unterstützen (siehe Absatz 7.4.11).

b) Die Zertifizierungsstelle stellt die Einhaltung der in nationales Recht umgesetzten europäischen Datenschutzrichtlinie sicher.

c) Gegen die nicht autorisierte oder nicht rechtmäßige Verarbeitung von persönlichen Daten und gegen versehentlichen Verlust, Zerstörung oder Beschädigung von persönlichen Daten werden angemessene technische und organisatorische Maßnahmen ergriffen.

d) Die Informationen, die Benutzer an die Zertifizierungsstelle weitergeben, sind absolut vor einer Offenlegung ohne Einwilligung des betreffenden Benutzers, gerichtlichen Beschluss oder andere gesetzliche Bevollmächtigung geschützt.

7.4.11 Aufbewahrung von Informationen zu Zertifikaten

Die Zertifizierungsstelle muss sicherstellen, dass alle relevanten, ein Zertifikat betreffende Informationen über einen angemessenen Zeitraum hinweg aufbewahrt werden, insbesondere zum Zweck der Bereitstellung von Zertifizierungsnachweisen im Fall von Gerichtsverfahren (siehe Anhang II (i) der Signaturrichtlinie).

Hinweis 1: Datensätze zu qualifizierten Zertifikaten umfassen Registrierungsinformationen (siehe Absatz 7.3.1) und Informationen über wichtige Ereignisse bezüglich der Umgebung und der Verwaltung der Schlüssel und Zertifikate bei der Zertifizierungsstelle.

Insbesondere gilt:

Allgemein

a) Die Vertraulichkeit und Integrität von aktuellen und archivierten Datensätzen zu qualifizierten Zertifikaten wird gewahrt.

b) Datensätze zu qualifizierten Zertifikaten müssen vollständig und vertraulich sowie in Einklang mit den offen gelegten Geschäftspraktiken archiviert werden.

c) Datensätze zu qualifizierten Zertifikaten werden verfügbar gemacht, wenn dies für Zwecke des Nachweises der Zertifizierung für Gerichtsverfahren erforderlich ist. Der

Zertifikatseigentümer und, innerhalb der Grenzen der Datenschutzanforderungen (siehe Absatz 7.4.10), der Zertifikatswerber haben Zugang zu Registrierungsinformationen und anderen Informationen, die den Zertifikatseigentümer betreffen.

Hinweis 2: Dies kann beispielsweise für die Unterstützung der Verbindung zwischen dem Zertifikat und dem Zertifikatseigentümer angewendet werden.

d) Von wichtigen Ereignissen bezüglich der Umgebung und der Verwaltung der Schlüssel und Zertifikate bei der Zertifizierungsstelle wird die genaue Zeit festgehalten.

Hinweis 3: Es wird empfohlen, dass die Zertifizierungsstelle in ihren Praktiken die Genauigkeit der Uhr, die für die Zeitangabe von Ereignissen verwendet wird, festlegt und eine Aussage darüber macht, wie diese Genauigkeit sichergestellt wird.

e) Datensätze zu qualifizierten Zertifikaten werden über einen Zeitraum hinweg, der für die Bereitstellung erforderlicher rechtlicher Nachweise für elektronische Signaturen angemessen ist, aufbewahrt.

Hinweis 4: Die genaue Aufbewahrungsdauer der Datensätze ist schwer festzulegen und erfordert eine Abwägung zwischen dem Bedarf nach Bezugnahme auf diese Daten und dem für die Aufbewahrung notwendigen Aufwand. Die Datensätze könnten solange benötigt werden, wie eine auf dem gültigen Zertifikat basierende Transaktion in Frage gestellt werden kann. Bei den meisten Transaktionen schließen Begrenzungsregeln die Anfechtbarkeit der Transaktion irgendwann aus. Bei manchen Transaktionen jedoch, wie zum Beispiel der Übertragung von Eigentum, kann die gesetzliche Verjährung erst nach längerer Zeit eintreten, wenn überhaupt.

Hinweis 5: Dort, wo für Zertifikate mit unterschiedlichen Anwendungsbereichen verschiedene Aufbewahrungszeiten gelten, müssen sie klar angegeben werden, und es sollten verschiedene Kennungen für die jeweilige Qualified Certificate Policy verwendet werden. Falls für unterschiedliche Teile der Datensätze aus Registrierung und Systemprotokollierung verschiedene Aufbewahrungszeiten gelten, muss dies dem Zertifikatswerber und den vertrauenden Parteien entsprechend der Absätze 7.3.1 und 7.3.4 mitgeteilt werden.

f) Die Ereignisse werden so protokolliert, dass sie innerhalb des Zeitraums, über den sie aufbewahrt werden müssen, nicht einfach gelöscht oder zerstört werden können (mit Ausnahme einer Übertragung auf dauerhafte Medien).

Hinweis 6: Dies kann beispielsweise durch Verwendung von Medien, auf die nur Schreibzugriff möglich ist, einer Liste aller verwendeten löschbaren Medien und die Verwendung von Backup-Systemen außerhalb der Zertifizierungsstelle erreicht werden.

g) Die spezifischen, zu protokollierenden Ereignisse und Daten werden von der Zertifizierungsstelle dokumentiert.

Registrierung

h) Die Zertifizierungsstelle muss sicherstellen, dass alle Ereignisse, die mit der Registrierung zusammenhängen, einschließlich Anfragen zur Schlüsselerneuerung oder Verlängerung eines Zertifikats, protokolliert werden.

i) Die Zertifizierungsstelle muss sicherstellen, dass alle Registrierungsinformationen festgehalten werden, einschließlich der folgenden:

- Typ des Dokuments (der Dokumente), das (die) der Antragsteller bei der Registrierung vorgelegt hat
- Datensatz mit eindeutigen Identifikationsdaten, -nummern der Ausweisdokumente oder gegebenenfalls einer Kombination daraus (zum Beispiel Führerscheinnummer des Antragstellers)
- Speicherort von Kopien von Anwendungen und Ausweisdokumenten, einschließlich der unterschriebenen Vereinbarung für Zertifikatswerber (siehe Absatz 7.3.1 h))
- spezifisch ausgewählte Optionen in der Vereinbarung für Zertifikatswerber (zum Beispiel Zustimmung zur Veröffentlichung des Zertifikats)
- Identität der Entität, die den Antrag genehmigt
- Methode, die für die Validierung der Ausweisdokumente verwendet wird, falls vorhanden
- Name der Zertifizierungsstelle auf Empfängerseite und/oder der einreichenden Registrierungsstelle

j) Die Zertifizierungsstelle muss sicherstellen, dass die Vertraulichkeit von Informationen zum Zertifikatseigentümer gewahrt bleibt.

Zertifikatserstellung

k) Die Zertifizierungsstelle protokolliert alle Ereignisse, die sich auf die Lebensdauer von Schlüsseln der Zertifizierungsstelle beziehen.

l) Die Zertifizierungsstelle protokolliert alle Ereignisse, die sich auf die Lebensdauer von Zertifikaten beziehen.

Bereitstellung von Geräten für Zertifikatseigentümer

m) Die Zertifizierungsstelle protokolliert alle Ereignisse, die sich auf die Lebensdauer der von der Zertifizierungsstelle verwalteten Schlüssel beziehen, einschließlich aller durch die Zertifizierungsstelle generierten Schlüssel der Zertifikatseigentümer.

n) Falls anwendbar, protokolliert die Zertifizierungsstelle alle Ereignisse, die sich auf die Ausgabe sicherer Signaturerstellungseinheiten beziehen.

Sperrmanagement

o) Die Zertifizierungsstelle muss sicherstellen, dass alle Anfragen und Meldungen, die sich auf die Sperrung und die daraus resultierende Vorgehensweise beziehen, protokolliert werden.

7.5 Organisation

Die Zertifizierungsstelle stellt die Zuverlässigkeit ihrer Organisation sicher (siehe Anhang II (a) der Signaturrichtlinie).

Insbesondere gilt:

Allgemeine Anforderungen

a) Richtlinien und Prozeduren, die für den Betrieb der Zertifizierungsstelle gelten, sind nicht diskriminierend.

b) Die Zertifizierungsstelle macht ihre Dienste allen Antragstellern, deren Aktivitäten in das erklärte Betätigungsfeld der Zertifizierungsstelle fallen, zugänglich.

c) Die Zertifizierungsstelle ist entsprechend der nationalen Gesetze eine juristische Person.

d) Die Zertifizierungsstelle verfügt über ein System oder mehrere Systeme für das Qualitäts- und Informationssicherheits-Management, das (die) für die angebotenen Zertifizierungsdienste geeignet ist (sind).

e) Die Zertifizierungsstelle verfügt über adäquate Vereinbarungen zur Abdeckung von Haftungsfällen, die sich aus ihren Aufgabenbereichen und/oder Aktivitäten ergeben können.

f) Die Zertifizierungsstelle verfügt über ausreichende finanzielle Stabilität und Ressourcen, um in Einklang mit dieser Richtlinie betrieben werden zu können.

g) Die Zertifizierungsstelle beschäftigt eine ausreichende Anzahl an Mitarbeitern, die über die notwendigen Voraussetzungen bezüglich Ausbildung, Schulung sowie die technischen Kenntnisse und Erfahrung für diesen Typ, Bereich und Umfang von Arbeit verfügen, die für die Bereitstellung der Zertifizierungsdienste erforderlich sind.

h) Die Zertifizierungsstelle verfügt über Richtlinien und Prozeduren zur Beilegung von Klagen und Rechtsstreitigkeiten von bzw. mit Kunden oder vertrauenden Parteien über die Bereitstellung von vertrauenswürdigen elektronischen Diensten oder über andere, damit im Zusammenhang stehende Gegenstände.

i) Die Zertifizierungsstelle verfügt über eine ordnungsgemäß dokumentierte Vereinbarung und ein etabliertes vertragliches Verhältnis bei Bereitstellung der Dienste mittels Vergabe von Unteraufträgen, Outsourcing oder anderen Vereinbarungen mit Dritten.

Zertifikatserstellung, Sperrmanagement

j) Die mit der Verwaltung der Zertifikatserstellung und dem Sperrmanagement befassten Teile der Zertifizierungsstelle sind unabhängig von anderen Organisationen, da ihre Entscheidungen sich auf die Erstellung, Ausgabe, Pflege und Aufhebung von Diensten beziehen. Im Besonderen müssen Direktionsbevollmächtigte, leitende Angestellte und Personal in vertrauenswürdigen Rollen frei von jeglichen kommerziellen, finanziellen oder anderen Zwängen sein, die sich negativ auf die Vertrauenswürdigkeit der bereitgestellten Dienste auswirken könnte.

k) Die mit der Verwaltung der Zertifikatserstellung und dem Sperrmanagement befassten Teile der Zertifizierungsstelle haben eine dokumentierte Struktur, die die Objektivität der Arbeitsvorgänge gewährleistet.