Richtlinie Digitale Zertifikate (ISM)
Certificate Policy (CP)

Änderungsübersicht

Datum	Version	Beschreibung der Änderung	Autor
12.10.2015	0.1	Initialversion	
15.07.2016	0.9		Volker Simon (CSOI)
05.10.2016	0.91	Korrekturen und Ergänzungen	Wilhelm Engels
16.12.2016	0.92	Konkretisierungen bei Sperranträgen	Volker Simon
28.03.2017	0.93	Korrekturen Namen	Wilhelm Engels
26.05.2017	0.94	Korrekturen, Formatierungen, Kommentare	Volker Simon (CSOI)
04.07.2017	0.95	Anpassungen struktureller Natur	Volker Simon (CSOI)
21.07.2017	0.99	Pre-finale Version für Übergabe an GLs im IT-Betrieb.	Volker Simon (CSOI)
21.02.2019	1	Erstellung Finaler Version	Tobias Kußmaul (GSOI)

1 Einleitung

Digitale Zertifikate werden zur Absicherung rechnergestützter Kommunikation verwendet. Mit Ihnen kann die Identität der jeweiligen kommunizierenden Systeme oder Nutzer festgestellt, sowie eine vertrauliche und integritätsgeschützte Kommunikation aufgebaut werden.

Als eine Public-Key-Infrastruktur (PKI) wird ein System bestehend aus IT-Systemen und Prozessen bezeichnet, dass digitale Zertifikate ausstellen, verteilen und prüfen kann. Eine PKI stellt mit der Ausstellung eines Zertifikats das Binden eines öffentlichen Schlüssels an eine Entität (Person, IT-System) sicher.

Den technischen Kern der PKI bilden die Certification Authorities (**CAs**) (dt. Zertifizierungsstellen), die digitale Zertifikate ausstellen und verwalten.

Für die PKI ist die Einschätzung der Vertrauenswürdigkeit der ausgestellten Zertifikate von entscheidender Bedeutung. Die dazu notwendigen Vorgaben werden in dieser Certificate Policy (**CP**) (dt. Richtlinie für digitale Zertifikate) beschrieben.

1.1 Überblick

Die CP ist Bestandteil des Richtlinienwerks Informationssicherheit der DZ BANK AG. Außer den hier beschriebenen Richtlinien, gelten die internen Richtlinien und Vorgaben der DZ BANK AG. In diesem Dokument werden insbesondere die Rahmenbedingungen für die Ausstellung von Zertifikaten entsprechend der internationalen Norm X.509 (X.509, 2012) festgelegt. Die Richtlinien in diesem Dokument beziehen sich ausschließlich auf die DZ BANK AG PKI und sind bindend für alle IT-Systeme der DZ BANK AG, die durch diese PKI ausgestellte Zertifikate nutzt.

Eine PKI, die in Übereinstimmung mit dieser CP arbeitet, kann folgende Sicherheitsmanagementdienstleistungen zur Verfügung stellen:

- Schlüsselgenerierung und Schlüsselspeicherung
- Generieren, Modifizieren, Re-Key (dt. erneute Schlüsselvergabe) und Verteilen von Zertifikaten
- Key Escrow (dt. Schlüsselhinterlegung) und Wiederherstellung von privaten Schlüsseln mit der dazugehörigen Verschlüsselung zugeordneter Zertifikate (z.B. Schlüsselmanagement, -verwaltung)
- Zertifikat-Status-Dienst: Certificate Revocation List (**CRL**) (dt. Zertifikatssperrliste) oder/und Online Certificate Status Protocoll (**OCSP**) (dt. Online Zertifikate Status Protokoll)
- Zertifikate auf Tokens (z.B. Smartcards): Initialisierung/Programmierung/Management

Die Nutzung dieser PKI wird u.a. angestrebt für die Erteilung und dem Management von Zertifikaten für:

- Nutzer (Authentifizierung, Sichere Email, Single-Sign-On, etc.)
- Computer (Clients und Server) und Netzwerkkomponenten (SSL/TLS, IPSec, etc.)
- Dienste (engl. Services)
- Softwaresignatur (Integrität und Authentizität von Programmen und Skripten)

Eine Übersicht der derzeitig gültigen CAs der internen PKI kann unter http://pki.dzbank.de eingesehen werden.

Pro gültiger CA gibt es ein entsprechendes Certificate Practice Statement (**CPS**) (dt. Erklärung zum Zertifizierungsbetrieb). Das CPS konkretisiert wie die Anforderungen der CP der DZ BANK AG im Detail umgesetzt werden. Das CPS kann Anforderungen nur konkretisieren bzw. verschärfen jedoch nicht abschwächen.

1.1.1 Ziel dieser Richtlinie

Das Ziel dieser Richtlinie ist es, Mindestanforderungen für den sicheren Betrieb der PKI zu definieren und dementsprechend für ein einheitliches Sicherheitsniveau ausgestellter Zertifikate zu sorgen. Der sichere Betrieb bezieht sich insbesondere auf die Prozesssicherheit sowie die technische IT-Sicherheit.

1.1.2 RFC 3647 Struktur

Der Aufbau des Dokuments lehnt sich an die Empfehlungen der Internet Engineering Task Force (IETF) ([RFC 3647], et al., 2003) an.

1.1.3 Konventionen

Innerhalb dieser Sicherheitsrichtlinie werden (analog zum Englischen must/shall – should – may) entsprechend IETF ([RFC 2119] & Bradner, 1997) die Begriffe **muss – soll – kann** verwendet:

- **muss, darf nicht, darf nur, ist/sind verpflichtet, ist/sind zuständig**
  Verbindliche Vorgabe
- **soll**, (**sollte**)
  Empfehlung (Nichteinhaltung nur in begründeten Ausnahmen)
- **kann, muss nicht**
  optional

1.1.4 Gültigkeit

Diese Richtlinie ist für Teilnehmer der DZ BANK AG PKI ab Veröffentlichung bindend. Für Zertifikatsnehmer der DZ BANK AG besteht ein Übergangszeitraum zur Umsetzung von 2 Jahren ab Veröffentlichung dieser Richtlinie. Jede Erneuerung von bestehenden digitalen Zertifikaten ist gemäß dieser CP durchzuführen.

1.2 Name und Kennzeichnung

Der Object Identifier (**OID**) (dt. Objektkennung) dokumentiert in den ausgestellten Zertifikaten die Konformität zu (X.509, 2012).

Die, durch die Internet Assigned Numbers Authority (**IANA**) vergebene OID an die DZ BANK AG lautet 1.3.6.1.4.1.38845.

Diese CP ist folgendermaßen identifiziert:

- Titel: Certificate Policy DZ BANK AG
- Version: 1.0
- Object Identifier (OID): 1.3.6.1.4.1.38845.509.1.1.1.1.1.1

Die OID ist wie folgt zusammengesetzt:

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) DZ BANK AG(38845) Technologie(509) Subsidary(1) Department(1) Environment(1) General Policy(1) running Number (1) Major Version(1)}

1.3 Teilnehmer der PKI

1.3.1 PKI-Verwaltung

In diesem Abschnitt werden Rollen und Aufgaben, die für die Verwaltung und den Betrieb der PKI im Rahmen dieser CP notwendig sind, beschrieben.

1.3.1.1 Policy Authority (PA) (dt. Richtlinienverwaltung)

Die Zuständigkeit der Verwaltung der CP liegt bei:

DZ BANK AG
Deutsche Zentral-Genossenschaftsbank, Frankfurt am Main
Informationssicherheit

Platz der Republik
60265 Frankfurt am Main
E-Mail: is-office@dzbank.de

Nachfolgende Aufgaben werden von der PA wahrgenommen:

- Etablierung und Update der CP
- Konformitätsprüfung: Abnahme von CPS, die dieser CP unterliegen (Prüfung der Dokumentenlage CP und CPS)
- Audit: Prüfung der Umsetzung der CP bzw. CPS. Begleitung von CA-Audits im Rahmen des geregelten ISMS Betriebs

Siehe auch Kapitel 5.2.1.

1.3.1.2 Trust Anchor Manager (TAM)

Hier handelt es sich um die Autorität, die die DZ BANK AG Root CA verwaltet:

DZ BANK AG
Deutsche Zentral-Genossenschaftsbank, Frankfurt am Main
Public Key Infrastructure
Platz der Republik
60265 Frankfurt am Main

E-Mail: pki-info@dzbank.de

Nachfolgende Aufgaben werden von der TAM wahrgenommen:

- Erstellung und Pflege des CPS der DZ BANK AG Root CA
- Erzeugung eines kryptographisch geeigneten Schlüsselpaares der DZ BANK AG Root CA in einer gesicherten Umgebung.
- Erzeugung des selbstsignierten Zertifikats der DZ BANK AG Root CA.
- Verwaltung und Veröffentlichung aller DZ BANK AG Root CA Zertifikate.

- Ausstellen von Issuing CAs (CAs, die End-Entitätszertifikate ausstellen)
- Integre und authentische Veröffentlichung von:
    - DZ BANK AG Root CA Zertifikat einschließlich des dazugehörigen Fingerabdrucks
    - Durch DZ BANK AG Root CA ausgestellte Zertifikate
    - Durch DZ BANK AG Root CA ausgestellte Sperrlisten
- Erstellung von Sperraufforderungen an CAs (Root und Issuing CAs) im Fall von Kompromittierungsmeldungen.
- Einleitung von geeigneten Maßnahmen bei Kompromittierung einer CA.

Sofern eine Vertrauensbeziehung mit externen PKIs aufgebaut werden soll, ist der TAM verantwortlich für:

- Analyse des Schutzniveaus einer Root CA zu der eine Vertrauensbeziehung aufgebaut werden soll durch Prüfung des jeweiligen CPS gegenüber der DZ BANK CP.

Der TAM definiert und etabliert gemeinsam mit den Verantwortlichen der Issuing-CA einen Prozess für den Kompromittierungsfall.

Siehe auch Kapitel 5.2.1.

1.3.1.3 Certification Authority (CA)

Den CAs (Root, Issuing oder Intermediate CAs) obliegt die Ausstellung von Zertifikaten innerhalb der DZ BANK AG PKI.

Die oberste CA (DZ BANK AG Root CA) der DZ BANK AG PKI zertifiziert ausschließlich Zertifikate von unmittelbar nachgeordneten CAs entsprechend dieser CP und dem CPS der DZ BANK AG Root CA.

Unter den Betrieb der PKI fallen folgende Tätigkeiten:

- Genehmigung der Ausgabe von allen Zertifikaten, einschließlich solcher, die untergeordnete CAs und Registration Authoritys (**RAs**) (dt. Registrierungsstellen) ausstellen.
- Veröffentlichung von Zertifikaten
- Sperren (Widerruf) von Zertifikaten
- Generierung und Vernichtung der Signaturschlüssel der CA
- Aufbau und Pflege der CA
- Aufbau und Pflege des CPS der CA

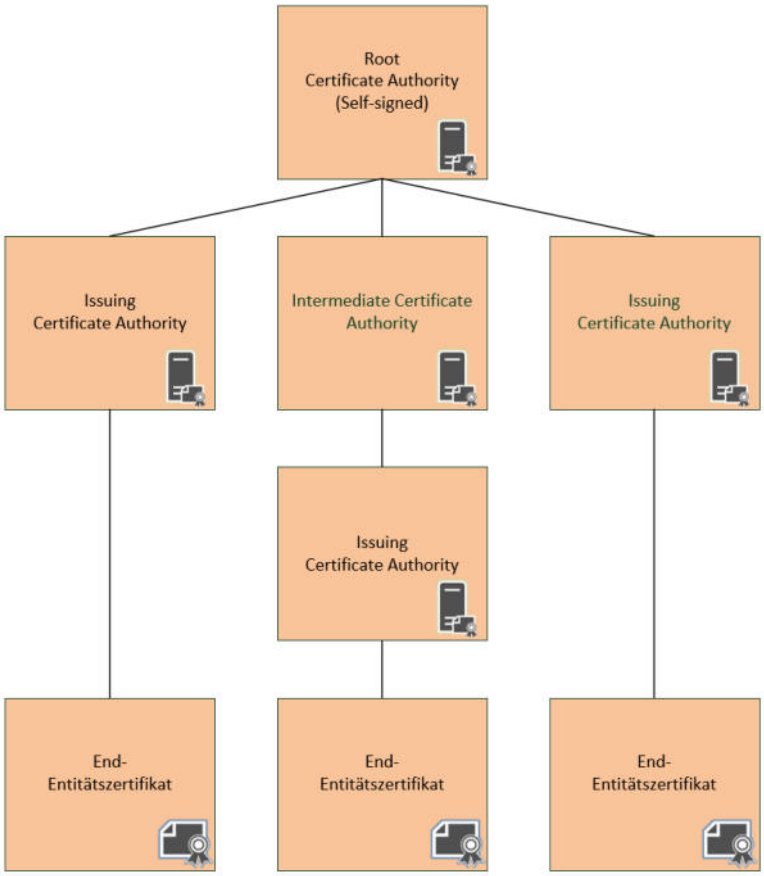

Abbildung 1 Beispielhafte mögliche CA PKI Hierarchie

1.3.1.4 Certificate Status Servers (CSS)

PKIs stellen einen Online-Dienst bereit, über welchen der Status eines Zertifikats abgefragt wird. Dies kann über das Online Certificate Status Protocol (OCSP) oder Certificate Revocation Lists (CRLs) gewährleistet werden.

1.3.2 Registration Authority (dt. Registrierungsstelle)

Jeder CA innerhalb der DZ BANK AG PKI ist mindestens eine Registration Authority (**RA**) zugeordnet, die im zugehörigen CPS zu benennen ist. Die RA führt die Registrierung der Zertifikatsnehmer durch. Die RA-Tätigkeit wird von dedizierten RA-Mitarbeitern durchgeführt, sofern keine automatische Prüfung der notwendigen Informationen in den Anträgen möglich ist.

Alle CAs innerhalb der DZ BANK AG PKI haben die Möglichkeit, weitere RAs für die lokale Überprüfung der Identität und Authentizität der Zertifikatsnehmer zu benennen.

Benennung und Entbindung von RAs sind zu dokumentieren und an PA und TAM zu kommunizieren.

1.3.3 Trusted Agents (dt. Vertrauensperson)

Ein Trusted Agent (**TA**) ist eine Person, die stellvertretend für eine RA Registrierungsanträge erfassen und Identitätsprüfungen vornehmen kann. Im CPS der jeweiligen CA sind die Verantwortlichen für die Bereitstellung des Dienstes und die Prozesse zur Bestimmung der Vertrauenswürdigkeit eines TA entsprechend dem Schutzbedarf festzulegen.

1.3.4 Subscriber (dt. Zertifikatsnehmer)

Subscriber (dt. Zertifikatsnehmer) sind natürliche Personen, Organisationen und Systeme, für die Zertifikate ausgestellt werden.

Der Subscriber ist im Besitz des zum öffentlichen Schlüssel gehörenden privaten Schlüssel und kann somit über das ausgestellte Zertifikat seine Identität ausweisen. Er ist auskunftspflichtig gegenüber Fragen der RA und verpflichtet sich zur Geheimhaltung des privaten Schlüssels sowie sein Schlüsselpaar und das zugehörige Zertifikat nur gemäß dieser Certificate Policy einzusetzen.

Darüber hinaus ist er verpflichtet eine Kompromittierung des privaten Schlüssels an die CA zu melden.

1.3.5 Relying Parties (dt. Zertifikatsnutzer)

Eine Relying Party ist eine Entität (Kommunikationsteilnehmer, z.B. Person, Gerät, Applikation oder Prozess), die auf die Gültigkeit der Bindung der Identität des Kommunikationspartners zu seinem öffentlichen Schlüssel vertraut. Der Kommunikationsteilnehmer verwendet das vom Kommunikationspartner erhaltene Zertifikat zur Überprüfung oder Etablierung dessen Identität und des Status des Partners.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendung von Zertifikaten

Die im Rahmen der DZ BANK AG PKI ausgestellten Zertifikate sind grundsätzlich für Personen, Geräte oder Anwendungen vorgesehen und für folgende Einsatzzwecke vorgesehen:

- Authentisierung einer Person, Gerät oder Anwendung
- Erstellung einer digitalen Signatur durch eine Person, Gerät oder Anwendung
- Verschlüsselung der Kommunikation zwischen Personen, Geräten oder Anwendungen.

Zertifikatsnehmer sind selbst für die Nutzung in den Anwendungsprogrammen zuständig. Es muss durch die Dienstebereitsteller/Informationstreuhänder sichergestellt werden, dass die Verwendung von Zertifikaten den Sicherheitsanforderungen (Verwendung gemäß der Certificate Usage Parameter, siehe Kapitel 6.1.7) genügt.

1.4.2 Verbotene Verwendung von Zertifikaten

Die Nutzung des Zertifikats darf nicht im Widerspruch zu den im Zertifikat enthaltenen Schlüsselverwendungszwecken erfolgen, insbesondere ist die Ausstellung von Zertifikaten und Sperrlisten ausschließlich CAs vorbehalten. Auf produktiven IT-Assets sind nur Zertifikate der PKI-Produktionsumgebung zu nutzen.

1.5 Verwaltung des Dokuments

1.5.1 Zuständigkeit für das Dokument

Die im Kapitel 1.3.1 unter Richtlinienverwaltung genannte organisatorische Einheit (Policy Authority) ist zuständig für alle Aspekte dieser CP.

1.5.2 Ansprechpartner und Kontakt

Siehe Kapitel 1.3.1.1 Policy Authority.

1.5.3 Zuständigkeit für die Anerkennung eines CPS

Die im Kapitel 1.3.1 unter Policy Authority benannte organisatorische Einheit ist zuständig für die Prüfung und Genehmigung des CPS jeder CA, die Zertifikate im Rahmen dieser CP ausstellt.

1.5.4 CPS-Aufnahmeverfahren

CAs, die im Rahmen dieser CP Zertifikate ausstellen, müssen die in diesem Dokument genannten Anforderungen erfüllen.

Die CA und RA müssen vor Aufnahme ihrer Tätigkeit alle Anforderungen des durch die PA genehmigten CPS umgesetzt haben.

Siehe auch Kapitel 8.

1.6 Definitionen und Abkürzungen

Siehe Kapitel 12 und 13.

2 Veröffentlichung und Informationsdienste

2.1 Informationsdienste

Jede CA innerhalb der DZ BANK AG PKI muss die in Kapitel 2.2 genannten Informationen gemäß Kapitel 2.3 und Kapitel 2.4 vorhalten.

2.2 Veröffentlichung von Informationen

Jede CA innerhalb der DZ BANK AG PKI muss folgende aktuelle Informationen veröffentlichen und die Adressen der entsprechenden Informationsdienste in ihrem CPS angeben:

- CP der DZ BANK AG PKI
- CPS der DZ BANK AG Root CA
- Zertifikat der zugehörigen DZ BANK AG Root CA und dessen Fingerabdruck
- CPS oder eine CPS-Zusammenfassung der CA
- Zertifikat der CA und dessen Fingerabdruck
- Liste der RAs, die zur CA gehören
- Verweis auf einen Verzeichnisdienst für die ausgestellten Zertifikate, sofern ein solcher betrieben wird
- Pflichten der Zertifikatnehmer

- Verweis auf den Certificate Status Service der CA und der DZ BANK AG Root CA
- Kontaktinformationen, unter denen eine Zertifikatsperrung beantragt werden kann

Darüber hinaus sollten den Zertifikatsnehmern Informationen über die DZ BANK AG PKI zur Überprüfung der Gültigkeit von Zertifikaten, über die korrekte Anwendung von Kryptographie und über die Verwendung von Zertifikaten zur Verfügung gestellt werden.

2.2.1 Veröffentlichung von Zertifikaten und Zertifikatsstatus

Siehe Kapitel 2.2, sowie Kapitel 4.9.7 bis 4.9.11 und Kapitel 4.10.

2.2.2 Veröffentlichung von CA-Informationen

Die CP der DZ BANK AG PKI muss für alle PKI-Teilnehmer verfügbar sein. Das CPS einer CA ist ein internes Dokument, das nur in einer mit der PA abgestimmten, reduzierten Form herausgegeben werden darf.

2.3 Aktualisierung von Informationen

Für die Aktualisierung der in Kapitel 2.2 genannten Informationen gelten folgende Fristen:

- Zertifikate: spätestens drei Werktage nach der Ausstellung
- CP und CPS: zum Inkrafttreten einer neuen Version (nach Ankündigung, siehe Kapitel 9.10.1)
- Liste der RAs: spätestens drei Werktage nach einer Veränderung
- CRLs: Siehe Kapitel 4.9.7.
- OCSP: analog zu CRLs (siehe Kapitel 4.9.7)

2.4 Zugriff auf Informationsdienste

Der lesende Zugriff auf alle in Abschnitt 2.2 aufgeführten Informationen, außer den CPSs-Dokumenten (siehe 2.2.2) ist allen PKI-Teilnehmern möglich. Schreibender Zugriff wird nur berechtigten Personen gewährt. Der Zugriff wird gemäß den Standard IT-Betriebsvorgaben verwaltet.

3 Identifizierung und Authentifizierung

3.1 Namen

3.1.1 Namensform

Der Name des Zertifikatnehmers (IT-System oder physische Person) wird im Feld Subject (dt. Subjekt) des Zertifikats hinterlegt.

Das Subjekt kann aus unterschiedlichen Attributen bestehen:

Attribut	Wert	Pflichtfeld?
C	<2-Zeichen-Staaten-Kürzel>	Für CAs
ST	<Bundesland>	Optional
L	<Ort>	Optional
O	<Organisation>	Für CAs
OU	<Organisationseinheit>	Optional
CN	<Eindeutiger Name>	Ja
emailAddress	<E-Mail-Adresse	Optional

Die Verkettung mehrerer Attribute ergeben einen Distinguished Name (DN).

Das Subjekt muss einen eindeutigen Namen innerhalb der DZ BANK AG im Common Name (CN) beinhalten.

CAs verwenden als Subjekt eine Kennzeichnung, aus welchem unterschiedliche Generationen von CA-Zertifikaten, weiterhin unterscheidbar sind. Darüber hinaus ist bei CAs neben dem eindeutigen Namen die Organisation „O=DZ BANK AG“ im Subjekt zu hinterlegen.

Das Subjekt bei End-Entität-Zertifikaten beinhaltet bei IT-Systemen als Zertifikatnehmer grundsätzlich im Attribut „CN“ den A-Record bzw. den „fully qualified domain name“ (**FQDN**) (dt. Vollqualifizierter Domänenname) unter dem das IT-System im Domaine Name Service (**DNS**) (dt. Domänennamenservice) abrufbar ist. Für Zertifikate, die auf Personen ausgestellt werden, sind andere eindeutige Kennzeichnungen (z.B. Email-Adresse, User Principal Name) zu verwenden.

Jede CA definiert einen eindeutigen Namensraum, der im CPS zu beschreiben ist. Sind neben dem CN weitere Attribute im Subject notwendig, so sind diese im CPS zu beschreiben. Eine CA darf bei der Ausstellung von Zertifikaten nur Subjektnamen verwenden, die in ihrem vereinbarten Namensraum liegen. Die Verantwortung für die Eindeutigkeit der Namen obliegt der ausstellenden CA.

3.1.2 Aussagekraft von Namen

Das Subjekt muss den Zertifikatnehmer eindeutig identifizieren.

Sofern weitere Attribute neben dem FQDN im Subject verwendet werden, gelten die folgenden Regelungen:

Das Attribut „C“ muss das 2-Zeichen-Staaten-Kürzel (festgelegt im ISO Standard 3166-1 ([ISO-3166-1]) des Staates enthalten, in dem die im Attribut „O“ genannte Organisation ihren Standort hat.

Falls das Attribut „ST“ angegeben wird, muss es den offiziellen Namen eines Bundeslandes enthalten. Falls das Attribut „L“ angegeben wird, muss es den offiziellen Namen eines Ortes enthalten. Das anzugebende Bundesland bzw. der anzugebende Ort muss im zugehörigen CPS spezifiziert werden.

Das Attribut „O“ muss den Namen der Organisation des Zertifikatsnehmers enthalten. Die Authentizität des Namens wird nach Kapitel 3.2.2 überprüft.

Falls das optionale Attribut „OU“ ein- oder mehrfach angegeben wird, muss es jeweils den Namen einer organisatorischen Untereinheit der im Attribut „O“ genannten Organisation enthalten. Falls

mehrere Attribute „OU“ angegeben werden, müssen diese im DN jeweils direkt hintereinander aufgeführt werden und die Reihenfolge der benannten organisatorischen Untereinheiten sollte von größeren zu kleineren Untereinheiten absteigen.

Das Subject enthält mindestens ein Attribut „CN“. Jedes Attribut „CN“ muss eine angemessene Darstellung des Namens des Zertifikatsnehmers enthalten. Anhand des CN muss eindeutig der Zertifikatsnehmer bestimmbar sein. Sofern der Zertifikatsnehmer keine natürliche Person ist, muss ein entsprechender Ansprechpartner indirekt (z.B. per Configuration Management Database (**CMDB**)) ableitbar sein.

Zertifikate, die Host Namen mit Wildcards (z.B. „*.dzbank-anwendung.vrnet“) enthalten, sind nicht zulässig. Ausnahmen müssen durch die PA genehmigt werden.

Falls das optionale Attribut „emailAddress“ ein- oder mehrfach angegeben wird, muss es jeweils eine nach RFC 822 ([RFC822] & Crocker, 1982) formatierte E-Mail-Adresse enthalten. Die E-Mail-Adresse muss dem Zertifikatnehmer zugeordnet sein oder Zertifikatnehmer müssen vom Besitzer der E-Mail-Adresse autorisiert sein, diese zu nutzen. Falls mehrere Attribute „emailAddress“ angegeben werden, müssen diese im DN jeweils direkt hintereinander aufgeführt werden.

Für E-Mail-Adressen, IP-Adressen und Domain-Namen, die in die Zertifikaterweiterung für alternative Zertifikatnamen („subjectAlternativeName“) unter den Typen „rfc822Name“, „iPAddress“ bzw. „dNSName“ aufgenommen werden, gelten obige Regelungen analog. Ist ein Attributwert länger als durch den jeweiligen Standard erlaubt, so muss stattdessen eine angemessene, wenn möglich wohlbekannte und eingeführte Abkürzung verwendet werden.

3.1.3 Anonymität oder Pseudoanonymität von Zertifikatsnehmern

Für natürliche Personen kann anstelle des Namens im Zertifikat ein Pseudonym aufgeführt werden. Dieses muss im Attribut „CN“ eindeutig kenntlich gemacht werden (siehe Kapitel 3.1.2).

Das Pseudonym ist dem Zertifikatnehmer (authentifiziert nach Kapitel 3.2.3) eindeutig zugeordnet. Dies ist in den bei der Beantragung des Zertifikats anfallenden Unterlagen in einer Art zu dokumentieren, dass jederzeit die Zuordnung nachvollziehbar ist (z.B. im Falle eines internen oder externen Audits). Das Pseudonym kann somit auf die reale Identität des Zertifikatsnehmers zurückgeführt werden.

Anonyme Zertifikate dürfen nicht ausgestellt werden.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

In den DN-Attributen „O“, „OU“ und „CN“ dürfen ausschließlich die folgenden Zeichen verwendet werden:

a-z A-Z 0-9 ' ( ) + , - . / : = ? Leerzeichen

Für die Ersetzung deutscher Sonderzeichen gelten folgende Substitutionsregeln:

Ä -> Ae, Ö ->Oe, Ü -> Ue, ä -> ae, ö -> oe, ü -> ue, ß -> ss

Sonderzeichen mit Akzenten verlieren diese. Ansonsten wird eine für das betreffende Zeichen gemeinhin verwendete Schreibweise aus den Zeichen a-z und A-Z so zusammengesetzt, dass der entsprechende Laut entsteht.

Die oben genannten Regeln zur Interpretation gelten auch für die Subject Alternative Names (**SAN**) (dt. Subjekt alternativer Name).

3.1.5 Eindeutigkeit von Namen

Vor der Zertifizierung muss die Korrektheit und Eindeutigkeit des angegebenen Namens von RA/TA der jeweiligen CA überprüft werden. Das Subject eines Zertifikatsnehmers muss eindeutig sein und darf nicht mehrfach an unterschiedliche Zertifikatnehmer vergeben werden.

Bei Namensgleichheit gilt grundsätzlich das Prinzip: „Wer zuerst kommt, wird zuerst bedient“. In Streitfällen entscheidet die RA/TA der jeweiligen CA. Die Eindeutigkeit des Subjects kann durch die Verwendung von „OU“, „UID“ oder „SER“ Attributen oder durch die Verwendung von Pseudonymen im Attribut „CN“ wie z. B. „PN: Max Mustermann 2“ erreicht werden.

3.1.6 Erkennung, Authentifizierung und Funktion von Warenzeichen

Sofern sich der Subject eines Zertifikats auf eine natürliche Person bezieht, ist eine Anerkennung von Warenzeichen o. ä. nicht relevant. In allen anderen Fällen liegt es in der alleinigen Verantwortung des Zertifikatnehmers, dass die Namenswahl keine Warenzeichen o. ä. verletzt. Die CAs der DZ BANK AG PKI sind nicht verpflichtet, solche Rechte zu überprüfen. Falls eine CA über eine Verletzung solcher Rechte informiert wird, muss sie das Zertifikat sperren.

3.2 Identitätsüberprüfung bei Neuantrag

3.2.1 Verfahren zur Überprüfung des Besitzes des privaten Schlüssels

Bei Antragsstellung ist nachzuweisen, dass der zukünftige Zertifikatinhaber im Besitz des privaten Schlüssels ist. Detaillierte Regelungen sind in den entsprechenden CPS zu treffen. Bei Systemen, die keine Schlüsselgenerierung und Erstellung eines Zertifikatsantrags unterstützen, entfällt dieser Punkt.

3.2.2 Authentifizierung einer Organisation

Sofern eine Organisation hinzugefügt wird, ist vor Ausstellung eines Zertifikats zu prüfen, ob der Zertifikatnehmer dieser Organisation angehörig und berechtigt ist. Details sind im CPS zu beschreiben.

3.2.3 Authentifizierung einer Entität

3.2.3.1 Authentifizierung einer natürlichen Person

Die Authentifizierung der Identität einer natürlichen Person muss durch die ausstellende Issuing CA bzw. deren RA/TA geprüft werden. Gültige Mechanismen stellt die Prüfung eines amtlichen Lichtbildausweises oder den Nachweis durch eine erfolgreiche technische Authentifizierung (z.B. Windows-Passwort) durch die natürliche Person. Detaillierte Anforderungen an die Authentifizierung und Prüfung sind in dem entsprechenden CPS festzulegen.

3.2.3.2 Authentifizierung von Geräten

Zu authentifizierende Geräte müssen eine eindeutige Registrierungsinformation zur Verfügung stellen. Diese Information muss in einer zentralen Ursprungsdatenquelle (z.B. CMDB) überprüft werden können.

3.2.3.3 Authentifizierung von Anwendungen oder Diensten

Zu authentifizierende Anwendungen oder Dienste müssen eine eindeutige Registrierungsinformation zur Verfügung stellen. Diese Information muss in einer zentralen Ursprungsdatenquelle (z.B. CMDB bzw. RSA Archer IT-Asset ID) überprüft werden können.

3.2.3.4 Authentifizierung für Rollen-Zertifikate

Ein geeigneter Nachweis der Rollenzugehörigkeit ist erforderlich. Detaillierte Regelungen sind in dem entsprechenden CPS zu treffen.

3.2.3.5 Authentifizierung für Code-Signatur-Zertifikate

Ein Nachweis, dass die Berechtigung zur Signatur von Software vorliegt, ist erforderlich. Detaillierte Regelungen sind in den entsprechenden CPS zu treffen.

3.2.4 Nicht überprüfte Informationen

Jegliche Information, die nicht über das Zertifikats-Template vorgegeben ist, ist zu prüfen.

Die entsprechenden Prüfverfahren sind im CPS zu dokumentieren.

3.2.5 Handlungsvollmacht

Abhängig vom Schutzbedarf für den jeweiligen Zertifikatstyp kann der zukünftige Zertifikatsinhaber eine Vollmacht zur Beantragung des Zertifikats erteilen. In diesem Fall ist sowohl die Gültigkeit der Vollmacht als auch die Authentizität des Bevollmächtigten (auf die gleiche Weise wie die Authentizität des zukünftigen Zertifikatsinhabers geprüft werden würde) zu prüfen. Detaillierte Regelungen sind in den entsprechenden CPS zu treffen.

3.2.6 Cross-Zertifizierungs-Kriterien für die Interoperabilität

Die Möglichkeit der Cross-Zertifizierung besteht ausschließlich für die DZ BANK AG Root CA.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

Eine Zertifikatserneuerung bedeutet, dass ein bestehendes Zertifikat mit einem späteren Ablaufdatum und einem neuen öffentlichen Schlüssel, basierend auf einem neu generierten Schlüsselpaar, ausgestellt wird.

Ist es notwendig weitere Attribute (z.B. Subject) neben der Laufzeit und dem öffentlichen Schlüssel anzupassen, so handelt es sich nicht um eine Zertifikatserneuerung im Sinne dieser CP.

3.3.1 Routinemäßige Zertifikatserneuerung

Für jede Zertifikaterneuerung eines End-Entität-Zertifikats kann die Identität durch den Nachweis festgestellt werden, dass die Entität im Besitz des privaten Schlüssels ist, der dem öffentlichen Schlüssel des noch gültigen Zertifikats zugeordnet ist. Das genutzte Zertifikat darf weder abgelaufen noch gesperrt sein.

Bei der routinemäßigen Zertifikatserneuerung eines End-Entität-Zertifikats ist neben den Methoden aus Kapitel 3.2.3 zusätzlich in Abhängigkeit vom Schutzbedarf die Authentifizierung der Identität durch ein gültiges persönliches Zertifikat aus der DZ BANK AG PKI zulässig. Falls dies zutrifft, sind die Details im entsprechenden CPS zu regeln.

3.3.2 Zertifikatserneuerung nach einer Sperrung

Nach dem Sperren eines Zertifikats kann eine Authentifizierung nicht mehr mit dem gesperrten Zertifikat durchgeführt werden.

Im Falle einer Zertifikatsperrung kann nur ein neues Zertifikat erteilt werden. Das Ausstellen eines neuen Zertifikats muss immer voraussetzen, dass der Zertifikatnehmer den in Kapitel 3.2 genannten Registrierungsprozess durchläuft.

3.4 Identifizierung und Authentifizierung bei einer Sperrung

Die Authentifizierung einer Sperrung kann auf die folgenden Arten erfolgen (siehe auch Kapitel 4.9.2):

- Übermittlung einer vorher vereinbarten Authentisierungsinformation (schriftlich, per Telefon, oder elektronisch).
- Übergabe eines Sperrantrags mit einer geeigneten elektronischen Signatur, die den Zertifikatnehmer bzw. eine andere zur Beantragung der Sperrung berechtigte Entität authentifiziert
- Übergabe eines Sperrantrags mit einer handschriftlichen Unterschrift

Detaillierte Informationen finden sich in den entsprechenden CPS.

4 Betriebsanforderungen im Zertifikats-Lebenszyklus

4.1 Zertifikatsantrag

Die Beantragung eines CA-Zertifikats (Root und Issuing CA) ist in Form eines Logbuchs und handschriftlicher Unterschrift durch mindestens zwei Genehmiger (Root CA: PA + TAM, Issuing CA: TAM + CA Manager) zu dokumentieren. Hierbei sind der Zertifikatsantrag sowie das ausgestellte Zertifikat in Textform zu hinterlegen.

Zertifikatsanträge für End-Entität-Zertifikats sind nur zulässig über die folgenden Verfahren:

- Beantragung über eine automatisierte Schnittstelle
- Beantragung über ein von der CA bereitgestelltes Formular im Intranet

Ein Zertifikatsantrag ist immer basierend auf einem neu generierten Schlüsselpaar zu stellen. Das Schlüsselpaar sollte auf dem IT-System generiert werden für welches auch das Zertifikat ausgestellt wird.

Der Zertifikatbeantragungsprozess muss genügend Information zur Verfügung stellen um:

- Prüfen zu können, dass der Antragsteller autorisiert ist (für die Organisation oder die Auftrag gebende Organisation), ein Zertifikat zu beantragen (siehe Kapitel 3.2.3).
- Die Feststellung und Dokumentation der Antragssteller-Identität.
- Den Erhalt des öffentlichen Schlüssels des Antragstellers und Überprüfung, dass der Antragsteller im Besitz des privaten Schlüssels für jedes Zertifikat der Beantragung ist (siehe Kapitel 3.2.1). Hiervon ausgenommen sind Anträge bei denen die Schlüssel serverseitig, aus

technischen oder regulatorischen Gründen (z.B. Key Escrow), generiert werden.
- Prüfung von Autorisierungs- oder Rollen-Informationen, die zur Aufnahme in das Zertifikat angegeben wurden.

Diese Schritte können in beliebiger Reihenfolge durch die RA und den Antragsteller durchgeführt werden, jedoch müssen vor der Zertifikatserstellung alle Schritte erfüllt sein.

4.1.1 Wer kann ein Zertifikat beantragen?

In der DZ BANK AG PKI können Zertifikatnehmer gemäß Kapitel 1.3.4 Zertifikate beantragen. Hierfür muss für ein Zertifikat für eine natürliche Person deren Autorisierung beim Teilnehmer vorliegen.

4.1.2 Registrierungsprozess und Zuständigkeiten

Vor Ausstellung eines Zertifikats ist ein angemessener Registrierungsprozess zu durchlaufen.

Im Registrierungsprozess müssen die folgenden Arbeitsschritte durchlaufen und dokumentiert werden:

- Prüfung des Zertifikatsantrags hinsichtlich Vollständigkeit und Korrektheit
- Prüfung, ob für das Subjekt (CN) maximal ein weiteres Zertifikat (im Fall der Erneuerung) existiert.
- Prüfung aller Attribute, die nicht durch das Zertifikats-Template von der CA gesetzt werden.
- Prüfung auf die maximale zulässige Anzahl von 10 Subject Alternative Names (**SAN**)
- Prüfung des beantragten Subjekts (CN) nach Kapitel 3.1.2 und 3.1.5
- Prüfung des Vorliegens einer Authentifizierung der Identität des Zertifikatnehmers nach Kapitel 3.2.3
- Prüfung der Authentifizierung einer Organisation nach Kapitel 3.2.2
- Überprüfung des Besitzes des privaten Schlüssels nach Kapitel 3.2.1 (außer bei CA-seitig generierten Schlüsseln)
- Bestätigung der Authentizität des Zertifikatantrags durch Prüfung der Freigabe des Antrags durch eine bevollmächtigte Person, siehe Kapitel 3.2.5

Angefallene Papierunterlagen müssen archiviert und in einem verschlossenen Schrank aufbewahrt werden. Angefallene digitale Unterlagen müssen archiviert und vor unbefugtem Zugriff geschützt aufbewahrt werden.

Die Übermittlung der für die Zertifizierung notwendigen Informationen an die CA erfolgt integritätsgeschützt und in authentisierter Form.

4.2 Verarbeitung des Zertifikatsantrags

Informationen, die in der Zertifikatbeantragung enthalten sind, müssen vor der Erteilung eines Zertifikats geprüft und richtig sein.

Verfahren zur Gültigkeitsprüfung der im Zertifikats-Beantragungsformular enthaltenen Information müssen im CPS spezifiziert sein.

4.2.1 Durchführung der Identifizierung und Authentifizierung

Die Identifizierung und Authentifizierung von Zertifikatsnehmern wird gemäß Kapitel 3.2 durchgeführt. Die RAs, die verantwortlich für die Authentifizierung der Zertifikatsnehmer-Identität sind, müssen in jedem Fall in den entsprechenden CPS spezifiziert werden.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Ein Zertifikatantrag kann von der zuständigen RA akzeptiert werden, wenn alle Arbeitsschritte gemäß Kapitel 4.1.2 erfolgreich durchlaufen wurden. Andernfalls wird der Zertifikatantrag abgewiesen und dies dem Antragsteller unter Angabe von Gründen mitgeteilt. Trotz Erfüllung der formalen Voraussetzungen besteht kein Anspruch auf Erteilung eines Zertifikats.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Die Bearbeitungsdauer eines Zertifikatantrags muss im entsprechenden CPS spezifiziert werden.

4.3 Zertifikatsausgabe

4.3.1 Aktionen der Zertifizierungsstelle (CA) während der Zertifikatsausgabe

Die formalen Voraussetzungen für die Ausstellung eines Zertifikats werden durch die zugeordnete RA in angemessener Weise überprüft. Insbesondere überprüft sie die Berechtigung des Zertifikatsnehmers, ein Zertifikat für den im Subject sowie SANs angegebenen Namen zu erhalten. Hierzu ist insbesondere bei Zertifikaten für IT-Systeme das Vorhandensein eines freigebenden IT-Änderungsantrags („IT-Change“) zu verifizieren. Der IT-Change selbst muss mindestens eine Freigabe durch Vieraugenprinzip erfüllen. Die für das IT-System/Service technisch und fachlich Verantwortlichen müssen explizit im Rahmen der Change-Freigabe der Ausstellung des Zertifikats zustimmen. Die Verantwortung zur Verifizierung von möglichen Zertifikatsnehmer-Informationen muss in den entsprechenden CPS spezifiziert werden.

Sind alle Voraussetzungen erfüllt, erstellt die CA ein Zertifikat entsprechend dem Antrag.

4.3.2 Benachrichtigung des Zertifikatsnehmers nach der Zertifikatsausgabe

Nach der Zertifikatausstellung wird dem Zertifikatsnehmer das ausgestellte Zertifikat sicher übermittelt oder der Zertifikatsnehmer wird über dessen Ausstellung und Ablageort informiert.

4.4 Zertifikatsannahme

Der Zertifikatsnehmer ist verpflichtet, die Korrektheit des eigenen Zertifikats sowie des Zertifikats der ausstellenden CA nach Erhalt zu verifizieren.

4.4.1 Annahme eines Zertifikats

Die Annahme eines Zertifikats erfolgt mit der Nutzung des Zertifikats oder wenn innerhalb von 14 Tagen nach Erhalt kein Widerspruch erfolgt.

4.4.2 Veröffentlichung eines Zertifikats durch die CA

Ausgestellte CA Zertifikate müssen veröffentlicht werden (siehe auch Kapitel 2.1). Alle übrigen Zertifikate können veröffentlicht werden.

4.4.3 Benachrichtigung weiterer Instanzen

Die unter Kapitel 1.3.1 genannten PKI Verwaltungsautoritäten (PA und TAM) müssen über die Ausstellung eines Zertifikates für eine untergeordnete CA durch eine unter dieser CP arbeitenden CA benachrichtigt werden.

Eine Benachrichtigung weiterer Instanzen ist nicht erforderlich.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Der zulässige Umfang der Verwendung eines privaten Schlüssels muss im Zertifikat durch Zertifikatserweiterungen, inklusive der keyUsage (dt. Schlüsselverwendung) und deren extendedKeyUsage (dt. erweiterte Schlüsselverwendung), spezifiziert werden.

Private Schlüssel müssen angemessen vor Zugriff und unautorisierter Nutzung geschützt werden. Zertifikate dürfen ausschließlich in Übereinstimmung mit dieser CP und dem entsprechenden CPS eingesetzt werden.

4.5.2 Verwendung des öffentlichen Schlüssels und Zertifikats durch Relying Parties

Relying Parties dürfen Zertifikate aus der DZ BANK AG PKI nur verwenden, wenn diese ein dem Anwendungskontext angemessenes Sicherheitsniveau haben. Darüber hinaus sind Relying Parties verpflichtet, sicherzustellen, dass das verwendete Zertifikat korrekt und gültig ist. Dies beinhaltet eine Prüfung des Zertifikats auf Sperrung, sowie eine Prüfung der Signatur des Zertifikats, sowie der Attribute keyUsage und der Erweiterung extendedKeyUsage. Hierbei muss die Zertifikatskette bis zu einer vertrauenswürdigen Instanz geprüft werden. Die vertrauenswürdige Instanz ist im CPS zu spezifizieren.

4.6 Zertifikatserneuerung ohne Schlüsselwechsel

Eine Zertifikatserneuerung auf Basis des bestehenden Schlüsselpaares ist nicht zugelassen. Bei jeder Zertifikatserneuerung wird immer ein neues Schlüsselpaar generiert.

4.6.1 Gründe für eine Zertifikatserneuerung ohne Schlüsselwechsel

Eine Zertifikatserneuerung ohne Schlüsselwechsel ist nicht zulässig.

4.6.2 Wer darf eine Zertifikatserneuerung ohne Schlüsselwechsel beantragen

Nicht zulässig.

4.6.3 Ablauf der Zertifikatserneuerung ohne Schlüsselwechsel

Nicht zulässig.

4.6.4 Benachrichtigung des Zertifikatsnehmers

Nicht zulässig.

4.6.5 Annahme einer Zertifikatserneuerung

Nicht zulässig.

4.6.6 Veröffentlichung einer Zertifikatserneuerung durch die CA

Nicht zulässig.

4.6.7 Benachrichtigung weiterer Instanzen über die Zertifikatserneuerung

Nicht zulässig.

4.7 Zertifikatserneuerung mit Schlüsselwechsel (Re-Key)

Bei einer Zertifikaterneuerung mit Schlüsselwechsel wird einem Zertifikatsnehmer, der bereits ein Zertifikat besitzt, durch die zuständige CA ein neues Zertifikat für ein neues Schlüsselpaar ausgestellt, sofern die im Zertifikat enthaltenen Informationen (ausgenommen Seriennummer, Gültigkeit, Public Key, ggf. CDPs, AIAs der Issuing CA) unverändert bleiben. Daher müssen die Informationen des Zertifikatnehmers, die ins Zertifikat eingetragen werden, nicht erneut überprüft werden.

Folgende Felder müssen mit einem geänderten Wert belegt werden:

- public key

Folgende Felder dürfen verändert werden:

- Gültigkeit

Die restlichen Attribute, die nicht automatisch durch das Template der CA gesetzt werden, müssen so wie im zu erneuernden Zertifikat belegt sein.

CA-Zertifikate können nicht erneuert werden, da diese bei einer Neuausstellung ein neues Subject bekommen. Für CA-Zertifikate muss immer gemäß des Prozess einer Neu-Beantragung vorgegangen werden.

4.7.1 Gründe für eine Zertifikatserneuerung mit Schlüsselwechsel

Die folgenden Gründe führen u.a. zu einer Zertifikatserneuerung mit Schlüsselwechsel:

- Routinemäßige Zertifikatserneuerung

4.7.2 Wer darf eine Zertifikatserneuerung mit Schlüsselwechsel beantragen?

Eine Zertifikatserneuerung wird grundsätzlich durch den Zertifikatsnehmer oder eine explizit hierzu autorisierte Entität beantragt. Eine in dieser Weise autorisierte Entität kann sich zur Erfüllung ihrer Aufgaben technisch automatisierter Prozesse bedienen.

Falls außerplanmäßig die Erneuerung von Zertifikaten erforderlich sein sollte (z.B. aus Sicherheitsgründen hinsichtlich Schlüssellänge, Gültigkeitsdauer oder Zertifikatsstruktur), ist dieser Prozess zentral durch autorisierte Mitarbeiter der DZ BANK AG PKI anzustoßen. Hierbei müssen die betroffenen Entitäten in angemessener Weise informiert werden. Dieser Prozess ist im Detail im CPS zu spezifizieren.

4.7.3 Ablauf der Zertifikatserneuerung mit Schlüsselwechsel

Der Ablauf der Zertifikaterneuerung entspricht den Regelungen für Erstanträge unter Kapitel 4.3, für die Identifizierung und Authentifizierung gelten die Regelungen gemäß Kapitel 3.3.1.

Die Authentisierung des Antrags kann zusätzlich zu den dort beschriebenen Verfahren auch durch Signatur mit dem zu erneuernden Zertifikat erfolgen, sofern dieses zum Zeitpunkt der Antragsstellung gültig ist. Bei einem vollautomatisierten Verfahren zur Erneuerung eines Zertifikats muss das initiale Enrollment des Zertifikats mit einem IT-Change gemäß 4.3.1 autorisiert sein.

Mit Ausnahme von CA-Zertifikaten muss nach Erneuerung und Nutzung des neu erstellten Zertifikats das alte noch gültige Zertifikat gesperrt werden, sofern die Restgültigkeit 8 Wochen überschreitet.

4.7.4 Benachrichtigung des Zertifikatsnehmers

Es gelten die Regelungen gemäß Kapitel 4.3.2.

4.7.5 Annahme einer Zertifikatserneuerung mit Schlüsselwechsel

Es gelten die Regelungen gemäß Kapitel 4.4.1.

4.7.6 Veröffentlichung einer Zertifikatserneuerung durch die CA

Es gelten die Regelungen gemäß Kapitel 4.4.2.

4.7.7 Benachrichtigung weiterer Instanzen über die Zertifikatserneuerung

Es gelten die Regelungen gemäß Kapitel 4.4.3.

4.8 Zertifikatsmodifizierung

Nicht zulässig.

4.8.1 Gründe für eine Zertifikatsmodifizierung

Nicht zulässig.

4.8.2 Wer kann eine Zertifikatsmodifikation beantragen?

Nicht zulässig.

4.8.3 Ablauf der Zertifikatsmodifikation

Nicht zulässig.

4.8.4 Benachrichtigung des Zertifikatsnehmers

Nicht zulässig.

4.8.5 Annahme einer Zertifikatsmodifikation

Nicht zulässig.

4.8.6 Veröffentlichung einer Zertifikatsmodifikation durch die CA

Nicht zulässig.

4.8.7 Benachrichtigung weiterer Instanzen über die Zertifikatsmodifikation

Nicht zulässig.

4.9 Sperrung und Suspendierung von Zertifikaten

Kontaktinformationen für Sperranträge sind online zu veröffentlichen. Diese Informationen müssen für alle Teilnehmer erreichbar sein. Details sind im CPS zu spezifizieren.

Notfälle, bei denen Zertifikate der DZ BANK AG PKI missbräuchlich oder betrügerisch verwendet werden, können 24x7 telefonisch, elektronisch oder per Fax gemeldet werden. Innerhalb von 24 Stunden nach Eingang muss mit der Behandlung der Meldung (d.h. Prüfung des Sperrrequests und Bestätigung oder Ablehnung) begonnen werden.

Die Sperrung eines Zertifikats kann nicht rückgängig gemacht werden.

4.9.1 Gründe für eine Sperrung

Ein Zertifikat muss gesperrt werden, wenn mindestens einer der folgenden Gründe vorliegt:

- Die im Zertifikat enthaltenen Angaben sind nicht oder nicht mehr gültig
- Die kryptografischen Merkmale des Zertifikats entsprechen nicht mehr dem Stand der Technik und werden als Risiko für Relying Parties eingestuft.
- Der private Schlüssel wurde kompromittiert.
- Der Zertifikatnehmer ist nicht mehr berechtigt, das Zertifikat zu nutzen (siehe Kapitel 1.3.4).
- Der Zertifikatnehmer bzw. das IT-System benötigt das Zertifikat nicht mehr (Dekomissionierung des IT-Systems, Mitarbeiter verlässt das Unternehmen).
- Die Nutzung des Zertifikats verstößt gegen die CP oder CPS.
- Die ausstellende CA stellt den Zertifizierungsbetrieb ein. In diesem Fall werden sämtliche von der CA ausgestellten Zertifikate gesperrt.
- Der private Schlüssel der ausstellenden oder einer übergeordneten CA wird kompromittiert. In diesem Fall werden sämtliche von diesen CAs ausgestellte Zertifikate gesperrt.

4.9.2 Wer kann eine Sperrung beantragen?

Die Sperrung eines Zertifikats kann vom Zertifikatnehmer, RA oder berechtigten Dritten beantragt werden.

Personen, die die Identität bzw. Berechtigung eines Zertifikatnehmers bei der Beantragung des Zertifikats bestätigt haben, können ebenfalls jederzeit die Sperrung beantragen, wenn der Zertifikatsnehmer nicht mehr berechtigt ist, das Zertifikat zu nutzen.

4.9.3 Ablauf einer Sperrung

Zertifikatnehmer, RA oder Dritte können einen Sperrantrag nur mit Angabe von Gründen (siehe Kapitel 4.9.1) stellen.

Die Sperrung eines Zertifikats kann folgendermaßen beantragt werden:

- Elektronisch
- Telefonisch
- Schriftlich

- Per Fax

Antragssteller für eine Zertifikatssperrung müssen sich gegenüber der ausstellenden CA authentifizieren. Die möglichen Verfahren sind in Kapitel 3.4 dargestellt.

Die RA führt eine Prüfung der angegebenen Sperrgründe durch.

Liegt einer der in Kapitel 4.9.1 genannten Gründe vor, führt die RA Sperrung nach Rücksprache mit dem Zertifikatnehmer oder einen dazu explizit autorisierten Delegierten durch.

Vor der Sperrung einer CA werden die Auswirkungen auf alle Zertifikatsnehmer geprüft.

Die Sperrung einer CA ist nur nach Einholung einer Genehmigung per Email oder Schriftdokument bei der Policy Authority möglich.

Nach erfolgter Sperrung werden Teilnehmer und ggf. Zertifikatnehmer darüber elektronisch informiert. Die Sperrinformation muss mindestens bis zum Ablaufdatum des gesperrten Zertifikats über die Sperrdienste verfügbar gemacht werden.

Der Zertifikatsperrprozess ist im Detail im entsprechenden CPS zu spezifizieren.

4.9.4 Fristen für den Zertifikatsnehmer

Der Zertifikatsnehmer ist verpflichtet, bei bekannt werden eines Sperrgrunds (siehe Kapitel 4.9.1) unverzüglich die Sperrung des Zertifikats zu beantragen.

4.9.5 Fristen für eine CA

Eine CA muss eine Zertifikatsperrung unverzüglich vornehmen, wenn die Voraussetzungen dafür gegeben sind (siehe Kapitel 4.9.3).

4.9.6 Anforderungen zu Sperrprüfungen durch Relying Parties

Relying Parties müssen zur Prüfung der Gültigkeit von Zertifikaten aktuelle Sperrinformationen verwenden. Diese beinhalten mindestens:

- Gültigkeitsprüfung der Zertifikatlaufzeit
- keyUsage
- Common Name bzw. SAN

Details sind im entsprechenden CPS zu spezifizieren.

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

CRLs müssen in regelmäßigen Abständen (diese sind im entsprechenden CPS zu definieren) herausgegeben werden, auch wenn diese Listen keine Änderungen beinhalten.

On-Line CAs, die CRLs ausstellen, müssen diese mindestens einmal alle 24 Stunden herausgeben. Der Inhalt des Feldes „nextUpdate“ darf nicht später als 96 Stunden nach der Ausgabezeit („thisUpdate“) sein.

Off-Line CAs müssen entsprechend ihres Schutzbedarfs regelmäßig CRLs ausstellen. Details, inklusive der genauen Fristen, sind im entsprechenden CPS zu spezifizieren.

Bei Sperrung eines Zertifikats muss die ausstellende CA unverzügliche eine neue CRL veröffentlichen, spätestens jedoch 24 Stunden nach der erfolgten Sperrung. Dies gilt sowohl für CRLs ausgestellt durch die Root CA als auch für da runter ausgestellte CAs.

Umstände im Zusammenhang mit einer Notfall-CRL-Ausstellung sind in Kapitel 4.9.12 beschrieben.

4.9.8 Maximale Latenzzeit für CRLs

Nach Erzeugung neuer CRLs sollten diese umgehend, spätestens jedoch nach 24 Stunden, veröffentlicht werden.

4.9.9 Online Sperr- und Statusüberprüfung von Zertifikaten

Eine CA kann einen OCSP Dienst zur Verfügung stellen. Details sind im entsprechenden CPS zu spezifizieren.

4.9.10 Anforderungen an Online Sperr- und Statusüberprüfungsverfahren

Der Schutz des privaten Schlüssels für den OCSP-Responder hat dem Schutz eines CA-Schlüssels zu entsprechen.

Es gelten die Anforderungen zum Schutz des privaten Schlüssels gemäß Abschnitt 6.2.

Die Korrektheit der durch die CA bereitgestellten Sperr- bzw. Statusinformationen über Zertifikate wird durch die allgemeinen Sicherheitsmechanismen der DZ BANK AG PKI (siehe Kapitel 5 und 6 sowie das entsprechende CPS) sichergestellt. Auf dem Transportweg sind die Sperr- bzw. Statusinformationen durch elektronische Signaturen gegen Manipulation geschützt (siehe Kapitel 7.2 und 7.3).

Einträge zu gesperrten Zertifikaten werden nicht vor Ablauf des ursprünglichen Gültigkeitszeitraums des betroffenen Zertifikats aus der CRL oder dem OCSP-Dienst entfernt.

4.9.11 Andere Formen der Anzeige von Sperrinformationen

Nichtzutreffend.

4.9.12 Kompromittierung von privaten Schlüsseln

Keine zusätzlichen oder abweichenden Bestimmungen/Anforderungen zu Kapitel 4.9.1

4.9.13 Gründe für eine Suspendierung

Eine temporäre Sperrung bzw. Suspendierung von Zertifikaten ist nicht erlaubt. Einmal gesperrte Zertifikate können nicht reaktiviert werden.

4.9.14 Wer kann eine Suspendierung beantragen?

Nichtzutreffend.

4.9.15 Ablauf einer Suspendierung

Nichtzutreffend.

4.9.16 Dauer einer Suspendierung

Nichtzutreffend.

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

Eine CA kann einen OCSP Dienst zur Verfügung stellen. Details sind ggf. im entsprechenden CPS zu spezifizieren.

Zertifikate, für die OCSP angeboten wird, müssen einen Verweis auf diesen Dienst beinhalten. Der OCSP-Dienst erteilt für alle gültigen, ausgestellten Zertifikat der jeweiligen CA eine Antwort. Der OCSP-Dienst gibt für nicht ausgestellte Zertifikate eine negative Auskunft.

4.11 Beendigung der Zertifikatsnutzung durch den Zertifikatsnehmer

Eine Beendigung der Zertifikatnutzung durch den Zertifikatnehmer erfolgt entweder durch die Sperrung des Zertifikats oder mit Ablauf der Gültigkeitsdauer. Abgelaufene Zertifikate dürfen nicht mehr durch den Zertifikatnehmer verwendet werden.

4.12 Schlüsselhinterlegung (Key Escrow) und –wiederherstellung

4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und –wiederherstellung

Es ist eine Escrow-Möglichkeit für kryptographische Schlüssel vorzusehen, die zur dauerhaften Verschlüsselung von Nutzdaten verwendet werden.

Eine Escrow-Möglichkeit für kryptographische Schlüssel, die nicht zur dauerhaften Verschlüsselung von Nutzdaten verwendet werden, ist nicht erlaubt.

Der Zugriff auf Escrow-Schlüssel ist nur im 4-Augen-Prinzip zu erlauben. Weitere Details u.a. Ablauf eines Zugriffs auf Escrow-Schlüssel bzw. per escrow entschlüsselte Daten sind im entsprechenden CPS zu spezifizieren.

4.12.2 Richtlinien und Praktiken zum Schutz von Sitzungsschlüsseln und deren Wiederherstellung

Nichtzutreffend.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Die infrastrukturellen Sicherheitsmaßnahmen sind gemäß dem Schutzbedarf für alle CAs im zugehörigen CPS zu spezifizieren. Es gelten die Vorgaben der DZ BANK AG.

5.1.1 Lage und Konstruktion

Siehe Kapitel 5.1.

5.1.2 Zugangskontrolle

Siehe Kapitel 5.1.

5.1.2.1 Zutrittskontrolle auf CA-Ausrüstung

Siehe Kapitel 5.1.

5.1.2.2 Zutrittskontrolle auf RA-Ausrüstung

Siehe Kapitel 5.1.

5.1.2.3 Zutrittskontrolle auf CSS-Ausrüstung

Siehe Kapitel 5.1.

5.1.3 Stromversorgung und Klimatisierung

Siehe Kapitel 5.1.

5.1.4 Abwehr von Wasserschäden

Siehe Kapitel 5.1.

5.1.5 Feuer

Siehe Kapitel 5.1.

5.1.6 Lagerung der Datenträger

Siehe Kapitel 5.1.

5.1.7 Abfallentsorgung

Siehe Kapitel 5.1.

5.1.8 Externes Backup

Siehe Kapitel 5.1.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Sicherheitsrelevante Rollen

Nachfolgend sind die sicherheitsrelevanten Rollen definiert, die im Rahmen des Zertifizierungsprozesses erforderlich sind. Um einen ordnungsgemäßen und revisionssicheren Betrieb einer CA zu gewährleisten, muss eine entsprechende Aufgabenverteilung und Funktionstrennung vorgenommen werden. Es ist möglich, eine Rolle auf mehrere Mitarbeiter zu verteilen. Ebenso kann ein Mitarbeiter in mehr als einer Rolle auftreten, dabei sind die Rollenunverträglichkeiten aus Abschnitt 5.2.4 zu beachten. Die Zuweisung von Entitäten zu Rollen (außer PA und TAM) ist im zugehörigen CPS zu spezifizieren.

Erweiterungen am Rollenmodell sind möglich, müssen aber im jeweiligen CPS beschrieben werden.

5.2.1.1 Policy Authority (PA)

Rolle	Aufgaben der Rolle	Kürzel
Policy Authority	• Kenntnis oder Besitz einer Hälfte des Zugriffsmechanismus (z.B. Smartcard) zum privaten Schlüssel der DZ BANK AG Root CA	PA

Tabelle 1: Policy Authority (PA)

Siehe auch Kapitel 1.3.1.1.

5.2.1.2 Trust Anchor Manager (TAM)

Rolle	Aufgaben der Rolle	Kürzel
Trust Anchor Manager	• Ansprechpartner für sicherheitsrelevante Fragen • Zuordnung von Personen zu Rollen und Berechtigungen • Kenntnis oder Besitz einer Hälfte des Zugriffsmechanismus (z.B. Smartcard) zum privaten Schlüssel der DZ BANK AG Root CA • Kenntnis oder Besitz einer Hälfte des Zugriffsmechanismus (z.B. Smartcard) zum privaten Schlüssel jeder untergeordneten DZ BANK AG verwalteten CA	TAM

Tabelle 2: Trust Anchor Manager (TAM)

Siehe auch Kapitel 1.3.1.2.

5.2.1.3 System- und Netzwerkadministrator (SA)

Es gelten die Anforderungen gemäß der Rollenbeschreibung des internen IT-Betriebs.

5.2.1.4 Systemoperator (SO)

Es gelten die Anforderungen gemäß der Rollenbeschreibung des internen IT-Betriebs.

5.2.1.5 CA-Manager (CAM)

Rolle	Aufgaben der Rolle	Kürzel
CA-Manager	• Erstellung und Pflege des zugehörigen CPS • Kenntnis oder Besitz einer Hälfte des Zugriffsmechanismus (z.B. Smartcard) zum privaten Schlüssel der DZ BANK AG verwalteten CA	CAM

Tabelle 3: CA-Manager (CAM)

Siehe auch Kapitel 1.3.1.3.

5.2.1.6 CA-Betriebspersonal (CAO)

Rolle	Aufgaben der Rolle	Kürzel
CA-Betriebspersonal	• Betrieb der CA (z.B. Ausstellung von Zertifikaten, Verteilung von Sperrlisten)	CAO

Tabelle 4: CA-Betriebspersonal (CAO)

Siehe auch Kapitel 1.3.1.3.

5.2.1.7 RA-Personal (RA)

Rolle	Aufgaben der Rolle	Kürzel
RA-Personal	• Entgegennahme, Prüfung und Freigabe von Zertifikats- und Sperranträgen • Prüfung der Autorisierung der Teilnehmer • Archivierung von Dokumenten • Verwaltung der Rolle TA	RA

Tabelle 5: RA-Personal

Siehe auch Kapitel 1.3.2.

5.2.1.8 Trusted Agents (TA)

Sollte eine RA den Dienst von Trusted Agents anbieten, so müssen die Bereitstellung des Dienstes und die Verfahrensweise zur Bestimmung der Vertrauenswürdigkeit eines TA im CPS der CA beschrieben werden.

Siehe Kapitel 1.3.3.

5.2.1.9 Sicherheitsrevisor (SR)

Rolle	Aufgaben der Rolle	Kürzel
Sicherheitsrevisor	• Prüfung des Ist-Zustands von CAs und RAs gemäß dieser CP	SR

Tabelle 6: Sicherheitsrevisor (SR)

5.2.2 Erforderliche Anzahl von Personen je Tätigkeit

Nachfolgend sind die Tätigkeiten beschrieben, bei denen Mehrpersonen-Prinzip – realisiert durch jeweils einen Vertreter der angegebenen Rollen – eingehalten werden muss. Alle anderen Tätigkeiten können von einer Person durchgeführt werden. Es muss sichergestellt werden, dass jede Rolle mit ausreichend vielen Mitarbeitern besetzt ist, um einen kontinuierlichen Betrieb zu gewährleisten.

CA	Tätigkeit	Rolle
Root CA	Erzeugung/Vernichtung von eigenen Schlüsselpaaren	PA & TAM
Root CA	Aktivierung von eigenen Schlüsselpaaren	PA & TAM
Root CA	Ausstellung von CA-Zertifikaten	PA & TAM
Root CA	Signierung von Sperrlisten für gesperrte CA-Zertifikate	PA & TAM
Root CA	Austausch von Hard- und Softwarekomponenten der Root CA	SA & TAM
CA (außer Root CA)	Erzeugung/Vernichtung von eigenen Schlüsseln	CAM & CAO
CA (außer Root CA)	Aktivierung von eigenen Schlüsselpaaren	CAM & CAO
CA (außer Root CA)	Freigabe eines Sperrantrags für das eigene Zertifikat (CA-Zertifikat)	CAM & CAO
CA (außer Root CA)	Austausch von Hard- und Softwarekomponenten	SA & CAM

Tabelle 7: Tätigkeiten, die das Mehrpersonen-Prinzip erfordern

5.2.3 Identifizierung und Authentifizierung der Rollen

Die Identifizierung und Authentifizierung der Rollen muss auf Grundlage des in Kapitel 5.2.1 und Kapitel 5.2.2 beschriebenen Rollenmodells erfolgen.

5.2.4 Trennung von Rollen

In folgender Tabelle ist aufgeführt, welche Rollen miteinander unverträglich sind.

Rolle	Unverträglich mit								
	PA	TAM	SA	SO	CAM	CAO	RA	TA	SR
PA		X	X	X	X	X	X	X	
TAM	X			X		X	X	X	X
SA	X					X	X	X	X
SO	X	X							X
CAM	X					X	X	X	X
CAO	X	X	X		X				X
RA	X	X	X		X			X	X
TA	X	X	X		X		X		X
SR		X	X	X	X	X	X	X	

5.3 Personelle Sicherheitsmaßnahmen

Es gelten die internen Vorgaben der DZ BANK AG entsprechend des Schutzbedarfs der CA.

5.3.1 Anforderung an die Mitarbeiter

Es gelten die internen Vorgaben der DZ BANK AG entsprechend des Schutzbedarfs der CA.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Es gelten die internen Vorgaben zur Sicherheitsüberprüfung der DZ BANK AG entsprechend des Schutzbedarfs der CA.

5.3.3 Anforderung an die Schulung

Das mit dem Betrieb der DZ BANK AG PKI verantwortliche Personal ist hinsichtlich der Sicherheitsrelevanz zu sensibilisieren und tätigkeitsbezogen zu schulen.

Spezielle Schulungen sind im entsprechenden CPS zu beschreiben.

5.3.4 Frequenz von Schulungen

Siehe Kapitel 5.3.3.

5.3.5 Ablauf und Sequenz der Job Rotation

Bei einem Rollenwechsel muss sichergestellt werden, dass das Mehrpersonen-Prinzip eingehalten wird.

5.3.6 Sanktionen für unautorisierte Handlungen

Es gelten die internen Vorgaben für der DZ BANK AG zum Thema Sanktionen entsprechend des Schutzbedarfs der CA.

5.3.7 Anforderungen an unabhängige, selbstständige Zulieferer

Externe Mitarbeiter, die für die Administration oder den Betrieb der DZ BANK AG Root CA oder einer untergeordneten CA zuständig sind, bedürfen einer expliziten Freigabe durch die PA.

5.3.8 Dokumente für die Mitarbeiter

Den Mitarbeitern der DZ BANK AG PKI sind folgende Dokumente zur Verfügung zu stellen:

- Certificate Policy (CP)
- Certificate Practice Statement (CPS)

5.4 Sicherheitsüberwachung

Die Maßnahmen zur Sicherheitsüberwachung sind für alle CAs in den entsprechenden CPS zu beschreiben.

5.4.1 Überwachte Ereignisse

Die internen Vorgaben der DZ BANK AG zur Informationssicherheit sind zu erfüllen. Jegliche von Hersteller deklarierte Sicherheitsevents sind zu überwachen.

Es muss sichergestellt werden, dass die Systeme über Protokollierungsmechanismen verfügen, um eine unberechtigte oder fehlerhafte Nutzung zu erkennen und analysieren zu können. Dies beinhaltet u.a. ein Protokollieren von:

- Systeminitialisierung (insbesondere das Hochfahren der Root CA)
- Zertifikatsanträgen
- Registrierung der Benutzer
- Schlüsselerzeugung
- Zertifikatserstellung
- Datensicherungen
- Zertifikatsveröffentlichung
- Auslieferung von privaten Schlüsseln und Zertifikaten
- Sperranträge
- Sperrung eines Zertifikats
- Erstellung einer Sperrliste
- Veröffentlichung einer Sperrliste
- Ablauf einer Sperrliste, sofern noch keine neue ausgestellt wurde

Weitere Informationen sind in den entsprechenden CPS zu beschreiben.

5.4.2 Frequenz der Protokollanalyse

Die Überwachungsprotokolle müssen regelmäßig überprüft werden, bevor sie archiviert werden. Alle wichtigen Ereignisse müssen in einer Prüfungsprotokoll-Zusammenfassung erklärt werden. Maßnahmen als Folge der Überprüfung sind zu dokumentieren.

Eine solche Prüfung muss sicherstellen, dass die aufgezeichneten Prüfungsprotokolle nicht manipuliert wurden und eine gründliche Untersuchung der Warnungen oder Unregelmäßigkeiten durchgeführt wird. Es muss sichergestellt werden, dass ein bedeutender statistischer Anteil (Menge) der sicherheitsrelevanten Prüfungsdaten, die von einer CA, einem CSS oder einer RA generiert werden, geprüft werden. Die Menge wird im CPS beschrieben.

Zur Analyse sollten automatisierte Echtzeit-Analyse-Werkzeuge eingesetzt werden. Alle Warnungen, die durch ein solches System generiert werden, müssen ausgewertet werden.

Bei Verdacht auf außergewöhnliche Ereignisse werden Sonderprüfungen vorgenommen.

5.4.3 Aufbewahrungszeitraum für Protokolldaten

Die internen Vorgaben der DZ BANK AG zur Informationssicherheit sind zu erfüllen.

5.4.4 Schutz der Protokolldaten

Die internen Vorgaben der DZ BANK AG zur Informationssicherheit sind zu erfüllen.

5.4.5 Backup der Protokolldaten

Die internen Vorgaben der DZ BANK AG zur Informationssicherheit sind zu erfüllen.

5.4.6 Überwachungssystem

Die internen Vorgaben der DZ BANK AG zur Informationssicherheit sind zu erfüllen.

5.4.7 Benachrichtigung bei schwerwiegenden Ereignissen

Alle schwerwiegenden Ereignisse sind im Rahmen des Security-Incident-Prozesses zu bearbeiten.

5.4.8 Schwachstellenuntersuchung

Die internen Vorgaben der DZ BANK AG zur Informationssicherheit sind zu erfüllen.

5.5 Archivierung

Die Maßnahmen zur Archivierung sind entsprechend der Vorgaben der DZ BANK AG durchzuführen. Davon abweichende Maßnahmen sind in den entsprechenden CPS zu beschreiben.

5.5.1 Archivierte Daten

Siehe Kapitel 5.5.

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Siehe Kapitel 5.5.

5.5.3 Schutz der Archive

Siehe Kapitel 5.5.

5.5.4 Datensicherungskonzept

Die Issuing CAs haben die internen Vorgaben zur Datensicherung gemäß ihres Schutzbedarfs zu erfüllen. Nach jeder Tätigkeit an der DZ BANK Root CA ist der interne Status der Root CA (z.B. aktuelle Anzahl ausgestellter Root CA CRLs etc.) zu sichern.

5.5.5 Anforderungen für Zeitstempel

Siehe Kapitel 5.5.

5.5.6 Archivierungssystem

Siehe Kapitel 5.5.

5.5.7 Prozeduren zum Abrufen und Überprüfen von archivierten Daten

Siehe Kapitel 5.5.

5.6 Schlüsselwechsel

Die Gültigkeitsdauer von Schlüsseln ist in Kapitel 6.3.2 festgelegt. Falls der Schlüssel einer CA kompromittiert wurde, gelten die in Kapitel 5.7 aufgeführten Regelungen. Nach Erzeugung eines neuen CA-Schlüssels muss dieser gemäß Kapitel 2 veröffentlicht werden.

5.7 Kompromittierung und Wiederherstellung

5.7.1 Prozeduren bei Sicherheitsvorfällen und Kompromittierung

Die internen Vorgaben der DZ BANK AG sind zu erfüllen. Alle Ereignisse sind im Rahmen des Security-Incident-Prozesses zu bearbeiten.

5.7.2 Prozeduren bei IT-Systemen

Werden innerhalb einer CA fehlerhafte oder manipulierte Rechner, Software und/oder Daten festgestellt, die Auswirkungen auf die Prozesse der CA haben, muss der Betrieb des entsprechenden IT-Systems unverzüglich eingestellt werden.

Alle Ereignisse sind im Rahmen des Security-Incident-Prozesses zu bearbeiten.

Falls Zertifikate mit fehlerhaften Angaben generiert wurden, ist der Zertifikatsnehmer unverzüglich zu informieren und das Zertifikat zu sperren.

5.7.3 Kompromittierung von privaten Schlüsseln

Wurde ein privater Schlüssel eines Zertifikatnehmers kompromittiert, so muss das dazugehörige Zertifikat gesperrt werden (siehe Abschnitt 4.9.1).

Wurde der private Schlüssel einer CA kompromittiert, so müssen das Zertifikat der CA und alle damit ausgestellten Zertifikate gesperrt werden. Außerdem müssen alle betroffenen Zertifikatnehmer informiert werden.

5.7.3.1 Prozeduren bei einer Root CA-Kompromittierung

Zu definieren im CPS.

5.7.3.2 Prozeduren bei einer CA- oder Sub-CA-Kompromittierung

Zu definieren im CPS.

5.7.3.3 Prozeduren bei einer CSS-Kompromittierung

Zu definieren im CPS.

5.7.3.4 Prozeduren bei einer RA-Kompromittierung

Zu definieren im CPS.

5.7.4 Betrieb nach einer Katastrophe

Die internen Vorgaben zum Business-Continuity-Management der DZ BANK AG sind zu erfüllen.

5.8 Einstellung des Betriebs

Wird der Betrieb einer CA eingestellt, müssen folgende Maßnahmen ergriffen werden:

- Information der Zertifikatsnehmer bzw. der Zertifikatsinhaber sowie der Relying Parties
- Sperrung aller von der CA ausgestellten Zertifikate
- Veröffentlichung der entsprechenden CA- und Root CA-Sperrlisten
- Sichere Vernichtung der privaten Schlüssel der CA
- Widerrufung aller an Auftragnehmer vergebenen Autorisierungen, im Namen der CA zu handeln

Die DZ BANK AG PKI muss den Fortbestand der Archive und die Abrufmöglichkeit einer vollständigen Sperrliste für den zugesicherten Aufbewahrungszeitraum sicherstellen. Dies ist im zugehörigen CPS zu spezifizieren. Grundsätzlich muss das Archiv 2 Jahre aufbewahrt werden. Ggf. höhere existierende Anforderungen (z.B. rechtsverbindliche digitale Unterschriften) werden in der CPS beschrieben.

6 Technische Sicherheitsmaßnahmen

Technische Sicherheitsmaßnahmen sind detaillierter im entsprechenden CPS zu beschreiben.

6.1 Schlüsselerzeugung und Installation

6.1.1 Schlüsselerzeugung

6.1.1.1 CA-Schlüsselerzeugung

Die Schlüsselpaare aller CAs müssen in einem Hardware-Sicherheits-Modul (HSM), das den Anforderungen aus Kapitel 6.2.1 genügt, im Mehrpersonen-Prinzip erzeugt werden (siehe Kapitel 5.2.2). Die Anzahl der hierzu autorisierten Mitarbeiter sind auf das betrieblich notwendige Maß zu beschränken.

Die Durchführung der Schlüsselerzeugung sowie Zertifikatserstellung ist für alle CAs im Rahmen von dokumentierten Schritten per Logbuch zu dokumentieren.

6.1.1.2 RA-Schlüsselerzeugung

Keine Angaben.

6.1.1.3 Zertifikatsnehmer-Schlüsselerzeugung

Schlüsselpaare sind möglichst auf dem System zu generieren, auf dem sie genutzt werden und sollten dieses nicht verlassen. Abweichungen, z.B. bei Key-Escrow-Anforderungen, sind im CPS zu

definieren.

Für die Schlüsselerstellung sind adäquate systemseitige Entropiequellen zu nutzen.

6.1.1.4 CSS Schlüsselerzeugung

Keine Angaben.

6.1.2 Übermittlung des privaten Schlüssels an den Zertifikatsnehmer

Sofern die Schlüssel des Zertifikatsnehmers CA-seitig generiert werden, ist dieser Prozess im entsprechenden CPS zu spezifizieren. Die Übermittlung der privaten Schlüssel an den Zertifikatsnehmer muss vertraulich, integritätsgeschützt und in authentisierter Form erfolgen. Die Anzahl der bei der Schlüsselübermittlung involvierten Entitäten ist minimal zu halten.

6.1.3 Übermittlung des öffentlichen Schlüssels an die CA

Die Übermittlung des Certificate Signing Request (**CSR**) (dt. Zertifikatsignierungsanforderung) an die CA muss integritätsgeschützt und in authentisierter Form erfolgen. Dieser Prozess ist im entsprechenden CPS zu spezifizieren.

6.1.4 Übermittlung des öffentlichen CA-Schlüssels

Die öffentlichen Schlüssel aller CAs der DZ BANK AG PKI können über einen Informationsdienst gemäß Kapitel 2 abrufen werden.

6.1.5 Schlüssellängen

Zertifikate müssen die folgenden Anforderungen an die Schlüssellängen für die verschiedenen Algorithmen erfüllen.

Algorithmen und Schlüssellänge	
Signatur-Algorithmen	RSA
Signatur-Hash-Algorithmen	SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384, SHA3-512
Schlüssellängen / Gültigkeit	CAs: • Min. 2048 Bit (bis maximales Laufzeitende in 2022) • Min. 4096 Bit (max. 20 Jahre Gültigkeit) End-Entität-Zertifikate: • Min. 2048 Bit; max. 2 Jahre Gültigkeit (ohne HW-Schutz), 3 Jahre Gültigkeit (bei separaten HW-Schutz d.h. Smartcard/TPM/HSM), Das Laufzeitende sollte sich an der BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen orientieren • Für Zertifikate mit Laufzeitende nach dem Jahr 2022 gilt: >= 3072 Bit; max. 2 Jahre Gültigkeit (ohne HW-Schutz), bzw. 3 Jahre Gültigkeit (bei separaten HW-Schutz d.h. Smartcard/TPM/HSM).

Tabelle 8: Überblick über Algorithmen und Schlüssellänge

Bei Einsatz anderer Algorithmen oder Schlüssellängen sind diese im CPS der CA zu beschreiben und von der PA abzunehmen.

6.1.6 Parameter der öffentlichen Schlüssel und Qualitätssicherung

Alle Zertifikate werden mindestens mit SHA-2 unter Verwendung des Paddings nach PKCS#1 v1.5 signiert.

Bekanntermaßen kompromittierte Schlüssel (z.B. „Debian weak keys“) oder Schlüssel mit schwachen Parametern wie RSA-Exponenten mit Wert 1 dürfen nicht verwendet werden. Ein Schlüssel gilt auch als kompromittiert, wenn bekannt wird, dass er für verschiedene Zertifikatsnehmer verwendet wird/werden soll.

6.1.7 Verwendungszweck der Schlüssel und Beschränkungen

Die zulässigen Schlüsselverwendungszwecke (Key Usage) sind im entsprechenden CPS zu spezifizieren.

Bei der Ausstellung der Zertifikate muss der Verwendungszweck so minimal wie möglich gehalten werden.

Die folgenden Bits dürfen gemäß dieser Richtlinie in Zertifikaten grundsätzlich nicht gesetzt werden:

- „dataEncipherment“
- „encipherOnly“
- „decipherOnly“
- „anyExtendedKeyUsage“

6.2 Schutz des privaten Schlüssels

Der private Schlüssel einer CA darf nicht außerhalb eines HSMs rekonstruierbar sein. HSMs müssen manipulationssicher transportiert und gelagert werden.

Erfolgt die Anwendung des privaten Schlüssels der CA auf einem vernetzen IT-System, so darf der private Schlüssel nicht außerhalb eines HSMs rekonstruierbar sein.

6.2.1 Standard des kryptographischen Moduls

HSMs, die gemäß Kapitel 6.2 eingesetzt werden, sollten einem der folgenden bzw. dazu äquivalenten Standards genügen:

- FIPS 140-2 Level 3
- CC EAL4+
- ITSEC E3 der Stärke "hoch"

Der Betriebsmodus für das HSM ist im entsprechenden CPS zu spezifizieren.

6.2.2 Kontrolle des privaten Schlüssels durch mehrere Personen

Der Zugriff auf den privaten Schlüssel der Root CA (Erstellung CRL, Aktivierung, Ausstellung CA-Zertifikat) muss immer im 4-Augenprinzip durch mindestens eine Person in der Rolle PA und mindestens eine Person in der Rolle TAM erfolgen.

Der Zugriff auf den privaten Schlüssel einer untergeordneten CA muss in den Fällen Aktivierung des privaten Schlüssels im 4-Augenprinzip durch mindestens eine Person in der Rolle CAM und mindestens eine Person in der Rolle CAO erfolgen.

Siehe auch Kapitel 5.2.2.

6.2.3 Treuhänderische Hinterlegung (Key Escrow) privater Schlüssel

Werden private Schlüssel hinterlegt, muss dies im CPS beschrieben werden (siehe Kapitel 4.12). Der private Schlüssel der DZ BANK AG Root CA oder einer untergeordneten CA darf niemals treuhänderisch hinterlegt werden.

Private Schlüssel von Zertifikaten mit Certificate-Usage-Parameter „digitalSignature“ dürfen nicht treuhänderisch hinterlegt werden.

6.2.4 Backup der privaten Schlüssel

Ein Backup von CA-Schlüsseln (auch Root CA) wird mit FIPS-140 Level 3-konformen Mechanismen des HSMs durchgeführt, hierbei liegen die Schlüssel in verschlüsselter Form vor. Die Entschlüsselung kann nur im HSM im 4-Augenprinzip durch mindestens eine Person in der Rolle PA und mindestens eine Person in der Rolle TAM erfolgen (siehe auch Kapitel 5.2.2.).

Das Backup der CA-Schlüssel sollte auf einem weiteren HSM aufbewahrt werden.

Wird von diesem Verfahren abgewichen, muss sichergestellt werden, dass ein angemessenes Sicherheitsniveau gehalten wird. Dies muss im CPS beschrieben werden.

Wird ein Backup privater Schlüssel von Zertifikatnehmern bei der RA oder CAM durchgeführt, so muss dies im CPS beschrieben werden.

6.2.4.1 Datensicherung des Signatur-Schlüssel einer CA

Siehe Kapitel 6.2.4.

6.2.4.2 Datensicherung des privaten Schlüssels eines Zertifikatsnehmers

Siehe Kapitel 6.2.4.

6.2.4.3 Datensicherung des privaten Schlüssels einer CSS

Siehe Kapitel 6.2.4.

6.2.4.4 Datensicherung des privaten Schlüssels von Geräten, Applikationen und Code-Signing

Siehe Kapitel 6.2.4.

6.2.5 Archivierung der privaten Schlüssel

Für die Archivierung privater Schlüssel gelten die Regelungen aus Kapitel 6.2.4.

6.2.6 Transfer privater Schlüssel in ein kryptographisches Modul

Private Schlüssel einer CA werden nach Kapitel 6.1.1 immer in einem HSM erzeugt. Der Transfer privater Schlüssel in ein kryptographisches Modul findet nur bei einem Backup oder bei einem Transfer von einem anderen kryptographischen Modul statt.

6.2.7 Speicherung privater Schlüssel in einem kryptographischen Modul

Private Schlüssel einer CA müssen sicher in einem kryptographischen Modulen abgelegt werden.

6.2.8 Aktivierung der privaten Schlüssel

Bei privaten Schlüsseln einer CA muss die Aktivierung gemäß Kapitel 6.2.2 durchgeführt werden.

6.2.9 Deaktivierung der privaten Schlüssel

Die Deaktivierung der privaten Schlüssel einer CA muss nach Beendigung des CA-Lifecycles erfolgen.

Für Offline-CAs ist die Deaktivierung in den entsprechenden CPS zu spezifizieren.

6.2.10 Vernichtung der privaten Schlüssel

Vor Außerdienststellung eines HSMs müssen alle darauf gespeicherten privaten Schlüssel vernichtet werden. Alle Kopien des privaten Schlüssels einer CA müssen mit Beendigung ihres Lebenszyklus vernichtet werden.

Bei der Vernichtung der privaten Schlüssel einer CA muss nach dem Mehrpersonen-Prinzip verfahren werden. Verantwortlich für die Vernichtung sind die Rollen gemäß Kapitel 5.2.2.

6.2.11 Güte des kryptographischen Moduls

Siehe Kapitel 6.2.1.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Siehe Kapitel 5.5.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Für alle Zertifikate die innerhalb der DZ BANK AG PKI ausgestellt werden, darf das Gültigkeitsende des Zertifikats das Gültigkeitsende des zur Ausstellung verwendeten CA-Zertifikats nicht überschreiten.

Weitere Details siehe Kapitel 6.1.5

6.4 Aktivierungsdaten

Interne Richtlinien der DZ BANK AG sind zu berücksichtigen und das Verfahren ist genauer im CPS zu beschreiben.

6.4.1 Aktivierungsdaten für Erzeugung und Installation

Siehe Kapitel 6.4.

6.4.2 Schutz der Aktivierungsdaten

Aktivierungsdaten müssen geheim gehalten werden und dürfen nur den Mitarbeitern bekannt sein, die diese nach Kapitel 5.2.1 für die Durchführung einer spezifischen Funktion benötigen. Eine schriftliche Fixierung ist allenfalls für das Backup nach Kapitel 6.2.4 zulässig.

6.4.3 Weitere Aspekte

Keine Angaben.

6.5 Sicherheitsmaßnahmen für Computer

Es gelten die internen Vorgaben der DZ BANK AG bzgl. der technischen Sicherheitsmaßnahmen. Die detaillierte Umsetzung ist im entsprechenden CPS zu spezifizieren.

6.5.1 Spezifische Anforderungen an technische Sicherheitsmaßnahmen

6.5.1.1 Zugriffskontrolle

Siehe Kapitel 6.5.

6.5.1.1.1 Richtlinie und Prozeduren der Zugriffskontrolle

Siehe Kapitel 6.5.

6.5.1.1.2 Kontenverwaltung

Siehe Kapitel 6.5.

6.5.1.1.3 Geringste Berechtigungen

Siehe Kapitel 6.5.

6.5.1.1.4 Zugriffskontrolle Best Practice

Siehe Kapitel 6.5.

6.5.1.1.5 Authentifizierung: Passwörter und Konten

Siehe Kapitel 6.5.

6.5.1.1.6 Erlaubte Aktionen ohne Identifikation oder Authentifikation

Siehe Kapitel 6.5.

6.5.1.2 System-Integrität

Siehe Kapitel 6.5.

6.5.1.2.1 System-Isolation und -Partitionierung

Siehe Kapitel 6.5.

6.5.1.2.2 Schutzmaßnahmen gegen böswilligen Programmcode (Malicious Code)

Siehe Kapitel 6.5.

6.5.1.2.3 Integrität von Soft. und Firmware

Siehe Kapitel 6.5.

6.5.1.2.4 Informations-Partitionen

Siehe Kapitel 6.5.

6.5.2 Güte / Qualität der Sicherheitsmaßnahmen

Siehe Kapitel 6.5.

6.6 Lebenszyklus der Sicherheitsmaßnahmen

Siehe Kapitel 6.5.

6.6.1 Softwareentwicklung

Siehe Kapitel 6.5.

6.6.2 Sicherheitsmanagement

Siehe Kapitel 6.5.

6.6.3 Sicherheitseinstufung

Siehe Kapitel 6.5.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Siehe Kapitel 6.5.

6.7.1 Isolierung von Netzwerk-Systemen

Siehe Kapitel 6.5.

6.7.2 Schutz der Zonengrenzen

Siehe Kapitel 6.5.

6.7.2.1 Übersicht der PKI-Netzwerk-Zonen

Siehe Kapitel 6.5.

6.7.2.2 Grenze des Spezial-Zugriffs Netzwerkbereich (engl. Special Access Network Area (SANA))

Siehe Kapitel 6.5.

6.7.2.3 Grenze des Eingeschränkten Netzwerkbereich (Restricted Network Area (RNA))

Siehe Kapitel 6.5.

6.7.2.4 Grenze des Betriebs Netzwerkbereich (Operational Network Area (ONA))

Siehe Kapitel 6.5.

6.7.3 Verfügbarkeit

CA-Systeme sollten mit dem Ziel einer Maximierung der Verfügbarkeit und Betriebszeit konfiguriert, gewartet und betrieben werden. Geplante Ausfallzeiten sollten den davon betroffenen Zertifikatsnehmern bekannt gegeben werden.

Die Verfügbarkeit der Dienste ist im Rahmen der Schutzbedarfsfeststellung zu definieren. Dies ist im Detail im entsprechenden CPS zu beschreiben.

6.7.3.1 Schutzmaßnahmen gegen Denial of Service (DoS)

Es gelten die internen Richtlinien der DZ BANK AG gemäß dem Schutzbedarf.

Die CAs müssen in ihrem CPS akzeptable Methoden benennen, wie sie bei einem Denial of Service-Angriff Sperr-Anforderungen bearbeiten. Mindestens eine der Methoden muss dies ohne eine Netzwerkverbindung (engl. out of band) erreichen.

6.7.3.2 Schutzmaßnahmen vor öffentlichem Zugriff

Es gelten die internen Richtlinien der DZ BANK AG gemäß des Schutzbedarfs Es ist sicherzustellen, dass nur von authentifizierten und autorisierten Nutzern aus zugelassenen Netzen auf die Systeme zugegriffen werden kann. Details sind im entsprechenden CPS zu spezifizieren.

6.7.4 Kommunikationssicherheit

Es gelten die internen Richtlinien der DZ BANK AG gemäß dem Schutzbedarf. Für alle CAs sind die Sicherheitsmaßnahmen für die Kommunikation im CPS der CA zu beschreiben.

6.7.4.1 Übertragungs-Integrität

Siehe Kapitel 6.7.4.

6.7.4.2 Übertragungs-Vertraulichkeit

Siehe Kapitel 6.7.4.

6.7.4.3 Trennung von Netzwerkverbindungen

Siehe Kapitel 6.7.4.

6.7.4.4 Etablierung kryptographischer Schlüssel und Management

Siehe Kapitel 6.7.4.

6.7.4.5 Kryptographie-Schutzmaßnahmen

Siehe Kapitel 6.7.4.

6.7.4.6 Authentizität von Applikations-Sitzungen

Siehe Kapitel 6.7.4.

6.7.5 Netzwerk-Überwachung

Die CA muss, um Angriffe oder Indikationen für mögliche Angriffe zu erkennen, gemäß dem jeweiligen Schutzbedarf überwacht werden. Die Überwachung erfolgt durch die Standardprozesse der DZ BANK AG.

6.7.5.1 Überwachte Ereignisse und Transaktionen

Für alle CAs sind die überwachten Ereignisse und Transaktionen im CPS der CA zu beschreiben.

6.7.5.2 Überwachung von Geräten

Für alle CAs sind die Maßnahmen der Überwachung von Geräten im CPS der CA zu beschreiben.

6.7.5.3 Überwachung von Sicherheitsalarmen, Empfehlungen und Direktiven

Eine CA muss diejenigen Informationssysteme laufend überwachen, die Sicherheitswarnungen, Sicherheitshinweise und Direktiven über ihre Komponenten herausgeben.

6.7.6 Remote Zugriff/externes Informations-System

6.7.6.1 Remote Zugriff

Für alle CAs ist der Remote Zugriff im entsprechenden CPS zu regeln.

6.7.6.2 Bastion Host (Proxy)

Alle Zugriffe auf sicherheitskritische Komponenten einer CA müssen über einen Bastions-Host (d.h. eine Maschine, die eine eingeschränkte Schnittstelle für die Interaktion mit anderen Elementen der CA zur Verfügung stellt, auch Jump-Host genannt) abgewickelt werden, sofern die CA nicht als Offline CA betrieben wird. Der direkte Zugriff ist nicht erlaubt. Der Bastions-Host muss regelmäßig gepatched und verwaltet werden. Es dürfen nur Anwendungen installiert sein, die zur Erfüllung seiner Aufgaben zwingend nötig sind.

6.7.6.3 Dokumentation

Die CA muss die zulässigen Methoden des Remote-Zugriffs auf die CA-Systeme einschließlich deren Nutzungsbeschränkungen und dem Implementierungsleitfaden für jede der zugelassenen Methoden in der CPS dokumentieren.

6.7.6.4 Aufzeichnung

Protokollierung muss für jede Sitzung mit der CA in Übereinstimmung mit Kapitel 5.4 auf dem Bastions-Host durchgeführt werden. Insbesondere müssen diese Protokolle das Datum und die Uhrzeit der Verbindung, die authentifizierte Identität des Verbindungsanforderers, die IP-Adresse des entfernt stehenden Systems und ebenfalls die Befehle, die an den Bastions-Host gesendet wurden, enthalten. Die aufgezeichneten Protokollierungen müssen auf einem zentralen Logserver abgelegt werden.

6.7.6.5 Automatisches Überwachen

Automatisierte Überwachung muss bei allen Remote Sitzungen mit dem Bastions-Host und allen Interaktionen zwischen dem Bastions-Host und anderen CA-Systeme erfolgen. Beim Erkennen eines nicht autorisierten Zugriffs muss die Verbindung zur CA getrennt und das Ereignis protokolliert werden.

6.7.6.6 Sicherheit von Remote-Management-Systemen

Siehe Kapitel 6.7.6.2.

6.7.6.7 Authentifizierung

Keine erweiterten Anforderungen sofern Bastions-Host (siehe Kapitel 6.7.6.2) eingesetzt wird.

6.7.6.8 Sicherheit der Kommunikation für Remote-Zugriff

Die gesamte Kommunikation zwischen dem Bastions-Host und dem CA-System muss im CPS beschrieben werden. Das Verfahren muss integritätsgeschützt und vertraulich sein.

6.7.7 Penetrations-Tests

Die internen Vorgaben der DZ BANK AG zur Informationssicherheit sind zu erfüllen.

6.8 Zeitstempel

Die Anpassung des Zeitstempels ist ein der Überprüfung unterliegendes Ereignis (siehe Kapitel 5.4.1). Der Zeitgeber ist der zentrale Zeitgeber der DZ BANK AG. Der Service ist hierbei an den zentralen Zeitgeber angebunden.

7 Profile von Zertifikaten, CRLs und OCSP

7.1 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen

Profile für Zertifikate, Sperrlisten und OCSP sind im entsprechenden CPS zu spezifizieren.

7.1.1 Versionsnummer(n)

Siehe Kapitel 7.1.

7.1.2 Zertifikatserweiterungen

Siehe Kapitel 7.1.

7.1.3 Algorithmus für die Objekt-Identifizierungskennung

Siehe Kapitel 7.1

7.1.4 Namensformen

Siehe auch Kapitel 3.1.

Domainnamen und IP-Adressen, die im Subject enthalten sind, müssen immer auch in den alternativen Zertifikatnamen („subjectAlternativeName“) unter den Typen „dNSName“ bzw. „iPAddress“ aufgeführt werden.

7.1.5 Namensbeschränkungen

Siehe Kapitel 3.1.

7.1.6 Objekt-Identifikator der CP in Zertifikaten

Zertifikate (außer dem Root CA-Zertifikat) die in Übereinstimmung mit dieser Richtlinie erstellt werden, müssen die folgenden OIDs bis zur Stelle für die Major-Version (ohne die Stellen für Minor-Version) einfügen:

- OID dieser CP nach Kapitel 1.2
- OID des für die ausstellende CA gültigen CPS

7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkung

Nichtzutreffend.

7.1.8 Syntax und Bedeutung von Richtlinienkennungen

Siehe Kapitel 1.2.

7.1.9 Abarbeitung von kritischen Erweiterungen der CP

Nichtzutreffend.

7.2 CRL Profil

Für jede CA in der DZ BANK AG PKI muss eine CRL bereitgestellt werden. Diese muss die gesperrten Zertifikate der jeweiligen CA enthalten. Jede CRL muss folgende Informationen enthalten:

- Versionsnummer (siehe Kapitel 7.2.1)
- Signaturalgorithmus
- Identifizierung der ausstellenden CA
- Zeitpunkt der Ausstellung
- Spätester Zeitpunkt des nächsten Updates (bei Sperrung eines Zertifikats wird sofort eine neue CRL generiert)
- Seriennummern und Sperrungsdaten der gesperrten Zertifikate
- Die digitale Signatur der ausstellenden CA

7.2.1 Versionsnummer(n)

Sperrlisten müssen gemäß der internationalen Norm X.509 in der Version 2 erstellt werden.

7.2.2 Erweiterungen von CRL und CRL Einträgen

In den Zertifikaten (außer dem Root CA-Zertifikat) muss ein Sperrlistenverteilpunkt enthalten sein.

7.3 Profile von OCSP

Der OCSP-Dienst muss konform zu RFC 6960 betrieben werden. OCSP-Antworten müssen mit einem Zertifikat signiert werden, das von der CA des zu prüfenden Zertifikats ausgestellt wurde.

Falls eine CA OCSP anbietet ist dies im CPS zu beschreiben.

7.3.1 Versionsnummer(n)

Die CSS die innerhalb dieser Richtlinie betrieben werden, müssen die OCSP Version 1 nutzen.

Die Verwendung von SCVP (engl. Server-based Certificate Validation Protocol) ist ebenfalls erlaubt.

7.3.2 OCSP Erweiterungen

OCSP Erweiterungen sind im entsprechenden CPS zu beschreiben.

8 Konformitätsprüfung

Die Abläufe für alle CAs der DZ BANK AG PKI sind so gestaltet, dass sie diesem CP und dem entsprechenden CPS der CA entsprechen.

Die Arbeitsprozesse der CAs, sowie an der Registrierung beteiligten Stellen werden regelmäßig bzw. anlassbezogen gemäß den internen Richtlinien der DZ BANK AG überprüft.

8.1 Frequenz oder Umstände der Überprüfung

Die Frequenz und Umstände einer Überprüfung richten sich nach den internen Richtlinien der DZ BANK AG entsprechend des Schutzbedarfs.

8.2 Identität und Qualifikation des Prüfers

Die Prüfung wird durch die in Kapitel 1.3.1.1 genannte Policy Authority durchgeführt.

8.3 Beziehung des Prüfers zu Überprüftem

Die PA ist nicht aktiv in den Produktionsbetrieb der untergeordneten CAs eingebunden.

Für die Root CA führt sie, zusammen mit der TAM, die unter Kapitel 5.2.2 genannten Tätigkeiten im 4-Augenprinzip durch.

8.4 Abzudeckende Themen einer Beurteilung

Es wird überprüft, ob eine CA inkl. zugehörige RAs alle Anforderungen des aktuellen CP und des entsprechenden CPS der CA einhält. Der Beurteilung unterliegen alle Abläufe des CA/RA Betriebs.

8.5 Ausführen von Aktionen basierend auf dem Ergebnis der Mängel

Sollte die Compliance-Prüfung Abweichungen zwischen den Anforderungen dieser CP, den Bestimmungen des entsprechenden CPS und dem Design, dem Betrieb oder der Wartung der PKI finden, müssen die folgenden Aktionen durchgeführt werden:

- Prüfer muss Mängel schriftlich festhalten
- Prüfer muss die PKI Verwaltung informieren
- Prüfer muss die in Kapitel 8.6 benannten Teilnehmer über die Mängel informieren
- Mängel werden durch den Prüfer einer Risikobewertung zugeführt
- Risikobewertung entscheidet weiteres Vorgehen zur Beseitigung der Mängel
- Verantwortlicher für die Korrektur der Mängel unterbreitet Lösungsvorschlag inkl. Benennung des Fertigstellungsdatum an die in Kapitel 1.3.1 benannte PKI Verwaltung
- Mängelbeseitigung erfolgt in Abstimmung mit der in Kapitel 1.3.1 benannten PKI Verwaltung

In Abhängigkeit der Natur und der Schwere der Mängel und wie schnell eine Behebung durchgeführt werden kann, kann die PA u.a.:

- Betrieb der CA oder RA temporär stoppen
- Sperrung von Zertifikaten die an die CA oder RA ausgestellt wurde durchführen
- Sperrung von durch die CA ausgestellte Zertifikate anfordern

8.6 Kommunikation der Ergebnisse

Die Kommunikation der Prüfungsergebnisse an interne und externe Stellen obliegt der DZ BANK AG. Es wird je nach Schutzbedürftigkeit der Informationen über die Veröffentlichung entschieden.

9 Rahmenvorschriften

9.1 Gebühren

Die Erhebung von Gebühren wird in der jeweiligen CPS geregelt.

9.1.1 Zertifikatsausstellungsgebühren oder Zertifikatserneuerungsgebühren

Siehe Kapitel 9.1.

9.1.2 Zertifikatszugriffsgebühren

Siehe Kapitel 9.1.

9.1.3 Sperrungen oder Statusinformationszugriffsgebühren

Siehe Kapitel 9.1.

9.1.4 Gebühren für zusätzliche Dienste

Siehe Kapitel 9.1.

9.1.5 Regelung für Erstattungen

Siehe Kapitel 9.1.

9.2 Finanzielle Verantwortung

Nichtzutreffend.

9.2.1 Versicherungsschutz

Nichtzutreffend.

9.2.2 Sonstige Gegenstände

Nichtzutreffend.

9.2.3 Versicherung oder Garantieabdeckung für Endeinheiten

Nicht zutreffen.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertraulich zu behandelnde Daten

Alle Informationen und Daten über Teilnehmer der DZ BANK AG PKI, die nicht unter Kapitel 9.3.2 fallen, werden als vertrauliche Informationen eingestuft.

9.3.2 Nicht vertraulich zu behandelnde Daten

Alle Informationen, die in den veröffentlichten Zertifikaten und Sperrlisten explizit (z. B. E-Mail-Adresse) oder implizit (z. B. Daten über die Zertifizierung) enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Die DZ BANK AG PKI trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen. Daten dürfen im Rahmen der Diensterbringung nur gemäß den internen Vorgaben der DZ BANK AG weitergegeben werden.

9.4 Schutz personenbezogener Daten (Datenschutz)

9.4.1 Richtlinie zur Verarbeitung personenbezogener Daten

Die DZ BANK AG PKI muss zur Leistungserbringung personenbezogene Daten elektronisch speichern und verarbeiten. Dies geschieht in Übereinstimmung mit dem (BDSG, Bundesdatenschutzgesetz, 2015).

9.4.2 Vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen aus Kapitel 9.3.1.

9.4.3 Nicht vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen aus Kapitel 9.3.2.

9.4.4 Verantwortlicher Umgang mit personenbezogenen Daten

Für personenbezogene Daten gelten die Regelungen aus Kapitel 9.3.3.

9.4.5 Nutzung personenbezogener Daten

Der Zertifikatsnehmer stimmt der Nutzung von personenbezogenen Daten durch die DZ BANK AG PKI zu, soweit dies zur Leistungserbringung erforderlich ist.

9.4.6 Offenlegung bei gerichtlicher Anordnung oder im Rahmen einer gerichtlichen Beweisführung

Die DZ BANK AG unterliegt dem Recht der Bundesrepublik Deutschland und muss vertrauliche und personenbezogene Informationen an staatliche Organe beim Vorliegen entsprechender Entscheidungen in Übereinstimmung mit den geltenden Gesetzen freigeben.

9.4.7 Andere Umstände einer Veröffentlichung

Nichtzutreffend.

9.5 Urheberrechte

Die DZ BANK AG ist Urheber dieser CP und der CPS-Dokumente. Die Weitergabe dieser CP und der CPS-Dokumente bedarf der Zustimmung der PA. Weitergehende Rechte werden nicht eingeräumt. Insbesondere ist die Weitergabe veränderter Fassungen und die Überführung in maschinenlesbare oder andere veränderbare Formen der elektronischen Speicherung, auch auszugsweise, ohne Zustimmung der DZ BANK AG nicht zulässig.

9.6 Verpflichtungen

9.6.1 Verpflichtung der Zertifizierungsstellen

Die DZ BANK AG PKI ist ein Dienst der DZ BANK AG.

Alle CAs die dieser Richtlinie der DZ BANK AG unterliegen, verpflichten sich alle im Rahmen dieser CP und dem entsprechenden CPS beschriebenen Bestimmungen einzuhalten.

9.6.2 Verpflichtung der Registrierungsstellen

Die RAs verpflichten sich, alle in dieser CP und den entsprechenden CPS der DZ BANK AG PKI beschriebenen Aufgaben nach bestem Wissen und Gewissen durchzuführen.

9.6.3 Verpflichtung des Zertifikatnehmers

Zertifikatnehmer müssen:

- Die privaten Schlüssel in Übereinstimmung mit dieser CP, den Bestimmungen der Zertifikats Akzeptanzvereinbarung, und den lokalen Verfahren, zu jeder Zeit schützen.
- Unverzüglich die entsprechende CA benachrichtigen, wenn der Verdacht des Verlustes oder die Beeinträchtigung (Kompromittierung) des privaten Schlüssels vorliegt. Die Benachrichtigung muss direkt oder indirekt durch die im entsprechenden CPS beschriebenen Mechanismen erfolgen.
- Sich an alle Bestimmungen, Bedingungen und Beschränkungen für die Verwendung von privaten Schlüsseln und Zertifikaten halten.

Siehe auch Kapitel 4.5.1.

9.6.4 Verpflichtung der Relying Parties

Es gelten die Bestimmungen aus Kapitel 4.5.2.

9.6.5 Verpflichtung anderer Teilnehmer

Sofern weitere Beteiligte als Dienstleister in den Zertifizierungsprozess eingebunden werden, ist die DZ BANK AG in der Verantwortung, den Dienstleister zur Einhaltung der CP und des entsprechenden CPS zu verpflichten.

9.7 Gewährleistung

Die DZ BANK AG PKI garantiert nicht die Verfügbarkeit der Leistungen.

9.8 Haftungsbeschränkung

Nichtzutreffend.

9.9 Haftungsfreistellung

Nichtzutreffend.

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Das CP und die CPS treten an dem in ihnen angegebenen Datum in Kraft. Sie werden über den entsprechenden Informationsdienst (siehe Kapitel 2) veröffentlicht.

9.10.2 Aufhebung

Dieses Dokument ist solange gültig, bis es durch eine neue Version ersetzt wird (siehe Kapitel 9.10.1) oder der Betrieb der DZ BANK AG PKI eingestellt wird.

9.10.3 Konsequenzen der Aufhebung

Die Anforderungen dieser CP, müssen bis zum Ablauf der Archivierungsfrist des zuletzt ausgestellten Zertifikates wirksam bleiben.

Von einer Aufhebung der CP oder des CPS unberührt bleibt die Verantwortung zum Schutz vertraulicher Informationen und personenbezogener Daten.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

Nichtzutreffend.

9.12 Änderungen des Dokuments

Eine Änderung der CP kann nur durch die PA der DZ BANK AG PKI erfolgen.

9.12.1 Prozess der Dokumentänderung

Diese CP ist einmal jährlich durch die PA zu prüfen. Korrekturen, Aktualisierungen oder Änderungen an dieser CP müssen öffentlich zur Verfügung gestellt und in einem Änderungskatalog im Vorwort zu dieser CP hinterlegt werden.

9.12.2 Benachrichtigung der Änderung und Zeitraum

Eine Anpassung dieser CP oder einer CPS, muss innerhalb von 30 Tagen veröffentlicht werden.

9.12.3 Gründe der Änderung einer OID

Die OID der CP und CPS wird bei einer Fortschreibung dieses Dokumentes nicht geändert.

Sollte die PA eine Änderung an der OID für gegeben erachten ist die Möglichkeit hierzu vorbehalten.

9.13 Konfliktbeilegung

Grundsätzlich ist die in Kapitel 1.3.1 Policy Authority genannte Stelle für die Konfliktbeilegung zuständig.

9.14 Gerichtsstand

Siehe Kapitel 9.16.4.

9.15 Konformität mit dem geltenden Recht

Der Betrieb der DZ BANK AG PKI unterliegt den Gesetzen der Bundesrepublik Deutschland. Alle CAs die innerhalb dieser Richtlinie unterliegen, müssen geltendes Recht anwenden.

9.16 weitere Regelungen

9.16.1 Vollständigkeit

Eine neue Version dieser CP oder einer CPS ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2 Übertragung der Rechte

Eine Abtretung von Rechten ist nicht vorgesehen.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser CP oder eines ihr untergeordneten CPS unwirksam sein oder Lücken enthalten, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Auch eine Lücke berührt nicht die Wirksamkeit der CP im Übrigen. Anstelle der unwirksamen Bestimmungen gilt diejenige wirksame Bestimmung als vereinbart, welche dem Sinn und Zweck der unwirksamen Bestimmung weitgehend entspricht.

9.16.4 Rechtliche Auseinandersetzungen / Erfüllungsort

Rechtliche Auseinandersetzungen, die aus dem Betrieb einer innerhalb der DZ BANK AG PKI operierenden CA herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland. Erfüllungsort und ausschließlicher Gerichtsstand sind Sitz der DZ BANK AG. Die DZ BANK AG ist im Handelsregister, Frankfurt am Main unter der Registernummer HRB 45651 registriert.

9.16.5 Höhere Gewalt

Keine Angaben.

9.17 Andere Bestimmungen

Nicht zutreffend.

10 Tabellenübersicht

11 Abbildungsverzeichnis

12 Abkürzungen

AD	Active Directory
AD DS	Active Directory Domain Service
AD CS	Active Directory Certificate Service
AIA	Authority Information Access
BFH	Betriebsführungshandbuch
BMI	Bundesministerium des Inneren
C	Country Staat
CA	Certification Authority Zertifizierungsstelle
CAM	Certificate Authority Manager Zertifizierungsstelle Manager
CAO	Certificate Authorities Operations Staff Zertifizierungsstelle Betriebspersonal
CMDB	Configuration Management Database Konfigurations Management Datenbank
CN	Common Name Gemeinsamer Name
CP	Certificate Policy Richtlinie für digitale Zertifikate
CPS	Certification Practice Statements Erklärung zum Zertifizierungsbetrieb
CR	Certificate Request Zertifikatanforderung
CRL	Certificate Revocation List Zertifikate Sperrliste Sperrliste, die Sperrinformationen über Teilnehmer-Zertifikate (und ggf. DZ BANK AG Root CA / CA-Zertifikate) enthält.
CSR	Certificate Signing Request Zertifikatsignierungsanforderung
CSS	Certificate Status Server Zertifikate Status Server
DN	Distinguished Name Eindeutigername
DNS	Domain Name Service Domänennamenservice
DRAC	Dell Remote Access Controller
EFS	Encrypting File System Verschlüsseltes Datei System

FQDN	Fully Qualified Domain Name Vollqualifizierter Domänenname
HSM	Hardware Security Module Hardware Sicherheitmodul, Hardware Kryptographiemodul
ILO	Integrated Lights-Out
IMK	Internal Master Key
IT	Information Technologie
ITU	Internationale Telekommunikation Union durch die Vereinten Nationen zur Verfügung gestellte Agentur für Informations- und Kommunikationstechnologie
ITU-T	ITU Telecommunication Sector
L	Locality Standort
MBK	Master Backup Key
O	Organization Name Organisationsname
OCSP	Online Certificate Status Protocol Online Sperr- und Statusüberprüfungsverfahren
OID	Object Identifier Objekt Identifizierungskennung
PA	Policy Authority Richtlinienverwaltung
PKI	Public-KeyInfrastructure ffentliche Schlüssel Infrastruktur
RA	Registration Authority Registrierungsstelle
RAS	Remote Access Services Fernzugriff Dienste
RFC	Request for Comments Anforderung eines Kommentars
Root CA	Oberste CA
SAN	Subject Alternative Name Alternativername des Subjekt
SNOW	ServiceNow (CMDB)
SR	Security Auditor Sicherheitsrevisor (intern)
S/MIME	Secure/Multipurpose Internet Mail Extensions
SSL	Secure Socket Layer Verschlüsselungsprotokoll zur Datenübertragung im Internet
SSO	Single Sign-On Einmalige Authentifizierung (Einmalanmelden)

ST	State Bundesland
TA	Trusted Agent Vertrauens Vertreter
TLS	Transport Layer Security ein Netzwerk Kommunikation Protokoll
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VPN	Virtual Privat Network
X.501	Ist ein ITU-T Empfehlung für Verzeichnis Struktur Modellen. Aktuell ist die Version 10/2012
X.509	Ist ein ITU-T Empfehlung für Public Key Infrastrukturen zur Erstellung von digitalen Zertifikaten. Aktuell ist die Version 3 (X.509v3)

13 Definitionen

Authority Information Access (AIA) Extension

Dies sind URIs die in den AIA Erweiterungsbereich (AIA Extension) eines Zertifikates eingefügt werden. Diese URIs können durch die Applikation oder den Dienst genutzt werden um das Zertifikat der ausstellenden CA abzurufen. Dieses CA-Zertifikat wird dann zur Gültigkeitsprüfung herangezogen, um den Vertrauenspfad zu einem vertrauenswürdigen Zertifikat aufzubauen.

Certificate Policy – Richtlinie für digitale Zertifikate (CP)

Eine CP ist eine spezielle Form einer Verwaltungsrichtlinie optimiert für die Behandlung von Zertifikaten. Eine CP adressiert alle Aspekte der Erzeugung, Produktion, Vertrieb, Buchhaltung, Wiederherstellung und Verwaltung von Zertifikaten. Durch die Kontrolle von kritischen Zertifikatserweiterungen, können solche Richtlinien und damit verbundene Technologien erforderliche Anforderungen an Sicherheitsstandards bestimmter Anwendungen durchsetzen.

Certification Authority – Zertifizierungsstelle (CA)

Eine Entität, deren Aufgaben das Erstellen, die Erteilung, der Widerruf und die Verwaltung von Zertifikaten sind. Der Begriff CA bezieht sich sowohl auf die Root CA als auch auf untergeordnete CAs.

Certification Practice Statement – Erklärung zum Zertifizierungsbetrieb (CPS)

Ist eine Umsetzungsvorgabe mit Anweisungen der zu implementierenden Praktiken, die eine Zertifizierungsstelle einsetzt für die Erteilung, Suspendierung, Sperrung und Erneuerung von Zertifikaten. Es regelt den Zugriff auf Zertifikate unter Berücksichtigung der spezifischen Anforderungen (z.B. Anforderungen die in diese Zertifikatsrichtlinie (CP) spezifiziert wurden oder spezielle Anforderungen die im Rahmen eines Dienstleistungsvertrags gestellt sind).

Certificate Signing Request - Zertifikat Signierungsanforderung (CSR)

Ein Zertifikat Signierungsanforderung ist ein standarisiertes Format zum Anfordern eines digitalen Zertifikats. Der CSR enthält den öffentlichen Schlüssel eines Schlüsselpaares und muss von der Registrierungsstelle (RA) auf Authentizität geprüft werden. Auf diese Weise bestätigt die RA mit ihrer Unterschrift die Gültigkeit der Angaben im Zertifikat.

End-Entität-Zertifikat

Unter einem End-Entität-Zertifikat wird ein durch eine Issuing CA ausgestelltes Zertifikat verstanden.

Issuing CA

Eine Issuing CA ist eine CA, die keine weiteren CAs ausstellt, sondern nur End-Entität-Zertifikate.

Key Pair – Schlüsselpaar

Ein Schlüsselpaar besteht aus einem öffentlichen und einem privaten Schlüssel. Diese sind mathematisch miteinander verbunden, sodass man mit dem:

1) öffentlichen Schlüssel z.B. Nachrichten verschlüsseln, Signaturen prüfen,
2) privaten Schlüssel z.B. Nachrichten entschlüsseln, Signaturen erstellen,

kann. Der private Schlüssel darf nur dem Zertifikatsnehmer bekannt sein. Der öffentliche Schlüssel kann öffentlich zur Verfügung gestellt werden.

Object Identifier - Objekt Identifizierungskennung (OID)

In der Informatik ist eine Objekt Identifizierungskennung ein weltweit eindeutiger Bezeichner, der benutzt wird um ein Informationsobjekt zu benennen.

Online Certificate Status Protocol (OCSP)

OCSP ist ein Netzwerkprotokoll das Clients ermöglichte einen Online Status von X.509 Zertifikaten abzufragen.

Public Key Infrastructure - öffentliche Schlüsselinfrastruktur (PKI)

Eine Reihe von Richtlinien, Prozesse, Server-Plattformen, Software und Arbeitsstationen zum Zweck der Administration von Zertifikaten und öffentlichen / privaten Schlüsselpaaren.

Registration Authority – Registrierungsstelle (RA)

Eine Einheit die für die Identifizierung und Authentifizierung von Zertifikats Objekten zuständig ist, jedoch keine Zertifikate signiert oder erteilt. (d. h. eine Registrierungsstelle übernimmt bestimmte Aufgaben die von einer autorisierten CA delegiert wurden.)

Re-key or Re-keying a certificate - Erneuerung (Neu-Erteilung)

Schlüsselerneuerung eines kryptographischen Schlüssels der bereits in einem Verschlüsselungssystem oder Anwendung eingesetzt ist. Dieses beinhaltet normalerweise das Ausstellen eines neuen Zertifikates für einen neuen Schlüssel.

Relying Party – Zertifikatsprüfer

Ist eine Entität (Kommunikationsteilnehmer (Person, Gerät oder Applikation)) die Zertifikate ihrer Kommunikationspartner nutzt um Sicherheitsziele wie z.B. Vertraulichkeit oder Authentizität zu gewährleisten.

Request for Comment (RFC)

Ein RFC (dt. Aufforderung zur Kommentierung) ist ein Papier (im übertragenen Sinne), das von der Internet Engineering Task Force (IETF) mit der Bitte um Kommentare veröffentlicht wird. Ein solches Papier stellt Vorschläge für Standards vor, die im Internet verbindlich werden sollen. Je nach Inhalt der Reaktionen (Kommentar) werden die Vorschläge abgewandelt oder verbindlich erklärt.

Rolle

Rollen werden in der IT verwendet um Verantwortlichkeiten festzulegen. Insbesondere werden sie dazu genutzt, Prozess-Verantwortliche für die unterschiedlichsten IT Prozesse zu bestimmen. Sie nennen Verantwortlichkeiten für einzelne Aktivitäten innerhalb von Arbeitsabläufen. In dieser Definition können Rollen Funktionen beinhalten und Gruppen darstellen.

RSA-Archer

Die RSA Archer Plattform bietet eine gemeinsame Grundlage für das Management von Richtlinien, Kontrollen, Risiken, Bewertungen und Mängeln über Geschäftsbereiche hinweg.

Teilnehmer

Als Teilnehmer werden alle Rollen und Verantwortlichkeiten im Kontext des Betriebs einer PKI verstanden. Dies beinhaltet:

- Administratoren verantwortlich für den Systembetrieb der einzelnen CAs
- Mitarbeiter, welche im Rahmen einer RA-Tätigkeit Zertifikatsanträge prüfen und freigeben
- Mitarbeiter, die einen Antrag zur Ausstellung eines Zertifikats stellen
- Relying Parties, also Mitarbeiter oder IT-Systeme, die ein bereits ausgestelltes Zertifikat prüfen.

Zertifikatnehmer

Als Zertifikatsnehmer werden in diesem Dokument Nutzer bzw. IT-Systeme verstanden, für deren Identität digitale Zertifikate ausgestellt werden.

14 Literaturverzeichnis

[ISO-3166-1]. (kein Datum). *International Organization for Standardization.* Abgerufen am 23. Juli 2015 von International Organization for Standardization: http://www.iso.org/

[RFC 2119], & Bradner, S. (März 1997). *Key words for use in RFCs to Indicate Requirement Levels.* Abgerufen am 02. Juli 2015 von The Internet Engineering Task Force: https://www.ietf.org/rfc/rfc2119.txt

[RFC 3647], Chokhani, S., Ford, W., Sabett, R., Merrill, C., & Wu, S. (November 2003). *Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework.* Abgerufen am 23. Juni 2015 von The Internet Engineering Task Force: https://www.ietf.org/rfc/rfc3647.txt

[RFC 6960], Myers, M., Ankney, R., Malpani, A., Galperin, S., & Adams, C. (2013). *Internet X.509 Public Key Infrastructure, Online Certificate Status Protocol - OCSP.* Abgerufen am 30. Juni 2015 von The Internet Engineering Task Force: https://www.ietf.org/rfc/rfc6960.txt

[RFC822], & Crocker, D. (August 1982). *Standard for the format of ARPA internet text messages.* Abgerufen am 30. Juni 2015 von The Internet Engineering Task Force: https://www.ietf.org/rfc/rfc822.txt

BDSG, Bundesdatenschutzgesetz. (25. Februar 2015). *Bundesministerium der Justiz und für Verbraucherschutz.* Abgerufen am 10. 08 2015 von http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf

BSI, IT-Grundschutz-Kataloge. (14. Ergänzungslieferung 2014). *Bundesamt für Sicherheit in der Informationstechnik.* Abgerufen am 15. 07 2015 von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/download/download.html

Bundesregierung, Gesetz über Rahmenbedingungen für elektronische Signaturen ... (16. Mai 2001). *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften.* Abgerufen am 24. 06 2015 von http://www.bgbl.de

DZ BANK AG, Richtlinie Informatsionssicherheits-Compilance-Evaluierung (ISM). (20. Mai 2015). Unternehmenssicherheit. *Version 001*. Frankfurt am Main, Hessen, Deutschland: DZ BANK AG.

DZ BANK AG, Richtlinie Mindestanforderungen an IT-Assets (ISM). (20. Mai 2015). Unternehmenssicherheit. *Version 001*. Frankfurt am Main, Hessen, Deutschland: DZ BANK AG.

DZ BANK AG, Technologievorgaben Backup und Archivierung Consumer IT. (15. September 2014). Informations Technologie. *Version 001*. Frankfurt am Main, Hessen, Deutschland: DZ BANK AG.

ETSI; [TS 102 042];. (Februar 2013). *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.* Abgerufen am 12. Juli 2015 von European Telecommunications Standars Institute: http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.04.01_60/ts_102042v020401p.pdf

EU; [Directive 1999/93/EC];E-Signatur in der EU. (13. December 1999). *Community framework for electronic signatures.* Abgerufen am 12. August 2015 von European Parlament and the Council: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l24118

X.501, I.-T. S. (Oktober 2014). *Open Systems Interconnection – The Directory: Models.* Abgerufen am 29. Juni 2015 von International Telecommunication Union: http://handle.itu.int/11.1002/1000/11733

X.509, I.-T. S. (Oktober 2012). *Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.* Abgerufen am 29. Juni 2015 von International Telecommunication Union: http://handle.itu.int/11.1002/1000/11735