KfW PKI
Certificate Policy

KfW Bankengruppe

KFW

Dokumentinformation

Dokumentname	KfW PKI Certificate Policy
Stand (Datum)	23.12.2021
Vertraulichkeit	Öffentlich

Tabelle 1: Dokumenteninformationen

Begriffe, Abkürzungen, Definitionen

Name
Siehe 1.6

Tabelle 2: Übersicht Begriffe, Abkürzungen, Definitionen

Mitgeltende Dokumente

Name
KfW Certificate Practice Statement

Tabelle 3: Mitgeltende Dokumente

Inhaltsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Überblick

Die KfW betreibt mehrere voneinander unabhängige PKIs mit unterschiedlichen Vertrauensbereichen.

Die Gliederung des Dokumentes erfolgt nach dem Muster des Standards RFC 3647.

Diese Certificate Policy fasst die für die Benutzer verbindlichen Anforderungen und Bedingungen der KfW als Betreiber der PKI (Public Key Infrastructure) sowie zum Zeitpunkt der Veröffentlichung dieser Certificate Policy geltenden technische Spezifikationen und interne Prozesse der KfW für die Ausstellung von Zertifikaten zur allgemeinen Verwendung in Form einer Certificate Policy (CP) zusammen.

Das zugehörige Certificate Practice Statement beschreibt die konkrete Umsetzung dieser Richtlinien.

1.1.1 Gültigkeit und Abgrenzung

Dieses Dokument bezieht sich auf die PKI-Generation 03 (ausgestellt 2019) sowie deren Folgegenerationen (04, 05…).

Frühere PKIs der KfW („KfW Root CA“, „KfW Enterprise CA“) werden explizit nicht von diesem Dokument abgedeckt.

1.1.2 KfW PKIs und Vertrauensbereiche

Die folgenden Vertrauensbereiche existieren innerhalb der KfW-PKI-Architektur für die unterschiedlichen PKIs:

PKI/Root CA CN	**Vertrauensbereich: KfW-intern vertrauenswürdig**	**Vertrauensbereich: außerhalb der KfW vertrauenswürdig**
Allgemeine PKI: **KfW Root CA 03 (…)**	OK	OK
Externe PKI: **KfW External Root CA 03 (…)**	**ausgeschlossen**[1]	OK
Interne PKI: **KfW Internal Root CA 03 (…)**	OK	**explizit ausgeschlossen**

Sofern nicht explizit anders erwähnt, beziehen sich die Vorgaben dieses Dokumentes auf alle von der KfW betriebenen PKIs mit Fokus auf die „Allgemeine PKI“.

Fallweise Unterschiede in Bezug auf Regelungen der „Externen PKI“ und der „Internen PKI“ werden explizit hervorgehoben.

1.1.2.1 Allgemeine PKI (Vertrauensanker: KfW Root CA)

Die KfW Root CA bildet den Vertrauensanker einer KfW-PKI, die Zertifikate für allgemeine Verwendung ausstellt. Es gibt keine Einschränkungen, wer dieser PKI trauen darf.

Die KfW Root CA und alle untergeordneten Issuing CAs werden von der PKI-Gruppe der KfW verwaltet.

[1] Ausnahmen und ggf. deren Risiken sind im konkreten Fall durch den Anforder im Detail zu beschreiben.

Obwohl der Hauptverwendungszweck in der Regel innerhalb der KfW selbst liegt, KÖNNEN externe Kommunikationspartner den Zertifikaten dieser PKI vertrauen.

1.1.2.2 Externe PKI (Vertrauensanker: KfW External Root CA)

Die KfW External Root CA ist der Vertrauensanker einer PKI, die nur von externen Partnern genutzt werden SOLL, beispielsweise um Kunden oder Geschäftspartner an die KfW-eigenen Systeme anzubinden, indem diesen Zertifikate unterhalb der KfW External Root CA ausgestellt werden.

Die KfW External Root CA und alle untergeordneten Issuing CAs werden von der PKI-Gruppe der KfW verwaltet.

Da hier gültige Zertifikate von externen Partnern gehalten werden, ist es nicht erwünscht, dass diese externen End Entites implizit Vertrauensbeziehungen zu beliebigen internen Systemen der KfW aufbauen können.

Aus diesem Grunde DARF die KfW External Root CA NICHT als *allgemein* vertrauenswürdige Root CA auf Systemen innerhalb der KfW konfiguriert werden.

KfW-intern DARF der KfW External Root CA fallweise nur auf genau denjenigen Systemen, die explizit als eine Relying Party für die Kommunikation mit externen Partner agieren, vertraut werden.

1.1.2.3 Interne PKI (Vertrauensanker: KfW Internal Root CA)

Externe Partner DÜRFEN dem Root-Zertifikat der „Internen PKI“ (KfW Internal Root CA) NICHT vertrauen. Diese Einschränkung wird auch deutlich durch die UserNotice im Root-CA-Zertifikat hervorgehoben.

Die KfW Internal Root CA der„Internen PKI“ ist der Vertrauensanker für alle CAs, die ausschließlich nur innerhalb der KfW vertrauenswürdig sein dürfen. Das Root-Zertifikat ist daher auf den Systemen der KfW als vertrauenswürdig verteilt.

Die KfW Internal Root CA wird von der PKI-Gruppe der KfW verwaltet. Betrieb und Verantwortung für die untergeordneten Issuing CAs können an die zuständigen Abteilungen bzw. Infrastrukturbetreiber innerhalb der KfW delegiert werden.

1.1.2.4 Weitere PKIs

Grundsätzlich sollten alle von der KfW ausgestellten Zertifikate logisch unterhalb einer der oben genannten PKIs hängen. Eventuelle Ausnahmen davon müssen unter Bezugnahme der geltenden Certificate Policy begründet werden.

Innerhalb der KfW können in solchen begründeten Ausnahmefällen weitere PKIs zur Umsetzung spezieller technischer oder organisatorischer Anforderungen bereitgestellt werden. Diese PKIs dürfen weder intern noch extern allgemein vertrauenswürdig sein, sondern sind nur explizit im Rahmen des konkreten Anwendungsfall als vertrauenswürdig zu akzeptieren.

1.2 Name und Kennzeichnung dieses Dokumentes

Name: KfW PKI Certificate Policy

Version: 0.4

Datum: 2020-06-08

Dieses Dokument wird durch folgende OIDs referenziert:

Primäre OID:

1.3.6.1.4.1.41124.10.1.1.1.1 (CP der „KfW Root CA“)

Sekundäre OIDs:

1.3.6.1.4.1.41124.10.1.1.2.1 (CP der „KfW Server CA“)

1.3.6.1.4.1.41124.10.1.1.3.1 (CP der „KfW Device CA“)

1.3.6.1.4.1.41124.10.1.1.4.1 (CP der „KfW User CA“)

1.3.6.1.4.1.41124.10.1.2.1.1 (CP der „KfW External Root CA“)

1.3.6.1.4.1.41124.10.1.2.2.1 (CP der „KfW Bankpartner CA“)

1.3.6.1.4.1.41124.10.1.2.3.1 (CP der „KfW External Issuing CA“)

1.3.6.1.4.1.41124.10.1.3.1.1 (CP der „KfW Internal Root CA“)

Weitere sekundäre OIDs können existieren.

Die Dokumenten-OIDs bleiben auch bei neuen Versionen dieses Dokumentes unverändert (siehe Kapitel 9.12).

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (CA)

Die Zertifizierungsstellen (Certification Authority, CA) sind der Teil der KfW PKI, die Zertifikate ausstellt, verteilt und Prüfmöglichkeiten (Validierung) für die Gültigkeit von Zertifikaten zur Verfügung stellt.

Die PKIs der KfW bestehen aus zwei Hierarchiestufen.

Die Root CA zertifiziert ausschließlich untergeordnete Issuing CA (Aussteller-Zertifizierungsstellen).

Die der Root CA untergeordneten Issuing CAs werden verwendet, um Zertifikate für Endsysteme oder Benutzer (End Entities) zu erstellen.

Für die KfW PKIs stehen, je nach Vertrauensbereich und Anwendungsbereich, unterschiedliche Stamm- und Zwischenzertifizierungsstellen (Root CAs, Sub CAs) zur Verfügung.

Anforderungen an die Root CAs, sowie an die von der Root CA ausgestellten Sub CA Zertifikate sind in der Certificate Policy, sowie den Certificate Practice Statements der KfW-PKI dokumentiert.

1.3.2 Registrierungsstellen (RA)

Registrierungsstellen (Registration Authoritiy, RA) verantworten die Überprüfung der Identität und Authentizität von Zertifikatsnehmern bzw. Antragstellern.

Das Registrierungsverfahren ist in Kapitel 3.2.3 dargestellt.

1.3.3 Zertifikatsnehmer

Ein Zertifikatsnehmer (End Entity) einer KfW PKI kann eine natürliche Person oder technische Entität (z. B. ein Computersystem oder ein Dienst) sein. Der Zertifikatsnehmer verwendet den privaten Schlüssel in seiner alleinigen Verfügungsgewalt.

Eine technische Entität ist ihrem Zertifikat durch eine eindeutige Kennung (z. B. den Servernamen) zuzuordnen.

Sind Zertifikatsnehmer natürliche Personen, so erfolgt die Zuordnung zwischen Zertifikat und Zertifikatsnehmer insofern eindeutig, als das Signatur-, Authentisierungs- oder Verschlüsselungszertifikat eindeutig auf die natürliche Identität (den vollen Namen) des Besitzers verweist.

1.3.4 Zertifikatsnutzer

Zertifikatsnutzer sind alle Systeme, Geräte, Softwarekomponenten, Personen und Organisationen, die Zertifikate von Zertifikatsnehmern der KfW nutzen können und/oder Zugang zu den Diensten oder Kommunikation der KfW haben, beispielsweise durch Aufbau einer Vertrauensbeziehung zu den Root-Zertifikaten der KfW PKIs.

Zertifikatsnutzer können vertrauende Dritte (Relying Parties) sein, die durch eine Vertrauensbeziehung zu einem oder mehreren Root CA Zertifikaten der KfW Kommunikationsbeziehungen der KfW akzeptieren.

Zertifikatsnutzer MÜSSEN die Einschränkungen laut Kapitel 1.1.2 beachten.

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

Zertifikate der KfW PKI DÜRFEN für die Feststellung der Identität (Authentifizierung) des Zertifikatsinhabers verwendet werden.

Der eigentliche Inhalt von Zertifikaten SOLL grundsätzlich NICHT direkt zur Autorisierung einer Kommunikationsbeziehung verwendet werden, stattdessen ist die Berechtigung zum Aufbau einer Kommunikation nach erfolgreicher Feststellung der Identität anhand des Zertifikats durch den vertrauenden Dritten durchzuführen.

Der Common Name (CN) des Zertifikats erlaubt dem vertrauenden Dritten eine eindeutige Identifikation des Zertifikatsinhabers im organisatorischen Kontext der KfW.

Die Identifikation von Zertifikatsinhabern verwendet gegebenenfalls KfW-interne Systematik.

1.4.1.1 Sicherheitsniveau

Das Sicherheitsniveau von End-Entity-Zertifikaten der KfW PKIs unterliegt folgenden praktischen Randbedingungen:

- private Schlüssel von End Entities der KfW PKIs werden in der Regel in Softwarekomponenten gespeichert (in Keystores des Betriebssystems bzw. der Anwendung oder in Schlüsseldateien wie z. B. Java Keystores oder PKCS#12).
- private Schlüssel von End Entities der KfW PKIs werden in der Regel von den End Entities selbst erzeugt und verwaltet.
- die End Entities bzw. deren Verwalter tragen selbst Verantwortung für den Schutz der privaten Schlüssel ihrer Zertifikate sowie die Einhaltung der geltenden KfW-Richtlinien, unter anderem auch in Bezug auf die Sicherheit von Schlüsselmaterial.

Zertifikate der KfW PKIs innerhalb der genannten Randbedingungen sind üblicherweise geeignet zur Endteilnehmer-Authentifizierung gegenüber Applikationen, Diensten, Servern, Netzen oder zur Authentifizierung aktiver Netzwerkkomponenten und –dienste untereinander, sowie zur Erstellung und Validierung von digitalen Signaturen.

1.4.1.2 Zertifikate für Serversysteme und Geräte

Die von den KfW PKIs zur Verfügung gestellten Zertifikate werden für Authentifizierung, digitale Signatur und Verschlüsselung im Rahmen unterschiedlicher Anwendungen je nach Belegung der keyUsage (Schlüsselverwendung) und extendedKeyUsage (Erweiterte Schlüsselverwendung) und den Festlegungen der CP/CPS eingesetzt.

Voraussetzung ist, dass ein vertrauender Dritter dem Zertifikat in angemessener Weise vertrauen kann und der Verwendungszweck nicht aufgrund von Einschränkungen dieser CP/CPS oder sonstigen Gesetzen oder Vereinbarungen verboten ist.

Einige Beispiele sind:

- Authentifizierung auf Protokoll- oder Anwendungsebene (z. B. TLS für Webserver oder ähnliche synchrone Kommunikationsbeziehungen, VPNs)
- Verschlüsselung auf Protokoll- oder Anwendungsebene (z. B. TLS, S/MIME)
- Digitale Signatur von Daten (z. B. S/MIME, Dokumentensignatur)

1.4.1.3 Zertifikate für Benutzer

Die von den KfW PKIs zur Verfügung gestellten Benutzerzertifikate werden aktuell nur für die digitale Signatur im Rahmen unterschiedlicher Anwendungen eingesetzt. Das Attribut keyUsage (Schlüsselverwendung) im Zertifikat ist auf „digital Signature“ gesetzt. Ebenso gelten die Einschränkungen aus Kapitel 1.4.1.5. Das Attribut extended keyUsage wird für diesen Anwendungsfall nicht kodiert.

Voraussetzung für die Nutzung von Benutzerzertifikaten ist, dass ein vertrauender Dritter dem Zertifikat in angemessener Weise vertrauen kann und der Verwendungszweck nicht aufgrund von Einschränkungen dieser CP/CPS oder sonstigen Gesetzen oder Vereinbarungen verboten ist.

1.4.1.4 Zertifikate für Funktionen/Software/Gruppen

In begründeten Fällen können Zertifikate für Anwendungen/Funktionen/Softwarekomponenten ausgestellt werden.

Zertifikate für Personengruppen werden zur Zeit nicht unterstützt.

1.4.1.5 Unzulässige Zertifikatsverwendung

Zertifikate der KfW dürfen nicht für nichtdienstliche oder private Zwecke verwendet werden.

Zertifikate der KfW PKIs unterstützen grundsätzlich **nicht** die RFC 5280 keyUsage nonRepudiation bzw. contentCommitment.

Es gelten die Einschränkungen laut Kapitel 1.1.2:

Zertifikate der Internen KfW PKI (unterhalb der KfW Internal Root CA) DÜRFEN NICHT außerhalb der KfW verwendet bzw. als vertrauenswürdige Zertifikate akzeptiert werden.

Zertifikate der „Externen PKI“ der KfW (unterhalb der KfW External Root CA) SOLLEN nicht innerhalb der KfW verwendet werden, es sei denn dass eine solche Verwendung explizit für die Kommunikation mit externen Partnern der KfW notwendig ist.

1.5 Verwaltung der Richtlinie

1.5.1 Zuständigkeit für das Dokument

Diese CP wird vom Betreiber der KfW PKI gepflegt.

1.5.2 Ansprechpartner und Kontakt

KfW

PKI - Team

Palmengartenstraße 5-9

60325 Frankfurt am Main

pki@kfw.de

1.5.3 Prüfung der Richtlinie

Diese Certificate Policy wird durch den Systemeigner der KfW PKI überprüft.

Der Systemeigner der KfW PKI stellt die Übereinstimmung der Certificate Practice Statements (CPS) mit den Vorgaben der jeweiligen Certificate Policy sicher.

Dieses Dokument (CP/CPS) behält seine Gültigkeit, solange es nicht vom Herausgeber (siehe Kapitel 1.5.1) widerrufen wird. Es wird bei Bedarf fortgeschrieben und erhält dann jeweils eine neue aufsteigende Versionsnummer.

Die OID dieses Dokumentes bleibt dabei unverändert (siehe Kapitel 9.12).

1.6 Definitionen und Abkürzungen

Begriff	Erläuterung
802.1x	Standard für die Authentifizierung/Autorisierung von Geräten an einem Netzwerkzugang.
AD CS	Active Directory Certificate Services - Die Active Directory Zertifikatsdienste (Active Directory Certificate Services, AD CS) sind eine Funktion von Microsofts Verzeichnisdienst Active Directory, mit der Administratoren Dienste für die Ausstellung und Verwaltung von Zertifikaten im Unternehmen mit einem öffentlichen Schlüssel erstellen können.
AD DS	Active Directory Domain Services – Serverrolle die den Aufbau einer Active-Directory-Gesamtstruktur ermöglicht. Ebenfalls ermöglicht die Rolle die Verwaltung und Speicherung von Informationen über Ressourcen von einem Netzwerk sowie von Anwendungsdaten in einer verteilten Datenbank.
ASN.1-Standard	Ist eine Beschreibungssprache zur Definition von Datenstrukturen sowie Festlegungen zur Umsetzung von Datenstrukturen und Elementen in ein netzeinheitliches Format. Sie ist gemeinsamer Standard der ITU-T und der ISO (Internationale Organisation für Normung).
AIA	Authority Information Access – Zugriff auf Ausstellerinformationen: Diese Angabe nennt Speicherorte, von denen Relying Parties das CA-Zertifikat zu einem bekannten Zertifikat erhalten können. https://tools.ietf.org/html/rfc5280#section-4.2.2.1
Asymmetrische Verschlüsselung	Public Key Verfahren – Kryptographisches Verfahren das mit einem Schlüsselpaar unterschiedlicher Schlüssel arbeitet. Dabei ist ein Schlüssel geheim (private key) und der andere Schlüssel öffentlich (public key). Der öffentliche Schlüssel wird dabei für die Verschlüsselung der Daten genutzt. Der geheime Schlüssel wird zum Entschlüsseln der verschlüsselten Daten verwendet.
Authentifizierung	Überprüfung einer Identität (Prüfung der Authentisierungsinformationen)
Authentisierung	Nachweis einer Identität
Auto Enrollment	Automatisierte Ausstellung von End Entity Zertifikaten aller Art
Autorisierung	Freigabe von Rechten nach erfolgreicher Authentifizierung
CA	Certificate Authority – Zertifikatsausgebende Stelle
CDP	CRL Distribution Point – Sperrlistenverteilpunkt der PKI. Dort werden gesperrte Zertifikate aufgelistet. https://tools.ietf.org/html/rfc5280#section-4.2.1.13
CEP	Microsoft-spezifisch: Certificate Enrollment Policy - Zertifikatregistrierungsrichtlinien-Webdienst – Ermöglicht das Abrufen von Informationen bzgl. Zertifikatsregistrierungsrichtlinien.

Certificate Policy (CP)	Sicherheitsrichtlinien der PKI und somit das Kerndokument in dem die unterstützten Prozesse/Applikationen und das angestrebte Sicherheitsniveau festgelegt werden. Siehe https://tools.ietf.org/html/rfc3647
Certification Practice Statement (CPS)	Hier und in der CP werden die verbindlichen Zertifizierungsrichtlinien für die Ausstellung von Zertifikaten zusammengefasst (inkl. Sicherheits- und Zertifizierungskonzept). Siehe https://tools.ietf.org/html/rfc3647
CES	Microsoft-spezfisch: Certificate Enrollment Web Service - Zertifikatregistrierungs-Webdienst
C-LCMP	Certificate Lifecycle Management Platform – Plattform für die Lebenszyklusverwaltung digitaler Zertifikate (Zertifikaterkennung, Zertifikatablauf etc.).
CRL	Certificate Revocation List – Von der CA signierte Zertifikatssperrliste. Enthält die Seriennummern aller zurückgezogenen Zertifikate einer CA. Siehe https://tools.ietf.org/html/rfc5280#section-5
CSR	Certificate Signing Request – Öffentlicher Teil eines Zertifikats, der der CA zur Prüfung und Signierung (Beglaubigung) vorgelegt wird. Siehe https://tools.ietf.org/html/rfc2986
Distinguished Name	Hierarchisch aufgebauter Name zur Beschreibung einer Entität im Kontext einer PKI.
DNS	Domain Name System – Dienst in einem Netzwerk zur Namensauflösung von Systemen und Diensten
EKU	Extended Key Usage – Von der CA erlaubte Verwendungsmöglichkeit für einen kryptographischen Schlüssel. Siehe https://tools.ietf.org/html/rfc5280#section-4.2.1.12
Embedded CA	Ein System mit einer „eingebetteten eigenen PKI“, das innerhalb dieses Systems eigenständig End Entity Zertifikate ausstellt.
End Entity	Zertifikatsinhaber, der Besitzer eines Zertifikats und des zugehörigen Private Key
FIPS140-2	Federal Information Processing Standard - Ist ein Standard der US-Regierung und beschreibt das Sicherheitsniveau zertifizierter Kryptohardware. Siehe https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
GPO	Microsoft-spezifisch: Group Policy Object – Gruppenrichtlinienobjekt – Sammlung von Systemeinstellungen.
Hash-Algorithmus / Hashfunktion	Die Hashfunktion/Der Hash-Algorithmus reduziert mittels Berechnung Zeichen einer beliebigen länge auf Zeichen mit einer festen länge. Ein Darüber hinaus kann die Hashfunktion als Integritätsschutz dienen, in dem ein digitaler Fingerabdruck berechnet wird.

HSM	Hardware-Sicherheitsmodul – Internes oder externes Peripheriegerät für die effiziente und sichere Ausführung kryptographischer Operationen/Applikationen.
IETF	Internet Engineering Task Force (Internettechnik-Arbeitsgruppe) ist eine Organisation, die sich mit der technischen Weiterentwicklung des Internets befasst, um dessen Funktionsweise zu verbessern.
Intermediate CA	Einer Root CA untergeordnete CA, möglicherweise mit mehreren CA-Ebenen.
Internet Assigned Numbers Authority (IANA)	ist eine Abteilung der ICANN (Internet Corporation for Assigned Names and Numbers) und für die Zuordnung von Nummern und Namen im Internet, insbesondere von IP-Adressen, zuständig.
Issuing CA	Ausgebende Zertifizierungsstelle – Zertifizierungsstelle die Zertifikate für End-Entity-Zertifikatsnutzer bereitstellt.
ITU	International Telecommunication Union (Internationale Fernmeldeunion) ist eine Sonderorganisation der Vereinten Nationen und die einzige Organisation, die sich offiziell und weltweit mit technischen Aspekten der Telekommunikation beschäftigt.
K-LCMP	Key Lifecycle Management Platform – Plattform für die Verwaltung von symmetrischen Schlüsseln (Bereitstellung, Verwaltung etc.). Übliche Bezeichnung: Key Management System (KMS)
KMIP	Key Management Interoperability Protocol - bietet einen einheitlichen Standard für die Kommunikation zwischen Krypotkomponenten. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip
Krypto-API	Application Programming Interface - Programmierschnittstelle für Programme, um auf kryptografische Methoden zugreifen können.
KU	Key Usage, von der CA erlaubte Verwendungsmöglichkeit eines Schlüssels. https://tools.ietf.org/html/rfc5280#section-4.2.1.3
LDAP	Lightweight Directory Access Protocol – Netzwerkprotokoll zur Abfrage und Änderung von Informationen und kommt bei Verzeichnisdiensten (zentrale Sammlung von Daten) zum Einsatz. https://tools.ietf.org/html/rfc4510
Life Cycle Management (LCM)	Lebenszyklusverwaltung der vorhandenen Zertifikate inkl. einer automatischen Benachrichtigung an den Stakeholder/Zuständigen.
LifeCycle Management Prozess (LCMP)	Prozess der Zertifikats-Lebenszyklusverwaltung (Verwaltung und Steuerung)
Loadbalancer	Lastverteilung – Der Loadbalancer verteilt Anfragen oder Sitzungen auf die verfügbaren Ressourcen/Server.

MAC	MAC-Adresse (Media-Access-Control-Adresse) – ist die Hardware-Adresse eines einzelnen Netzwerkadapters – Eindeutige Identifikation eines Geräts in einem Netzwerk.
NAC	Network Access Control (Netzwerkzugangskontrolle) -NAC hat zwei wesentliche Aufgaben: 1. Vollständige Übersicht über die Geräte, welche sich im Unternehmensnetzwerk befinden. 2. Überprüfung, ob die Endgeräte die sich im Netzwerk befinden den Sicherheitsanforderungen/ Sicherheitsrichtlinien des Unternehmens entsprechen
NDES	Microsoft-Terminologie: Network Device Enrollment Service - Registrierungsdienst für Netzwerkgeräte. Das zugrundeliegende Protokoll ist SCEP.
Non AD joined CA/RA	Offline betriebene CA/RA die nicht mit dem AD verbunden ist.
NTP	Network Time Protocol – Standard zur Synchronisierung von Uhren in Computersystemen.
Object Identifier (OID)	Ist ein weltweit eindeutiger Bezeichner, der benutzt wird um ein Informationsobjekt zu benennen. Ein OID stellt einen Knoten in einem hierarchisch zugewiesenen Namensraum dar, der durch den ASN.1-Standard definiert ist.
OCSP	Online Certificate Status Protocol – Protokoll zur Prüfung von Zertifikatsstatusinformationen. Liefert den Status zur Gültigkeit eines Zertifikats in einer signierten Antwort zurück.
OCSP Responder	Server der OCSP Anfragen prüft und signierte Statusinformationen bereitstellt.
PKCS	Public-Key Cryptography Standards - Standards für asymmetrische Kryptographie.
PKI	Public Key Infrastructure – Oberbegriff für eine Infrastruktur für die Ausgabe, Prüfung und Verwaltung digitaler Zertifikate. Beinhaltet zusätzlich alle technischen und organisatorischen Prozesse für den Betrieb der PKI.
Private Enterprise Number (PEN)	Private Unternehmensnummer – Diese wird von der IANA in einem öffentlichen Register erstellt und verwaltet. Dort wird ebenfalls eine öffentlich abgelegte E-Mailadresse, sowie ein Kontaktname des Unternehmens hinterlegt.
Private Key	Privater Schlüssel – Geheimer Schlüssel für die Entschlüsselung von Daten, die mit einem asymmetrischen Verschlüsselungsverfahren verschlüsselt wurde und für die Signatur elektronischer Daten.
Public Key	Öffentlicher Schlüssel mit dem bei asymmetrischen Verschlüsselungsverfahren elektronische Daten verschlüsselt werden.
RA	Registration Authority - Registrierungsstelle für dig. Zertifikate. Sie prüft die Richtigkeit der Daten im gewünschten Zertifikat und genehmigt den Zertifikatsantrag.
Relying Party	Kommunikationsteilnehmer (Empfänger) einer Kommunikation, die mit (X.509v3) Zertifikaten abgesichert ist. Die Relying Party prüft die Gültigkeit des übermittelten End Entity Zertifikats des Kommunikationspartners

	kryptographisch, in Bezug auf den Zertifikatsstatus der Zertifikatskette sowie gegen die Liste seiner vertrauenswürdigen Root-CA-Zertifikate.
Reverse Proxy	Netzwerkkomponente, die Anfragen (z. B. HTTP) auf logischer Ebene entgegennimmt und an ein Zielsystem weiterreicht. Wird als zusätzliche Sicherheitskomponente vor einen oder mehrere Webserver geschaltet, um Anfragen aus dem Internet stellvertretend entgegenzunehmen und an einen Backend-Server im Hintergrund weiterzuleiten.
Root CA	Stammzertifizierungsstelle – Höchste Vertrauensinstanz einer PKI
RSA	Rivest–Shamir–Adleman - Asymmetrisches Verfahren zum Verschlüsseln/ digitalen Signieren.
SAN	Subject Alternative Name – Um ein SSL-Server-Zertifikat auf einem Server unter mehreren Host-Namen einsetzen zu können, muss das Zertifikat alle diese Host-Namen als sogenannte alternative Namen (SAN) enthalten.
S/MIME	Secure / Multipurpose Internet Mail Extensions - Standard zum Verschlüsseln/Signieren von E-Mails. Siehe https://tools.ietf.org/html/rfc5751
SCCM	Microsoft System Center Configuration Manager – Tool zur zentralisierten Verwaltung von Hard- und Software (bspw. Inventarisierung, Softwareverteilung).
SCEP	Simple Certificate Enrollment Protocol – Ermöglicht einem vertrauenswürdigen Gerät die Anforderung /Ausstellung eines Zertifikats (ggf. authentisiert über ein zeitlich begrenztes Einmalkennwort).
SCVP	Server-based Certificate Validation Protocol – Ist ein Internet-Protokoll dass es Clients ermöglicht eine X.509-Zertifikatskette aufzubauen und deren Validierung auszulagern
SHA-1	Secure Hash Algorithm (erzeugt 160 Bit Hashwerte)
SHA-2	Oberbegriff für eine Sammlung von vier kryptographischen Hashfunktionen: - SHA-224 – 28 bytes (224 Bit) - SHA-256 – 32 bytes (256 Bit) - SHA-384 – 48 bytes (384 Bit) - SHA-512 – 64 bytes (512 Bit)
Signatur	Echtheitsbestätigung für elektronische Daten, die mittels eines Signaturalgorithmus (Anwendung eines privaten Schlüssels auf den Hash der zu signierenden Daten) erzeugt wird.
SMTP	Simple Mail Transfer Protocol – Protokoll zum E-Mail-Versand
SSO	Single Sign-on – "Einmalanmeldung" – Ein Benutzer kann sich nach einmaliger Authentifizierung an mehreren Programmen/Diensten anmelden für die er vorher berechtigt wurde.

Stammzertifikat	Ein Stammzertifikat identifiziert eine Zertifizierungsstelle (CA). Mit diesem Stammzertifikat signiert eine Root CA ein oder mehrere untergeordnete Zertifikate. Siehe Root CA.
Sub CA	Untergeordnete Zertifizierungsstelle in einer PKI Hierarchie, siehe Intermediate CA
TLS/ SSL	Transport Layer Security (TLS), Secure Sockets Layer (SSL) - Ist ein hybrides Verschlüsselungsprotokoll zur Datenübertragung im Internet. Siehe https://tools.ietf.org/html/rfc5246
VA	Verification Authority - Validierungsdienst
VIV	IT-Sicherheitsziele/Schutzziele – Vertraulichkeit, Integrität, Verfügbarkeit
VPN	Virtuelles Privates Netzwerk - Über VPN können lokale Netze über das Internet sicher miteinander verbunden werden.
WAF	Web Application Firewall - Analysiert den Verkehr zwischen Clients und Webservern auf Anwendungsebene, somit schützt sie Webanwendungen vor Angriffen über das HTTP Protokoll.
WAN	Wide Area Network – "Großräumiges Netzwerk", kann aus mehreren LANs bestehen (auch über Länder oder Kontinente).
X.509v3	Standard für die Erstellung von Zertifikaten Siehe https://tools.ietf.org/html/rfc5280
Zertifikat	Elektronischer Ausweis der von einer CA ausgestellt und durch deren digitale Signatur beglaubigt wurde.
Zertifikatsnutzer	Maschinen, Anwender oder Prozesse die digitale Zertifikate verwenden, siehe End Entity

2 Verantwortung für Veröffentlichung und Verzeichnisse

2.1 Verzeichnisse

Die KfW veröffentlicht CA-Zertifikate, Sperrinformationen sowie die Certificate Policy ihrer PKIs

- auf öffentlichen Web-Servern (erreichbar aus dem Internet)
- auf Web-Servern im internen Netzwerk der KfW (nicht erreichbar aus dem Internet)

Es werden keine LDAP-Verzeichnisse verwendet.

2.2 Veröffentlichung von Zertifikatsinformationen

Von der KfW PKI ausgestellte End-Entity-Zertifikate werden derzeit nicht in Verzeichnisdiensten veröffentlicht.

Die KfW-Root-Zertifikate und die Sperrlisten der KfW CAs werden im internen Netz veröffentlicht.

2.3 Aktualisierung von Veröffentlichungen (Zeitpunkt, Frequenz)

2.3.1 Artefakte der KfW PKIs

Für die Veröffentlichung von CA-Zertifikaten, Sperrlisten und CP bestehen folgende Zeitpläne:

- Root-Zertifikate: unmittelbar nach der Erzeugung
- Issuing-CA-Zertifikate: zu Beginn der aktiven Tätigkeit
- Sperrlisten: schnellstmöglich
- CP: nach Aktualisierung und Freigabe

2.3.2 Vorläufiger Zeitplan

Die KfW PKI ist auf langfristigen Betrieb ausgelegt. Um diesen zu gewährleisten, finden in regelmäßigen Abständen geplante PKI-Aktivitäten statt.

Der folgende Kalender gibt einen Ausblick auf die aktuell geplanten Aktivitäten der nächsten Jahre.

Hervorgehobene Aktivitäten erfordern Mitarbeit bzw. Kooperation der vertrauenden Parteien (Relying Parties) bzw. der Nutzer der PKI.

2019-04: Root-CA-Zeremonie Generation 03

- Erstellung KfW Root CA 03

- Erstellung KfW External Root CA 03

- Erstellung KfW Internal Root CA 03

2019-05: Verteilung der Root CAs Generation 03
Vertrauende Dritte müssen die verteilten Root-Zertifikate als vertrauenswürdig importieren.

2019-09: Issuing-CA-Zeremonie Generation 03.1 für:

- Erstellung KfW Server CA 03.1

2020-03: Weitere Issuing CA-Zeremonien der Generation 03.1 für:

- Erstellung KfW User CA 03.1

- Erstellung KfW External Issuing CA 03.1

2023-04: Root-CA-Zeremonie Generation 04

- Erstellung KfW Root CA 04
- Erstellung KfW External Root CA 04
- Erstellung KfW Internal Root CA 04

2023-04 – 2024-04: Verteilung der Root-CAs Generation 04.
Vertrauende Dritte müssen die verteilten Root-Zertifikate als vertrauenswürdig importieren.

2024-04: Issuing-CA-Zeremonie Generation 04.1

- Erstellung KfW Server CA 04.1
- Erstellung KfW User CA 04.1

2.4 Zugang zu Informationsdiensten

Der lesende Zugriff auf die unter den Ziffern 2.1 und 2.2 aufgeführten Informationen ist nicht eingeschränkt.

Die Informationsdienste sind 7x24h Stunden online verfügbar.

Der schreibende Zugriff liegt im Verantwortungsbereich der KfW PKI.

3 Identifikation und Authentifizierung

3.1 Namenskonventionen

3.1.1 Namensformen

Ein Distinguished Name (DN) ist innerhalb der KfW PKI ein eindeutiger Name für Verzeichnisobjekte nach dem X.500-Standard.

Mit dem Distinguished Name ist eine eindeutige Unterscheidbarkeit von Systemen und Personen gegeben.

Die Namenskonventionen für DNs sollen unterstützen, dass kein digitales Zertifikat für verschiedene End Entities unter demselben Namen ausgestellt wird.

Innerhalb eines Zertifikates ist zu unterscheiden nach

- IssuerDistinguishedName (Issuer DN)
- SubjectDistinguishedName (Subject DN)

Der Issuer DN repräsentiert den eindeutigen Namen der ausstellenden Zertifizierungsstelle (CA). Es gelten die Namensformen analog zum Subject DN.

3.1.1.1 Namensformen für CAs

Der CN eines CA-Zertifikates beschreibt den Zweck der CA möglichst präzise, jedoch allgemein genug, um späteren Erweiterungen der CA nicht im Wege zu stehen.

Die KfW PKI ist darauf angelegt, dauerhaft betrieben zu werden, wenngleich sich die KfW die Beendigung des Betriebs der PKI vorbehält. Die Namenskonventionen der CA-Zertifikate tragen dem Rechnung, indem eine Systematik für die fortlaufende Benennung von CA-Zertifikaten angewendet wird, mit der „Generationen“ von CA-Zertifikaten innerhalb des CN unterschieden werden können.

Die erste CA-Generation von PKIs im Geltungsbereich dieser Certificate Policy beginnt mit der Generations-ID 03.

CA-Zertifikate verwenden die klassische X.500-Namenskonvention mit folgendem DN:

`CN=`*<Name, Generation, ggf. SubCA-Generation >*`, OU=PKI, O=KfW, C=DE`

Der Basis-DN `OU=PKI, O=KfW, C=DE` wird von allen CAs der KfW Bankengruppe verwendet.

Der Common Name einer CA ist eineindeutig und beschreibt den Zweck der CA.

3.1.1.2 Namensformen für End Entities

End Entities verwenden die klassische X.500-Namenskonventionen mit folgendem DN-Format:

```
CN=<Name>, E=<Email>, OU=<Organisationseinheit>, O=KfW, L=<Stadt>,
S=<Bundesland>, C=DE
```

Das Attribut C enthält die weltweite Landeskennung. Festgelegt ist ein aus zwei Buchstaben bestehender Code, welcher in ISO 3166-1, Alpha-2 (International Organization for Standardization) spezifiziert ist. Dieses Feld spezifiziert das Land, in welchem der Zertifikatsinhaber niedergelassen ist.

Beispiele:

C = DE für Deutschland

Die Attribute L (Stadt) und S (Bundesland) werden je nach Ort der End Entity gesetzt (z. B. L=Frankfurt, S=Hessen).

Das Attribut O wird mit „KfW“ belegt.

Das Attribut OU wird auf die Organisationseinheit des Zertifikatsinhabers gesetzt.

Bei Systemen wird das Attribut E (Email) mit der Email-Adresse einer Support-Gruppe oder eines für das System verantwortlichen Person belegt. Gruppen-Adressen sind Personen-Adressen vorzuziehen.

Bei Systemen wird das Attribut CN (Common Name) mit dem eindeutigen primären Systemnamen belegt (FQDN, Fully Qualified Domain Name).

Es ist gestattet, dem FQDN einen Zusatz hinzuzufügen, der die Zertifikatsverwendung beschreibt, um mehrere Zertifikate für ein System auseinanderhalten zu können. Dieser Zusatz wird in der Regel durch einen Doppelpunkt vom FQDN abgetrennt (Beispiel: „host.example.com:anwendung“).

Hostnamen ohne Domain-Anteil im CN SOLLTEN vermieden werden. Falls es technische Gründe für die Verwendung solcher isolierter Hostnamen gibt, KÖNNEN diese verwendet werden.

3.1.1.2.1 Subject Alternative Names

Konventionen für die Bestandteile „Subject Alternative Name“ (SAN):

Die Einträge im Feld „Alternativer Antragstellername“ (Subject Alternative Name, SAN) sind abhängig von den jeweiligen Zertifikatstypen (Benutzer, System).

Die Erweiterung „Subject Alternative Name“ SOLL mindestens einen Eintrag „DNS-Name“ enthalten. Eine Ausnahme kann für Systeme gelten, die keinen eigenen Eintrag im DNS haben und denen die extendedKeyUsage „serverAuth“ fehlt.

Die Erweiterung „Subject Alternative Name“ KANN mehrere Einträge enthalten, sofern das fachlich durch die Verwendung des Zertifikats gerechtfertigt ist.

Aus technischen Gründen (Vermeidung von Interoperabilitätsproblemen mit mangelhaft implementierter Software von vertrauenden Dritten) SOLLTE vermieden werden, mehr als ca. 35 Subject Alternative Names in einem Zertifikat einzutragen.

Die Einträge im SAN können aus folgenden SAN-Typen zusammengesetzt sein:

3.1.1.2.1.1 DNS Name

Dieses Attribut wird bei Servern, Systemen und Geräten verwendet.

Der vollständige Name eines Systems wird als Fully Qualified Domain Name (FQDN) bezeichnet und kennzeichnet eine exakte Position in der Baumstruktur der DNS-Hierarchie. Das Feld „FQDN“ besteht mindestens aus Top-Level und weiteren Sub-Domains zuzüglich eines Hostnamens.

Beispiele:

FQDN = www.example.com

FQDN = example.kfw.de

Bei Server-Zertifikaten wird der FQDN als Pflichtfeld im Subject-DN als „Common Name“ eingetragen und in der Erweiterung „Alternativer Antragstellername“ (Subject Alternative Name) als „DNS-Name“ angezeigt.

3.1.1.2.1.2 RFC822 Name

Dieses Attribut SOLL nur bei Personenzertifikaten verwendet werden.

Der RFC822-Name entspricht der E-Mail-Adresse des Zertifikatsbesitzers. Bei Email-Gruppenzertifikaten entspricht dies der Email-Adresse der Gruppe.

3.1.1.2.1.3 IP Adress

IP-Adressen SOLLEN in Subject Alternative Names nicht verwendet werden.

Es ist stattdessen ein FQDN als DNS-Name einzutragen. Seltene Ausnahmen können in begründeten Einzelfällen vom PKI-Team genehmigt werden, z. B. wenn Fehler in Software-Produkten dies erforderlich machen.

3.1.1.2.1.4 Other Name

Für Domain-Controller-Zertifikate wird die „Microsoft-GUID“ (MSGUID) als Eintrag „DNS-Objekt-Guid“ unter „Other Name“ in der Erweiterung Subject Alternative Name als otherName aufgenommen.

Ein „otherName“ Subject Alternative Name mit dem proprietären Typ „User Principal Name“ (UPN) wird in Smartcard-LogOn-Zertifikaten von Benutzern verwendet.

3.1.2 Aussagekraft von Namen

Der Name des ausgestellten Zertifikates (DN) muss den Zertifikatsnehmer eindeutig und nachprüfbar identifizieren.

Es gelten die folgenden Regelungen:

- Zertifikate für Systeme werden auf den vollen Systemnamen, ggf. zuzüglich weiterer beschreibender Qualifizierer (siehe 3.1.1.2) innerhalb des CN ausgestellt
- Zertifikate für natürliche Personen sind auf den vollen Namen des Zertifikatsnehmers auszustellen.
- Zertifikate für Personengruppen sowie für organisationsbezogene Postfächer müssen sich deutlich erkennbar von Zertifikaten für natürliche Personen unterscheiden

3.1.3 Pseudonymität bzw. Anonymität von Zertifikatsinhabern

Benutzerzertifikate werden aktuell ausschließlich für Signaturanwendungen genutzt. In diesem Fall ist die Verwendung von Pseudonymen in Zertifikaten nicht gewünscht.

3.1.4 Regeln zur Interpretation verschiedenerer Namensformate

Keine Bestimmungen.

3.1.5 Eindeutigkeit von Namen

3.1.5.1 CA-Namen

Der Name von CA-Zertifikaten ist innerhalb der KfW PKIs eineindeutig.

3.1.5.2 End Entities (Systeme und Server): Anzahl gültiger Zertifikate pro DN

Ein DN muss eine End Entity eindeutig beschreiben. Bei der Vergabe von Namen für Systeme MUSS sichergestellt sein, dass der gewählte DN innerhalb der ausstellenden CA eindeutig ist.

Für einen gegebenen DN SOLL in der Regel zu jedem Zeitpunkt nur ein einziges Zertifikat gültig sein.

Muss ein Zertifikat aus technischen oder organisatorischen Gründen für denselben DN neu ausgestellt werden (z. B. wegen einer fehlerhaften Beantragung), sind alle vorhergehenden Zertifikate mit demselben DN zu sperren, so dass nur ein gültiges Zertifikat für den DN existiert.

Nähert sich ein Zertifikat dem Ende einer Gültigkeit, KANN ein neues Zertifikat für denselben DN ausgestellt werden, um nahtlos vom alten zum neuen Zertifikat umschalten zu können (Zertifikatsverlängerung, Certificate Renewal bzw. Rekeying, siehe Kapitel 4.7)

Die Ausstellung eines Verlängungs-Zertifikats für einen DN KANN in einem Zeitraum von bis zu 90 Tagen vor Laufzeitende des bestehenden Zertifikats erfolgen.

Bei Ausstellung des Verlängerungs-Zertifikats bleibt das alte Zertifikat bis zum natürlichen Ablauf weiterhin gültig.

Während dieser Verlängerungs-Frist KÖNNEN zwei Zertifikate mit demselben DN gleichzeitig gültig sein.

3.1.5.3 End Entities (Benutzer und Gruppen): Anzahl gültiger Zertifikate pro DN

Für Benutzer (natürliche Personen) können je nach Zertifikatstyp unterschiedlich viele Zertifikate mit demselben eindeutigen Subject-DN ausgestellt sein, die sich jedoch in der Schlüsselverwendung bzw. erweiterten Schlüsselverwendung und der Zertifikatsseriennummer unterscheiden (getrennte

Zertifikate für Authentifizierung, Signatur und Verschlüsselung). Authentisierungszertifikate und Verschlüsselungszertifikate können jeweils 3 vom gleichen Typ unter obigen Voraussetzugnen nebeneinander gültig sein. Die Anzahl der Signaturzertifikate pro Benutzer ist nicht eingeschränkt. Jedoch SOLL auf jedem Windows Client in der KfW pro Benutzerprofil nur ein gültiges Signaturzertifikat für die angemeldete Benutzerkennung existieren.

Durch die Erneuerung ablaufender Zertifikate KÖNNEN zudem zeitlich begrenzt auch mehrere nicht gesperrte Zertifikate mit dem gleichen Subject-DN und gleicher Schlüsselverwendung vorhanden sein.

3.1.5.4 End Entities (Technische Benutzer-Konten): Anzahl gültiger Zertifikate pro DN

Zertifikate für technische Konten (Systembenutzer) müssen sich von natürlichen Personen und Server-Zertifikaten unterscheiden. Auf einem System können mehrere Zertifikate für technische Benutzer existieren. Diese Zertifikate MÜSSEN sich im Subject DN unterscheiden, beispielsweise durch Hinzufügen von Qualifizierern zu dem Subject CN (siehe 3.1.1.2).

Durch die Erneuerung ablaufender Zertifikate KÖNNEN zudem zeitlich begrenzt auch mehrere nicht gesperrte Zertifikate mit dem gleichen Subject-DN und gleicher Schlüsselverwendung vorhanden sein.

3.1.6 Erkennung, Authentifizierung und Funktion von Warenzeichen

Für die „Allgemeine KfW PKI“ und die „Interne KfW PKI“ existieren keine besonderen Bestimmungen.

Für die „Externe KfW PKI“ gilt:

Im Rahmen der Beantragung von Zertifikaten für Geschäftspartner der KfW DÜRFEN nur solche Namensbestandteile innerhalb des Zertifikatsantrags oder Zertifikats des Antragsstellers verwendet werden, zu deren Verwendung dieser berechtigt sind.

Mit Antragstellung bei der „Externen KfW PKI“ bestätigt der Antragsteller, die verwendeten Namen und Namensbestandteile im Zertifikatsantrag verwenden zu dürfen.

Diese Berechtigung wird seitens der KfW bei der Registrierung nicht geprüft.

3.2 Authentisierung bei initialer Beantragung

3.2.1 Nachweis zum Besitz des privaten Schlüssels

Der Zertifikatsinhaber MUSS bei einem Neuauftrag gegenüber der Zertifizierungsstelle in geeigneter Weise nachweisen, dass er im Besitz des privaten Schlüssels ist, der dem zu zertifizierenden öffentlichen Schlüssel zugeordnet ist.

Der Besitznachweis KANN durch eine vom Antragsteller selbst erzeugten Datenstruktur im PKCS#10-Format erbracht werden.

Diese Anforderung gilt nicht, wenn die Schlüsselerzeugung durch die Zertifizierungsstelle selbst stattfindet, z. B. bei Schlüsselpaaren für Benutzer-Verschlüsselungszertifikate. In diesem Fall ist die Zuordnung zwischen öffentlichem und geheimem Schlüssel implizit gegeben.

3.2.2 Anforderungen an die organisatorische Zugehörigkeit von Antragstellern oder Teilnehmern in Bezug auf Identifikation und Authentifizierung

3.2.2.1 Allgemeine PKI der KfW

Zertifikate der „Allgemeinen PKI“ werden nur für Endnutzer (Systeme, Geräte, ggf. Personen) ausgestellt, die der KfW organisatorisch zugeordnet werden können.

3.2.2.2 Externe PKI der KfW

Zertifikate der „Externen PKI“ KÖNNEN für Endnutzer (Organisationen, Systeme) außerhalb der KfW ausgestellt werden. Falls eine entsprechende fachliche Anforderungen besteht, KÖNNEN diese

ausnahmsweise auch KfW-interne Endnutzer Zertifikate der „Externen PKI“ erhalten (eine generelle Vertrauensbeziehung zur „Externen PKI“ durch KfW-interne vertrauende Dritte DARF nicht eingerichtet werden, siehe 1.1.1).

3.2.2.3 Interne PKI der KfW

Zertifikate der „Internen PKI“ DÜRFEN nur für Antragsteller innerhalb der KfW vergeben werden.

3.2.3 Authentifizierung und Identifizerung von Teilnehmern

3.2.3.1 Allgemeine PKI der KfW

Für einen Zertifikatsantrag an die „Allgemeine PKI“ der KfW wird der Antragsteller durch seinen Benutzerlogin auf den KfW-internen Systemen identifziert, über die der Antrag gestellt wird.

Der Endteilnehmer bzw. Zertifikatsinhaber kann z. B. ein System unter der Verwaltung des Antragstellers sein, in diesem Fall stellt ein genehmigter Change die Beziehung zwischen Antragsteller und Endteilnehmer her.

3.2.3.2 Externe PKI der KfW

Zertifikatsanträge werden von externen Partner der KfW über die vereinbarten Kommunikationsmechanismen eingereicht.

Eine Prüfung der Antragsunterlagen und der Identität des Antragsstellers findet durch die zuständigen Mitarbeiter im Partnermanagement der KfW statt.

3.2.3.3 Interne PKI der KfW

Die Authentifizierung von Antragstellern für Zertifikate der „Internen PKI“ obliegt den Betreibern der betreffenden Aussteller-CA.

3.2.4 Nicht überprüfte Teilnehmerangaben

3.2.4.1 Allgemeine PKI der KfW

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

3.2.4.2 Externe PKI der KfW

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

3.2.4.3 Interne PKI der KfW

Die Authentifizierung von Antragstellern für Zertifikate der „Internen PKI“ obliegt den Betreibern der betreffenden Aussteller-CA.

3.2.5 Berechtigungsprüfung

3.2.5.1 Allgemeine PKI der KfW

Die Berechtigungsprüfung erfolgt auf Basis des etablierten Change-Prozesses der KfW. Ein Antragsteller muss einen genehmigten Change für das auszustellende Zertifikat vorweisen. Ein eingereichter Zertifikatsantrag wird fachlich mit dem genehmigten Change abgeglichen. Sofern der Change die Zertifikatsausstellung rechtfertigt, wird das Zertifikat ausgestellt.
Alternativ kann für bestimmte Zertifikatstypen (z.B. Signaturzertifikate die per Autoenrollment verteilt werden) ein Antrag im KfW Webshop auf die Mitgliedschaft der entsprechenden Gruppe gestellt werden. Die Genehmigung erfolgt über die Standard Berechtigungsprozesse. Bei einem positiven Bescheid erhält der Antragssteller die Gruppenmitgliedschaft und somit auch das Zertifikat.

3.2.5.2 Externe PKI der KfW

Die Berechtigungsprüfung erfolgt durch die für die jeweiligen Geschäftsvorfälle fachlich verantwortlichen Mitarbeiter der KfW. Bei erfolgreicher Berechtigungsprüfung wird das Zertifikat des Antragstellers ausgestellt.

3.2.5.3 Interne PKI der KfW

Die Berechtigungsprüfung von Antragstellern für Zertifikate der „Internen PKI“ obliegt den Betreibern der betreffenden Aussteller-CA.

3.2.6 Kriterien für Interoperabilität

Die Zertifikate der KfW PKIs sind konform zu RFC5280 (X.509v3).

Untergeordnete CAs der KfW PKI MÜSSEN die CP/CPS der KfW PKI einhalten.

Die CP und CPS der KfW PKIs legen Kriterien fest, die die technische und fachliche Interoperabilität administrativ einschränken können.

3.3 Identifikation und Authentifizierung bei einer Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Die Identifikation und Authentifizierung eines Zertifikatsinhabers KANN durch Digitale Signatur mit dem alten, gültigen Zertifikat des Zertifikatsinhabers erfolgen. Ebenso KANN die Ereuerung von Zertifikaten welche auf Grund einer Gruppenmitgliedschaft ausgestellt wurden, über die immernoch valide Gruppenmitgliedschaft erfolgen.

Alternativ MUSS die Identifikation und Authentifizierung bei einer manuellen Zertifikatserneuerung entsprechend der initialen Beantragung erfolgen.

3.3.2 Zertifikatserneuerung nach einer Sperrung

Die Identifikation und Authentifizierung bei einer Zertifikatserneuerung nach einer Sperrung des Zertifikats erfolgt analog zur initialen Beantragung.

3.3.3 Zertifikatserneuerung nach Ablauf des Gültigkeitszeitraumes

Die Identifikation und Authentifizierung bei einer Zertifikatserneuerung nach Ablauf des Zertifikats erfolgt analog zur initialen Beantragung.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Identifikation von Sperranträgen läuft analog zu der Zertifikatsbeantragung ab.

Für eingeschränkte, uniforme Gruppen von Endnutzern (Endgeräten) können die verwaltenden Systeme automatisiert Sperranträge erzeugen und zur Verarbeitung an die KfW PKI senden. Auf Basis dieser Vereinbarung können Massensperrungen umgesetzt werden.

4 Anforderungen zum Lebenszyklus von Zertifikaten

4.1 Zertifikatsbeantragung

Die in diesem Kapitel adressierten Registrierungsprozesse beziehen sich auf die Beantragung und Ausstellung von Endnutzer-Zertifikaten durch Aussteller-CAs unterhalb der Root CAs.

Aktivitäten der Root CAs werden von den Mitarbeitern der PKI-Abteilung geplant und durch den KfW-internen Change-Prozess sowie in den CPS dokumentiert und werden in diesem Kapitel nicht berücksichtigt.

4.1.1 Berechtigung zur Zertifikatsbeantragung

Antragsteller erhalten Zertifikate unter der grundlegenden Bedingung, dass die vorliegende Certificate Policy akzeptiert wird.

4.1.1.1 Allgemeine PKI der KfW

Zertifikate unterhalb der „Allgemeinen PKI“ der KfW können von technisch oder logisch zur KfW gehörenden IT-Systemen beantragt werden.

Sofern die „Allgemeine PKI“ Personen- oder Gruppenzertifikate ausstellt, können diese von internen oder externen Mitarbeitern der KfW bzw. den technisch Verantwortlichen für die Verwaltung von Benutzergruppen beantragt werden.

Zur Beantragung von Zertifikaten der „Allgemeinen PKI“ der KfW sind logischer Zugang zu den für die Beantragungssprozesse verwendeten Systeme der KfW sowie die entsprechenden fachlichen Berechtigungen des Antragstellers erforderlich.

4.1.1.2 Externe PKI der KfW

Zertifikate der „Externen PKI“ KÖNNEN von Geschäftspartnern der KfW beantragt werden.

4.1.1.3 Interne PKI der KfW

Zertifikate der „Internen PKI“ KÖNNEN von berechtigten Systemen der KfW für rein interne Verwendung beantragt werden.

4.1.2 Registrierungsprozess und Zuständigkeit

4.1.2.1 Allgemeine PKI der KfW

4.1.2.1.1 Manuelle Registrierung

Die manuelle Registrierung von Teilnehmern erfolgt über den KfW-internen Prozess für das Change Management. Antragsteller verwenden PKI-spezifische Vorlagen im zentralen System zur Erfassung von Anträgen zur Beantragung der Ausstellung oder Sperrung von Zertifikaten.

4.1.2.1.2 Automatische Registrierung

Die „Allgemeine PKI“ der KfW unterstützt automatisierte Zertifikatsanträge durch Systeme der KfW. Zu diesem Zweck existieren automatisierte Registrierungsstellen, die von den Systemen erzeugte Zertifikatsanträge über programmatische Schnittstellen entgegennehmen und verarbeiten.

4.1.2.2 Externe PKI der KfW

Externe Antragsteller reichen Zertifikatsanträge über einen für die jeweilige fachliche Anwendung/Vertragsbeziehung definierten Weg ein

4.1.2.3 Interne PKI der KfW

Die Registrierung von Antragstellern der „Internen PKI“ liegt im Verantwortungsbereich des internen Betreibers der betreffenden Aussteller-CA.

4.2 Bearbeitung von Zertifikatsanträgen

4.2.1 Durchführung von Identifikation und Authentifizierung

4.2.1.1 Allgemeine PKI der KfW

4.2.1.1.1 Manuelle Registrierung

Die Identitätsfeststellung erfolgt durch das KfW-interne Authentisierungssystem. Die Benutzerkennung des angemeldeten Benutzers wird bei der Erfassung des Zertifikatsantrags vom System automatisch mit dem Zertifikatsantrag verknüpft und gespeichert.

4.2.1.1.2 Automatische Registrierung

Die Identitätsfeststellung von Systemen oder Personen mit automatischer Registrierung erfolgt durch Standardmechanismen des Betriebssystems auf Basis der administrativen Zugehörigkeit zur IT-Infrastruktur der KfW.

Sofern Standard-Protokolle zur automatisierten Registrierung von Systemen oder Personen zum Einsatz kommen, werden die in den Protokollen definierten Authentisierungsverfahren für die Beantragung von Zertifikaten genutzt.

4.2.1.2 Externe PKI der KfW

Die Identität des Antragstellers für den Erhalt eines Zertifikats der „Externen PKI“ der KfW wird von der zuständigen Fachabteilung unter Verwendung eines getrennten Kommunikationskanals geprüft.

4.2.1.3 Interne PKI der KfW

Die Identifikation von Antragstellern der „Internen PKI“ liegt im Verantwortungsbereich des internen Betreibers der betreffenden Aussteller-CA.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

4.2.2.1 Allgemeine PKI der KfW

4.2.2.1.1 Manuelle Registrierung

Die Berechtigung des Benutzers für die beantragten Artefakte wird automatisch im Rahmen des Change-Prozesses geprüft.

Zusätzlich zu der Berechtigungsprüfung im Rahmen des Change Mangements erfolgt eine fachliche Prüfung des Zertifikatsantrags unter Berücksichtigung der Vorgaben der Certificate Policy sowie der Certificate Practice Statements, z. B. in Bezug auf Vollständigkeit und (technische) Korrektheit des Antrags, Einhaltung von Namenskonventionen sowie die Anzahl gültiger Zertifikate für den beantragten Namen.

4.2.2.1.2 Automatische Registrierung

Automatisch verarbeitete Zertifikatsanträge werden automatisch auf Basis der Standardmechanismen des Betriebssystemherstellers autorisiert. In der Regel bedingt eine administrative Domänenzugehörigkeit bzw. eine spezifisiche Zugehörigkeit in einer Gruppe oder Organizational Unit der Domäne zu den Systemen der KfW die implizite Berechtigung zum Erhalt eines Zertifikats.

4.2.2.2 Externe PKI der KfW

Die zuständige Fachabteilung überprüft die Berechtigung des externen Antragstellers durch Abgleich mit den vorliegenden Partnerdaten sowie anhand des bestehenden Geschäftsverhältnisses.

4.2.2.3 Interne PKI der KfW

Die Berechtigungsprüfung für Anträge an die „Interne PKI“ liegt im Verantwortungsbereich des internen Betreibers der betreffenden Aussteller-CA.

4.2.3 Bearbeitungsdauer von Zertifikatsanträgen

4.2.3.1 Allgemeine PKI der KfW

4.2.3.1.1 Manuelle Registrierung

Die Bearbeitungsdauer von Zertifikatsanträgen ist abhängig von verschiedenen Faktoren, unter anderem der Vollständigkeit und Korrektheit der Antragsdaten oder von der Auslastung der Registrierungsstelle und der vorgelagerten Genehmiger.

In der Regel erfolgt eine Zertifikatsausstellung innerhalb eines Arbeitstages nach Antragstellung. Deutlich längere Bearbeitungszeiten sind möglich, z. B. falls Antragsdaten fehlerhaft oder unvollständig sind und eine Wiederholung der Antragsstellung oder sonstige Mitwirkung des Antragstellers erfordern.

Es existierten keine verbindlichen Zusagen für die maximale Bearbeitungsdauer.

4.2.3.1.2 Automatische Registrierung

Die Zertifikatsaustellung bei automatischen Antragsprozessen erfolgt in der Regel unmittelbar nach erfolgreicher automatischer Berechtigungsprüfung.

4.2.3.2 Externe PKI der KfW

Die Bearbeitungsdauer von Zertifikatsanträgen ist abhängig von verschiedenen Faktoren, unter anderem der Vollständigkeit und Korrektheit der Antragsdaten, oder von der Auslastung der Registrierungsstelle und der vorgelagerten Genehmiger.

In der Regel erfolgt eine Zertifikatsausstellung innerhalb von zehn Arbeitstagen nach Antragstellung. Längere Bearbeitungszeiten sind möglich, z. B. falls Antragsdaten fehlerhaft oder unvollständig sind und eine Wiederholung der Antragsstellung oder sonstige Mitwirkung des Antragstellers erfordern.

Es existierten keine verbindlichen Zusagen für die maximale Bearbeitungsdauer.

4.2.3.3 Interne PKI der KfW

Die Bearbeitungsdauer für Anträge an die „Interne PKI“ liegt im Verantwortungsbereich des internen Betreibers der betreffenden Aussteller-CA.

4.3 Ausstellung von Zertifikaten

4.3.1 Aufgaben der Zertifzierungsstelle

Nach positiver Prüfung und Freigabe des Zertifikatsantrags durch die Registrierungsstelle wird das Zertifikat von der Zertifizierungsstelle unter Berücksichtigung eventueller administrativer Änderungen oder Vorgaben der Registrierungsstelle ausgestellt.

Die Zertifizierungsstelle vermerkt die Umstände der Zertifikatsausstellung in einer Protokolldatei, speichert das ausgestellte Zertifikat in ihrer Datenbank und liefert das ausgestellte Zertifkat an die Registrierungsstelle zurück.

4.3.2 Benachrichtigung des Teilnehmers

4.3.2.1 Allgemeine PKI der KfW

4.3.2.1.1 Manuelle Registrierung

Nach Ausstellung des Zertifikats wird der Zertifikatsinhaber in geeigneter Weise (z. B. über Mechanismen des Change-Prozesses und/oder per Email) informiert und das ausgestellte Zertifikat zugänglich gemacht.

4.3.2.1.2 Automatische Registrierung

Der Zertifikatsteilnehmer erhält das ausgestellte Zertifikat im Rahmen der programmatischen Kommunikation mit der Registrierungsstelle zugestellt.

4.3.2.2 Externe PKI der KfW

Nach Ausstellung des Zertifikats wird der Zertifikatsinhaber in Form eine Email informiert, in der das ausgestellte Zertifikat übermittelt wird.

4.3.2.3 Interne PKI der KfW

Die Benachrichtigung des Antragstellers im Rahmen der „Internen PKI“ liegt im Verantwortungsbereich des internen Betreibers der betreffenden Aussteller-CA.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme des Zertifikats

Die Annahme des Zertifikats erfolgt mit Bestätigung des Empfangs oder mit der Nutzung des Zertifikats durch den Zertifikatsinhaber.

4.4.2 Veröffentlichung des Zertifikats

Eine Veröffentlichung des Zertifikats findet zur Zeit nicht statt.

Im Rahmen dieser Certificate Policy ist nicht ausgeschlossen, eine Veröffentlichung von Zertifikaten in der Zukunft umzusetzen.

4.4.3 Benachrichtigung weiterer Instanzen

Eine Benachrichtigung weiterer Instanzen ist nicht vorgesehen, wird aber für zukünftige Erweiterungen im Rahmen dieser Certificate Policy auch nicht ausgeschlossen.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber

Die Nutzung des Zertifikats und des zugehörigen privaten Schlüssels darf nur entsprechend der Nutzungsbedingungen dieser Certificate Policy sowie der KfW-Richtlinien erfolgen.

Endteilnehmer und Mitarbeiter der Registrierungsstelle sind insbesondere verpflichtet,

- ihre privaten Schlüssel vor unbefugter Verwendung zu schützen
- den privaten Schlüssel nach Ablauf des Zertifikats nicht mehr zu benutzen (Ausnahme: Entschlüsselung verschlüsselter Daten)

Für Zertifikate von Systemen, juristischen Personen und Benutzergruppen gelten folgende Anforderungen:

- der Antragsteller ist für jegliches Kopieren oder Weitergeben des privaten Schlüssels verantwortlich. Der Umfang solcher Aktivitäten ist auf das unbedingt erforderliche Mindestmaß zu reduzieren.
- nach Wegfall der Voraussetzungen für den Besitz eines Zertifikats (z. B. Deaktivierung des Systems oder Beendigung eines Vertragsverhältnisses) ist das Zertifikat zu sperren.

Eine Sperrung des Zertifikats ist durchzuführen, wenn die Angaben im Zertifikat nicht mehr korrekt sind oder der private Schlüssel kompromittiert wurde.

Um dauerhaft sichere Kommunikationsbeziehungen aufbauen zu können, muss sich der Endteilnehmer vor Ablauf eines gültigen Zertifikats ein neues Zertifikat beschaffen.

Der Endteilnehmer ist für die Überwachung der Restgültigkeit seines Zertifikats grundsätzlich selbst verantwortlich.

4.5.2 Nutzung des öffentlichen Schlüssels und des Zertifikats durch vertrauende Dritte

Die Nutzung des Zertifikats und des öffentlichen Schlüsseln durch vertrauende Dritte erfolgt anhand der Vorgaben in RFC 5280.

Vertrauende Dritte dürfen von der KfW PKI ausgestellte Zertifikate nur für die im Zertifikat ausgewiesenen Verwendungszwecke einsetzen und haben die Gültigkeitsdauer der beteiligten Zertifikate, deren kryptographische Integrität sowie den Zertifikatsstatus zu prüfen und zu berücksichtigen.

Vertrauensbeziehungen zu KfW-Root-Zertifikaten unterliegen den Einschränkungen laut Kapitel 1.1.2.

4.6 Zertifikatserneuerung unter Beibehaltung des alten privaten Schlüssels (Certificate Renewal)

Eine Zertifikatserneuerung unter Beibehaltung des alten privaten Schlüssels ist nicht zulässig.

4.7 Zertifikatserneuerung mit Schlüsselwechsel (Rekeying)

4.7.1 Gründe für eine Zertifikatserneuerung

Eine Erneuerung eines gültigen Zertifikates ist in dem Erneuerungsintervall (innerhalb von 90 Tagen vor Ablauf des Zertifikats) möglich. Das alte Zertifikat bleibt in diesem Fall bis zum regulären Ablauf des Zertifikats weiterhin gültig.

Eine Zertifikatserneuerung kann unter den folgenden Bedingungen beantragt werden:

- die organisatorischen und fachlichen Bedingungen und Rechtfertigungen für den Besitz eines Zertifikats bestehen weiterhin. Dies ist organisatorisch oder technisch (im Fall einer automatisierten Erneuerung) nachzuweisen.
- die Antragsdaten (mit Ausnahme des Gültigkeitszeitraumes und des öffentlichen Schlüssels) sind ansonsten unverändert
- das bestehende Zertifikat ist gültig
- das bestehende Zertifikat ist noch weniger als 90 Tage gültig

4.7.2 Wer kann eine Zertifikatserneuerung beantragen

Eine Zertifikatserneuerung darf nur vom Zertifikatsinhaber bzw. dem Verantwortlichen für den Schlüssel beantragt werden.

4.7.3 Bearbeitung von Zertifikatserneuerungen

Das Erneuerungsverfahren MUSS gewährleisten, dass nur der Zertifikatsinhaber die Erneuerung durchführen kann.

Bei einer manuellen Zertifikatserneuerung ist der Prozess identisch zur ersten Beantragung eines Zertifikats.

Sofern die betreffende Aussteller-CA der KfW einen Dienst für die automatische Erneuerung von Zertifikaten anbietet, ist die automatische Erneuerung jederzeit innerhalb des Erneuerungsintervalls (siehe Kapitel 4.7.1) möglich.

Das Folgezertifikat wird (ggf. automatisch) zeitnah ausgestellt, sofern folgende Bedingungen erfüllt sind:

- das beantragte Folgezertifikat hat einen identischen Subject sowie identische Subject Alternative Names
- das bestehende Zertifikat ist gültig (nicht gesperrt)

- der automatisch übermittelte Zertifikatsantrag für das Folgezertifikat ist (im Rahmen des Übertragungsprotokolls für die Erneuerung) kryptographisch mit dem privaten Schlüssel des bestehenden Zertifikats signiert bzw. authentisiert (Beweis des Besitzes des alten Schlüssels).

Andere Verfahren zur Autorisierung einer Erneuerung können unterstützt werden, sofern sie ein äquivalentes Sicherheitsniveau bieten.

4.7.4 Benachrichtigung des Antragstellers nach Zertifikatserneuerung

Siehe Kapitel 4.3.2

4.7.5 Annahme einer Zertifikatserneuerung

Siehe Kapitel 4.4.1

4.7.6 Veröffentlichung der erneuerten Zertifikate durch die Zertifizierungsstelle

Siehe Kapitel 4.4.2

4.7.7 Benachrichtigung weiterer Instanzen über eine Zertifikatserneuerung durch die Zertifizierungsstellung

Siehe Kapitel 4.4.3

4.8 Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

4.8.1 Gründe für eine Zertifikatserneuerung

Eine Zertifikatserneuerung mit Datenanpassung kann unter den folgenden Bedingungen beantragt werden:

- die organisatorischen und fachlichen Bedingungen und Rechtfertigungen für den Besitz eines Zertifikats bestehen weiterhin. Dies ist organisatorisch oder technisch (im Fall einer automatisierten Erneuerung) nachzuweisen.
- das bestehende Zertifikat ist gültig

4.8.2 Wer kann eine Zertifikatserneuerung beantragen

Siehe Kapitel 4.7.2

4.8.3 Bearbeitung von Zertifikatserneuerungen

Das Erneuerungsverfahren muss gewährleisten, dass nur der Zertifikatsinhaber die Erneuerung durchführen kann.

Bei einer manuellen Zertifikatserneuerung ist der Prozess identisch zur ersten Beantragung eines Zertifikats.

Eine automatisierte Zertifikatserneuerung mit Datenanpassung ist nicht möglich.

4.8.4 Benachrichtigung des Antragstellers nach Zertifikatserneuerung

Siehe Kapitel 4.3.2

4.8.5 Annahme einer Zertifikatserneuerung

Siehe Kapitel 4.4.1

4.8.6 Veröffentlichung der erneuerten Zertifikate durch die Zertifizierungsstelle

Siehe Kapitel 4.4.2

4.8.7 Benachrichtigung weiterer Instanzen über eine Zertifikatserneuerung durch die Zertifizierungsstellung

Siehe Kapitel 4.4.3

4.9 Sperrung und Suspendierung von Zertifikaten

Die folgenden Regelungen beziehen sich auf die „Allgemeine KfW PKI“ und die „Externe KfW PKI“.

Zertifikate der „Internen KfW PKI“ werden von Aussteller-CAs ausgestellt, die von den zuständigen Stellen innerhalb der KfW, jedoch außerhalb der PKI-Gruppe betrieben werden. Für Aussteller-CAs der „Internen KfW PKI“ gelten ausschließlich die Regeln zur Sperrung und Suspendierung von Zertifikaten, welche die zuständige Fachgruppe für die von ihr betriebene Aussteller-CA definiert.

4.9.1 Gründe für eine Zertifikatssperrung

Eine Sperrung MUSS unter folgenden Umständen durchgeführt werden:

Die Angaben im Zertifikat (mit Ausnahme nicht verifizierter Endteilnehmer-Informationen) sind nicht mehr aktuell, ungültig oder falsch oder entsprechen nicht den Bestimmungen der Namensgebung.

Der private Schlüssel wurde kompromittiert, verloren, gestohlen oder offengelegt (dies gilt nicht im Zusammenhang mit einer Schlüsselsicherung) oder es besteht ein dringender Verdacht, dass dies geschehen ist.

Der Zertifikatsnehmer benötigt das Zertifikat nicht mehr bzw. der Zertifikatnehmer verlangt ausdrücklich die Sperrung des Zertifikats.

Der Zertifikatsnehmer ist nicht mehr berechtigt, das Zertifikat zu nutzen.

Der Zertifikatsinhaber (natürliche Person) verlässt das Unternehmen und benötigt daher kein Zertifikat mehr.

Der Zertifikatsinhaber (System, Dienst) wird deaktiviert bzw. abgebaut.

Es liegt ein Missbrauch, Missbrauchsverdacht durch zu der Nutzung des Schlüssels berechtigten Personen vor.

Es liegt eine unbefugte Nutzung oder der Verdacht einer unbefugten Nutzung des Schlüssels von nicht berechtigten Personen vor.

Der Zertifikatsnehmer hält Verpflichtungen gemäß dieses CP bzw. des CPS nicht ein.

Interne Vorgaben oder Richtlinien begründen eine Zertifikatssperrung.

Die KfW PKI stellt ihren Zertifizierungsbetrieb ein. In diesem Fall werden sämtliche von der betreffenden KfW-PKI ausgestellten Zertifikate gesperrt.

Der private Schlüssel der ausstellenden oder einer übergeordneten Root-CA wird kompromittiert. In diesem Fall werden sämtliche von diesen CAs ausgestellte Zertifikate gesperrt.

Die Algorithmen, die Schlüssellänge oder die Gültigkeitsdauer des Zertifikates bieten keine ausreichende Sicherheit mehr. Die KfW-PKI behält sich in diesem Fall vor, die betreffenden Zertifikate zu sperren.

4.9.2 Wer kann eine Zertifikatssperrung beantragen

Eine Sperrung von Zertifikaten für Systeme können von einem Mitglied der Verwalter-Gruppe des Systems oder ihren Vorgesetzten beantragt werden. Die Beauftragung zur Zertifikatssperrung kann von diesen Personen auch an einen Beauftragten delegiert werden.

Die Sperrung eines Benutzer-Zertifikates kann vom Zertifikatsnehmer, einem vom Zertifikatsnehmer Beauftragten oder von Vorgesetzten des Zertifikatsnehmers beauftragt werden.

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

Der Benutzer eines Personenzertifikats kann die Sperrung seines eigenen Zertifikates jederzeit beantragen, auch wenn keiner der in Ziffer 4.9.1 genannten Gründe vorliegt.

Autorisierte Mitarbeiter der KfW PKI können die Sperrung von Zertifikaten beauftragen.

4.9.3 Ablauf einer Zertifikatssperrung

Die Sperrung des Zertifikats erfolgt auf Basis eines genehmigten Sperrungs-Antrags im Change-System der KfW.

Mitarbeiter der KfW-PKI führen die Sperrung des Zertifikats in der entsprechenden PKI durch und veranlassen ggf. eine Publizierung der aktualisierten Sperrliste.

Der Zertifikatsnehmer oder die verantwortliche Systemverwaltergruppe wird über die Sperrung informatiert.

4.9.4 Fristen für den Antragsteller

Zertifikatsnehmer sind verpflichtet, bei Bekanntwerden eines Sperrgrundes (siehe Kapitel 4.9.1) unverzüglich die Sperrung des Zertifikats zu veranlassen.

4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle

Die Sperrung des Zertifikats wird bei Kompromittierung des Schlüssels oder vergleichbaren sicherheitsrelevanten Vorgängen unverzüglich nach Zugang des Sperrantrags durchgeführt.

In weniger kritischen Fällen (z. B. bei Neuausstellung des Zertifikats aufgrund falscher Zertifikatsinformation) erfolgt eine Bearbeitung in der Regel innerhalb einer Woche.

4.9.6 Überprüfungsvorgaben für vertrauende Dritte

Sperrinformationen werden über Sperrlisten an den publizierten Endpunkten veröffentlicht. Vertrauende Dritte (Relying Parties) sollten zur Prüfung der Zertifikatsgültigkeit jeweils die aktuell veröffentlichte Sperrliste verwenden.

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Sperrlisten der Root CAs werden in der Regel in einem Abstand von 6 Monaten erzeugt.

Die außerplanmäßige Erstellung einer Sperrliste ist jederzeit möglich.

Sperrlisten der Aussteller-CAs werden täglich automatisiert erzeugt. Sperrlisten können weiterhin jederzeit außerplanmäßig manuell erzeugt werden, z. B. um Zertifikatssperrungen beschleunigt zu veröffentlichen.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die Veröffentlichung von Sperrlisten der Root CAs erfolgt im Regelfall innerhalb von 10 Arbeitstagen nach Ausstellung, sofern keine Zertifikate gesperrt wurden.

Bei einer Sperrung einer oder mehrerer Aussteller-CAs erfolgt die Veröffentlichung der Sperrliste schnellstmöglich.

Die Veröffentlichung der von den Aussteller-CAs erzeugten Sperrlisten erfolgt schnellstmöglich nach Erstellung durch einen automatisierten Prozess.

4.9.9 Online-Verfügbarkeit von Sperr- und Statusinformationen

Zur Zeit wird die Online-Veröffentlichung von Sperrinformationen (z. B. via OCSP) nicht unterstützt.

Vertrauende Dritte SOLLEN die veröffentlichten Sperrlisten verwenden, um den Zertifikatsstatus der ausgegebenen Zertifikate zu prüfen.

4.9.10 Anforderungen an Online Sperr- und Statusüberprüfungsverfahren

Zur Zeit wird die Online-Veröffentlichung von Sperrinformationen (z. B. via OCSP) nicht unterstützt.

4.9.11 Andere Formen der Veröffentlichung von Sperrinformationen

Nach Sperrung eines Zertifikats wird der Zertifikatsinhaber über geeignete Kommunikationssysteme (z. B. per Email oder ein Ticket-System) über die Sperrung informatiert.

Andere Formen der Veröffentlichung von Sperrinformationen werden nicht unterstützt.

4.9.12 Kompromittierung von privaten Schlüsseln

Bei einer Kompromittierung eines privaten Schlüssels ist das entsprechende Zertifikat unverzüglich zu sperren (siehe Kapitel 4.9.1)

4.9.13 Umstände einer Suspendierung

Suspendierung von Zertifikaten wird nicht unterstützt.

4.9.14 Wer kann eine Zertifikatssuspendierung beantragen

Suspendierung von Zertifikaten wird nicht unterstützt.

4.9.15 Ablauf einer Zertifikatssuspendierung

Suspendierung von Zertifikaten wird nicht unterstützt.

4.9.16 Dauer einer Zertifikatssuspendierung

Suspendierung von Zertifikaten wird nicht unterstützt.

4.10 Online-Dienste zur Ermittlung des Zertifikatsstatus

Zur Zeit wird die Online-Veröffentlichung von Sperrinformationen (z. B. via OCSP) nicht unterstützt.

4.11 Beendigung der Zertifikatsnutzung durch den Zertifikatsinhaber

Die Beendigung der Zertifikatsnutzung durch den Zertifikatsinhaber erfolgt durch

- Sperrung des Zertifikats
- Unterlassen der Neubeantragung eines Zertifikats bei Ablauf des Zertifikats

4.12 Schlüsselhinterlegung und –wiederherstellung

Die Schlüssel der Zertifizierungsstellen werden mit den Mechanismen der verwendeten HSMs gesichert und können z. B. bei Ausfall von Hardware-Komponenten entsprechend wiederhergestellt werden.

Schlüssel von Endnutzern werden zur Zeit nicht hinterlegt.

5 Nicht-technische Sicherheitsmaßnahmen

Siehe CPS, Kapitel 5

6 Technische Sicherheitsmaßnahmen

Siehe CPS, Kapitel 6

7 Zertifikats-, Sperrlisten und OCSP-Profile

Siehe CPS, Kapitel 7

8 Konformitätsprüfung und Auditierung

8.1 Intervall und Gründe von Prüfungen

Die Prozesse der Zertifizierungsstelle sowie der an der Registrierung beteiligten Stellen werden regelmäßig bzw. anlassbezogen überprüft.

Audits des technischen Aufbaus der PKI und der operativen Abläufe werden in regelmäßigen Abständen durchgeführt.

8.2 Identität und Qualifikation von Prüfern

Prüfungen können durch interne oder externe Prüfer durchgeführt werden. Prüfer müssen über die nötigen technischen und organisatorischen Kenntnisse auf den Gebieten der Public Key Infrastructure sowie IT Security verfügen.

8.3 Beziehung des Prüfers zur geprüften Stelle, Unabhängigkeit des Prüfers

Prüfer dürfen nicht in die operativen Prozesse der KfW PKIs eingebunden sein.

Eine Selbstüberprüfung ist unzulässig.

8.4 Abgedeckte Bereiche der Prüfung

Es können alle organisatorischen und technischen Aspekte der KfW PKIs geprüft werden.

Bei einem durch die KfW PKI selbst veranlassten Audit wird eine Selektion oder Fokussierung auf bestimmte zu untersuchender Aspekte sowie die Art der Durchführung durch den Auftraggeber selbst festgelegt.

8.5 Maßnahmen zur Mängelbeseitigung

Festgestellte Mängel müssen in Abstimmung zwischen der Zertifizierungsstelle, den Prüfern und dem Auftraggeber der Prüfung zeitnah beseitigt werden.

8.6 Mitteilung der Ergebnisse

Eine Veröffentlichung der Prüfungsergebnisse findet nicht statt.

9 Weitere geschäftliche und rechtliche Regelungen

9.1 Entgelte

Nicht zutreffend

9.2 Finanzielle Verantwortlichkeiten

Finanzielle Verantwortung wird im Kontext der KfW PKIs nicht übernommen. Insbesondere besteht kein Versicherungsschutz.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Umfang von vertraulichen Informationen

Informationen und Daten über Zertifikatsinhaber und Teilnehmer der KfW PKIs werden als vertrauliche Information eingestuft, sofern sie nicht öffentliche Informationen nach Kapitel 9.3.2 sind.

9.3.2 Umfang von nicht vertraulichen Informationen

Nicht vertrauliche Informationen sind sämtliche Informationen, die in ausgegebenen Zertifikaten und Sperrlisten explizit (z. B. Namen) oder implizit (z. B. Signatur- oder Schlüsselalgorithmen) enthalten sind oder abgeleitet werden können.

Nicht vertrauliche Informationen sind weiterhin alle Dokumente der KfW PKI, die als öffentlich gekennzeichnet und/oder aktiv durch die KfW PKIs veröffentlicht werden.

Diese Certificate Policy ist eine öffentlich zugängliche Information.

9.3.3 Verantwortung zum Schutz von vertraulichen Informationen

Die KfW PKI trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen.

9.4 Schutz von personenbezogenen Daten (Datenschutz)

9.4.1 Datenschutzkonzept

Die Speicherung und Verarbeitung personenbezogener Daten erfolgt unter Berücksichtigung der KfW-internen Richtlinien sowie der gesetzlichen Regelungen aus der Datenschutzgrundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG).

9.4.2 Vertraulich zu behandelnde Daten

Für vertrauliche personenbezogene Daten -gemäß der Definition aus Artikel 4 I DSGVO- gelten die Regelungen entsprechend Kapitel 9.3.1.

9.4.3 Nicht-vertraulich zu behandelnde Daten

Für nicht vertrauliche personenbezogene Daten gelten die Regelungen entsprechend Kapitel 9.3.2.

9.4.4 Verantwortung zum Schutz personenbezogener Daten

Für personenbezogene Daten gelten die Regelungen entsprechend Kapitel 9.3.3. Alle Mitarbeiter des der KfW PKI sind auf die Einhaltung des Datenschutzes verpflichtet worden.

9.4.5 Mitteilung und Zustimmung zur Nutzung vertraulicher Daten

Der Zertifikatsnehmer wird spätestens bei Beantragung des Zertifikats über die Verarbeitung seiner personenbezogenen Daten informiert.

Sofern keine andere Rechtsgrundlage herangezogen wird, basiert die Verarbeitung auf einer Einwilligung des Betroffenen, welcher er mit Antragstellung der KfW gegenüber abgibt.

Personenbezogene Daten, welche zur erfüllen des Zwecks nicht mehr notwendig sind, werden unverzüglich (im Rahmen der gesetzliche Aufbewahrungspflichten) gelöscht.

Informationen, die nicht als vertraulich behandelt werden, können veröffentlicht werden.

9.4.6 Offenlegung bei gerichtlicher Anordnung oder im Rahmen einer gerichtlichen Beweisführung

Die KfW PKI hält die gesetzlichen Datenschutzbestimmungen bei der Verarbeitung von personenbezogenen Daten ein. Eine Offenlegung erfolgt bei Vorlage entsprechender richterlicher Anordnungen sowie auf Basis geltender Gesetze.

9.4.7 Andere Umstände einer Offenlegung

Nicht zutreffend

9.5 Urheberrechte

Die KfW ist Urheber dieser Certificate Policy. Dieses Dokument darf unverändert an Dritte weitergegeben werden.

9.6 Zusicherungen und Gewährleistungen

Grundsätzlich wird keine Gewährleistung übernommen. Die KfW garantiert nicht die Verfügbarkeit der Leistungen der KfW PKI.

9.7 Haftungserklärung

Nicht zutreffend

9.8 Haftungsbeschränkung

Verletzt die KfW bei der Vertragsdurchführung schuldhaft eine vertragswesentliche Pflicht, die hierfür im Einzelfall von besonderer Bedeutung ist, so haftet sie für den dadurch entstehenden Schaden. Bei einfacher Fahrlässigkeit ist die Haftung der KfW auf den vertragstypischen Schaden beschränkt.

Für die Verletzung sonstiger Pflichten haftet die KfW nur bei grobem Verschulden. Gegenüber Kaufleuten und öffentlichen Verwaltungen gilt die Haftungsbeschränkung des Absatz 1 Satz 2 auch bei grober Fahrlässigkeit einfacher Erfüllungsgehilfen.

Vorstehende Haftungsausschlüsse und –begrenzungen finden keine Anwendung auf die Haftung für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit; insofern haftet die KfW nach den gesetzlichen Bestimmungen.

9.9 Haftungsfreistellung

Bei der unsachgemäßen Verwendung des Zertifikats und dem zugehörigen privaten Schlüssel oder einer Verwendung des Schlüsselmaterials beruhend auf fälschlichen oder fehlerhaften Angaben bei der Beantragung ist die KfW von der Haftung freigestellt.

9.10 Laufzeit und Beendigung

Diese Certificate Policy tritt mit Veröffentlichung (siehe Kapitel 2) in Kraft.

Diese Certificate Policy ist solange gültig, bis eine neuere Version veröffentlicht wird oder die KfW PKI ihren Betrieb einstellt.

9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Nicht zutreffend

9.12 Änderungen

Änderungen dieser Certificate Policy werden rechtzeitig von ihrem Inkrafttreten veröffentlicht.

Die Richtlinienbezeichnung (OID) dieses Dokumentes wird bei Änderungen beibehalten.

9.13 Bestimmung zur Beilegung von Streitigkeiten

Nicht zutreffend

9.14 Geltendes Recht

Der Betrieb der KfW PKI unterliegt den Gesetzen der Bundesrepublik Deutschland. Der Gerichtsstand ist Frankfurt am Main, Bundesrepublik Deutschland.

9.15 Einhaltung geltenden Rechts

Die von der KfW PKI ausgestellten Zertifikate sind qualifizierten Zertifikaten im Sinne der Verordnung (EU) Nr. 910/2014. Sofern mit der von der KfW PKI ausgestellten Zertifikate elektronische Signaturen abgegeben werden, übernimmt die KfW keine Gewähr dafür, dass es sich dabei um fortgeschrittene elektronische Signaturen im Sinne der Verordnung (EU) Nr. 910/2014 handelt.

9.16 Verschiedene Bestimmungen

Sollte eine Bestimmung dieser Certificate Policy unwirksam oder undurchführbar sein, so berührt dies die Wirksamkeit der restlichen Certificate Policy nicht. Statt der unwirksamen Bestimmung gilt eine solche Bestimmung vereinbart, die dem Zweck dieses Dokumentes in rechtswirksamer Weise am nächsten kommt.

9.17 Sonstige Bestimmungen

Nicht zutreffend