Bundesministerium der Verteidigung
CIT II 2

BUNDESWEHR

Zertifizierungsrichtlinie der Bundeswehr für Zertifizierungsstellen in der PKI-1-Verwaltung des BSI

Die Kennung (OID) dieser Zertifizierungsrichtlinie lautet:

0.4.0.127.0.7.3.6.1.1.9.3 (Zertifikate ohne Zulassung für VS-NfD)

0.4.0.127.0.7.3.6.1.1.9.4 (Zertifikate mit Zulassung für VS-NfD)

1.3.6.1.4.1.14275.1.1.1.1.1.1 (Bw-Interne Verwendung)

Gender-Hinweis

Um die Lesbarkeit und das textliche Verständnis im folgenden Dokument zu gewährleisten, wird keine gendergerechte Sprache verwendet. Folgendes Dokument ist ausschließlich in männlicher Form geschrieben, spricht jedoch alle Geschlechter an. Die verkürzte Sprachform hat ausschließlich redaktionelle Gründe und beinhaltet keinerlei Wertung.

Dokumenteninformation

Dokumentenversion

Version	Datum	Bearbeiter	Bemerkungen/Änderungsvermerk zur vorherigen Version
1.0	29.08.2024	BMVg CIT II 2	Initiale Billigung und Herausgabe

Bearbeitungsstand: Genehmigt PMABw (BMVg CIT II 2)

Inhaltsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Überblick

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) stellt mit der „PKI-1-Verwaltung“ (V-PKI) eine Public-Key-Infrastructure-Struktur für den Bereich der Verwaltung zur Verfügung.

Die Bundeswehr kann im Rahmen der Public Key Infrastructure (PKI) der Bundeswehr (PKIBw) in dieser Struktur eigene nachgeordnete Zertifizierungsstellen (Certificate Authorities, CA) zur Deckung des eigenen Zertifikatsbedarfs betreiben.

Diese CA werden in diesem Dokument als „die CA“ bezeichnet.

Dieses Dokument ist die Zertifizierungsrichtlinie (Certificate Policy, CP) der Bundeswehr für Zertifizierungsstellen in der „PKI-1-Verwaltung“ des BSI, herausgegeben durch die PKI Management Authority der Bundeswehr (PMABw) im Bundesministerium der Verteidigung (BMVg). Sie ergänzt die Vorgaben der „Certificate Policy Root-CA der PKI-1-Verwaltung“[1], welche durch das BSI herausgegeben wird.

Die Umsetzungsbeschreibungen zu den in den CP vorgenommenen Vorgaben erfolgen in den Regelungen für den Zertifizierungsbetrieb (Certification Practice Statement (CPS)) der CA.

Die Gliederung dieses Dokuments, die Verwendung und Konvention von Begriffen orientiert sich an den Vorgaben der „Certificate Policy Root-CA der PKI-1-Verwaltung“ des BSI.

Konventionen

In dieser CP werden die Begriffe „muss“, „soll“, „kann“ äquivalent zu der Definition in der „Certificate Policy Root-CA der PKI-1-Verwaltung“ verwendet:

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

Sofern das BSI im gleichnamigen Abschnitt der „Certificate Policy Root-CA der PKI-1-Verwaltung“ keine Vorgaben für die CA macht und in dieser CP keine Ergänzungen vorgenommen werden, wird dies in dem entsprechenden Abschnitt dieser CP über die Formulierung „Keine weiteren Vorgaben.“ kenntlich gemacht.

Erfolgt eine Regelung in dem gleichnamigen Abschnitt der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und wird diese nicht weiter ergänzt, wird dies über den Satz „Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen“ verdeutlicht.

[1] Die „Certificate Policy Root-CA der PKI-1-Verwaltung“ ist auf der Webseite des BSI zur PKI-1-Verwaltung („V-PKI“) abrufbar.
Zum Zeitpunkt der Erstellung des vorliegenden Dokuments war der Abruf unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/VerwaltungsPKI/Certificate_Policy_2024.pdf möglich

1.2 Dokumentenname und Identifikation

Titel: Zertifizierungsrichtlinie der Bundeswehr für Zertifizierungsstellen in der PKI-1-Verwaltung des BSI

Version: 1.0

Das vorliegende Dokument trägt die folgenden Objektkennungen (Object Identifier (OID)):

0.4.0.127.0.7.3.6.1.1.9.3 (Zertifikate ohne Zulassung für VS-NfD)

0.4.0.127.0.7.3.6.1.1.9.4 (Zertifikate mit Zulassung für VS-NfD)

1.3.6.1.4.1.14275.1.1.1.1.1.1 (Bw-Interne Verwendung)

1.3 Teilnehmer der Zertifikatsinfrastruktur (PKI)

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

1.3.1 Zertifizierungsstellen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

1.3.2 Registrierungsstellen

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Die CA muss eine zentrale Registrierungsstelle (Central Registration Authority (CRA)) einrichten.

Für CA, die Teilnehmerzertifikate ausstellt, sollten lokale Registrierungsstellen (Local Registration Authorities (LRA)) bedarfsgerecht eingerichtet werden.

Die CRA ist Bestandteil der CA und muss der Leitung des CA-Betreibers unterstellt sein.

Die LRA müssen fachlich der CRA unterstellt sein.

Die CRA muss mindestens die folgenden übergeordneten organisatorischen Aufgaben übernehmen:

- Bereitstellung Sperrhotline
- Bearbeitung von Anträgen zum Aufbau einer LRA
- Überprüfung auf Einhaltung der Vorgaben durch die LRA
- Organisation von Schulungen für Mitarbeiter der LRA
- Verwaltung der Zugriffsrechte für das verwendete RA-System (RASys)

Eine LRA muss, vor Übergabe eines Hardware-Schlüsselträgers, die zweifelsfreie Identifizierung der Teilnehmer durchführen.

Die CA muss die LRA sowie die Aufgaben der CRA und der LRA in ihrem CPS benennen.

1.3.3 Zertifikatsinhaber (Subscriber)

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Zertifikatsinhaber werden für die CA in der Bundeswehr als Zertifikatsnehmer bezeichnet.

1.3.4 Zertifikatsnutzer (Relying Parties)

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen. Siehe auch erster Absatz Abschnitt 1.3 der „Certificate Policy Root-CA der PKI-1-Verwaltung“.

1.3.5 Weitere Teilnehmer

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Die CA muss alle weiteren am Zertifizierungsprozess beteiligten Teilnehmer im CPS in diesem Abschnitt benennen.

1.3.5.1 Policy Management Authority (PMA)

Eine PMA ist verantwortlich für:

- Die Herausgabe der CP
- Die Aufsicht über alle ihr unterstellten CA
- Die Prüfung und Billigung des CPS und aller verbundenen Dokumente für die CA
- Genehmigen des Betriebs einer CA
- Das Anordnen von Audits, Prüfung und Bewertung der Audit-Ergebnisse, Ableiten und Anordnen von Maßnahmen als Reaktion auf gefundene Mängel
- Das Genehmigen von Abweichungen von den Regelungen einer CP oder eines CPS
- Prüfen und Genehmigen von Vertrauensstellungen mit externen CA

Die Funktion der PMA der Bundeswehr wird durch die PMABw im BMVg CIT II 2 wahrgenommen.

Sie stimmt sich hierbei mit dem BSI ab und holt ggf. notwendige Kommentierungen, Billigungen und Freigaben bei dieser ein.

1.4 Anwendungsbereich

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

1.4.1 Geeignete Zertifikatsnutzung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

1.4.2 Untersagte Zertifikatsnutzung

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Funktionszertifikate für Rollen und Funktionen (wie „Offizier der Führungsbereitschaft“) dürfen nicht zur einfachen und fortgeschrittenen elektronischen Signatur nach eIDAS verwenden werden.

1.5 Verwaltung der Policy

1.5.1 Änderungsmanagement

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Änderungen dieser CP werden nur im Auftrag der PMABw vorgenommen und mit der Leitung des CA-Betreibers abgestimmt. Endgültige Entscheidung zum Inhalt bleiben der PMABw vorbehalten.

Neue Versionen der CP müssen durch die CA auf der Web-Seite der PKIBw öffentlich zugänglich veröffentlicht werden. Betroffene CA werden im Voraus durch die PMABw unterrichtet.

Vor Genehmigung und Herausgabe geänderter Versionen dieser CP wird das BSI von der PMABw informiert.

1.5.2 Kontaktdaten

Ansprechstelle für dieses Dokument:

PKI Management Authority der Bundeswehr (PMABw)
Bundesministerium der Verteidigung (BMVg)
Cyber/Informationstechnik - Fähigkeiten Cyber/IT – Informationssicherheit (CIT II 2)

Hardthöhe
Fontainegraben 150
53123 Bonn

E-Mail: BMVgCITII2@bmvg.bund.de

Die CA muss die Ansprechstelle der Zertifizierungsstellen im CPS in diesem Abschnitt benennen.

1.5.3 Eignungsprüfer für Regelungen für den Zertifizierungsbetrieb (CPS)

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

1.5.4 Verfahren zur Anerkennung von Regelungen für den CPS

Das CPS muss zur Billigung bei der für die CA zuständigen PMA vorgelegt werden. Diese legt das CPS gemäß den Anforderungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“ bei der Root-CA im BSI vor.

1.6 Definitionen und Akronyme/Abkürzungen

Die Liste der Definitionen und Abkürzungen in Tabelle 1~~Tabelle 1~~ ergänzt die entsprechende Liste in der „Certificate Policy Root-CA der PKI-1-Verwaltung“.

An den Stellen, an denen bei der Definition ein Widerspruch zu den Definitionen in der „Certificate Policy Root-CA der PKI-1-Verwaltung“ auftritt, gilt für diese CA und deren CPS die Definition aus dem vorliegenden Dokument.

Archivierung	Aufbewahrung von Daten duch den CA-Betreiber oder der Registrierungsstellen über einen längeren Zeitraum. Es handelt sich hierbei nicht um eine Archivierung im Sinn der Bereitstellung von Daten als Angebot zur Archivierung an das Bundesarchiv.
BMVg	Bundesministerium der Verteidigung
CA-Betreiber	Organisationseinheit, welche die CA fachlich und technisch betreibt. Die Teilaufgaben können dabei durch verschiedene Organisations-einheiten wahrgenommen werden.
CRA	Central Registration Authority, Zentrale Registrierungsstelle Registrierungsstelle, die direkt bei der CA betrieben wird, welche die fachliche Aufsicht

	über die LRA führt und besondere sowie zentrale Aufgaben übernimmt. Geregelt in Kapitel 1.3.2.
InfoSichhVork	Informationssicherheitsvorkommnis
PKIBw	Public Key Infrastructure der Bundeswehr
PMA	Policy Management Authority Geregelt in Kapitel 1.3.5.1.
PMABw	PKI Management Authority der Bundeswehr (im BMVg CIT II 2)
RA	Registration Authority, Registrierungsstelle
RASys	RA-System Hardware und Software für die Geschäftsprozesse einer RA.
RSA	Rivest-Shamir-Adleman-Algorithmus
Zertifikatsinhaber	Natürliche und juristische Personen, Personengruppen und Funktionen oder IT-Prozesse, welche im Rahmen der V-PKI Schlüssel und Zertifikate erhalten.
Zertifikatsnehmer	Begriff für den Zertifikatsinhaber für CA in der Bundeswehr.

Tabelle 1: Definitionen und Akronyme/Abkürzungen

2 Verantwortlichkeiten für Veröffentlichungen und Verzeichnisdienste

2.1 Verzeichnisdienste

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Der CA-Betreiber muss die verantwortlichen Betreiber der Verzeichnisdienste und Ablagepunkte im CPS benennen.

2.2 Veröffentlichung von Zertifizierungs-Informationen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

2.3 Aktualisierung der Information (Zeitpunkt, Frequenz)

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

2.4 Zugangskontrolle zu Verzeichnisdiensten

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

3 Identifizierung und Authentifizierung (I&A)

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

3.1 Namen

3.1.1 Namensformen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

3.1.2 Aussagekraft von Namen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsinhaber

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Die ausgestellten Teilnehmerzertifikate der CA müssen verpflichtend mindestens folgende Attribute enthalten:

OU = bmvg

O = bund

3.1.5 Eindeutigkeit von Namen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

3.1.6 Anerkennung, Authentifizierung und Funktion geschützter Namen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

3.2 Initiale Identitätsüberprüfung bei einer Zertifikatsanfrage

3.2.1 Nachweis des Besitzes des privaten Schlüssels

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

3.2.2 Authentifizierung einer Organisation

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

3.2.3 Authentifizierung natürlicher Personen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

3.2.4 Nicht überprüfte Teilnehmerangaben

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Alle Informationen müssen vor Aufnahme in ein Zertifikat durch die CA, die CRA oder eine LRA überprüft werden.

Die CA müssen im CPS alle Informationen angeben, welche in den Zertifikaten enthalten sein können.

3.2.5 Überprüfung der Berechtigung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

3.2.6 Kriterien für Zusammenarbeit

Keine weiteren Vorgaben.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung mit neuem Schlüssel

3.3.1 Routinemäßige Zertifikatserneuerung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

3.3.2 Zertifikatserneuerung nach einer Sperrung

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Bei einer Zertifikatserneuerung nach einer Sperrung muss die Identifizierung wie bei einer erstmaligen Antragsstellung durchgeführt werden (siehe Kapitel 3.2).

3.4 Identifizierung und Authentifizierung von Sperranfragen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4 Ablauforganisation

4.1 Zertifikatsanfrage

4.1.1 Wer kann eine Zertifikatsanfrage stellen

Keine über die CP „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.1.2 Registrierungsprozess

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.2 Bearbeiten von Zertifikatsanfragen

4.2.1 Durchführung von Identifikation und Authentifizierung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.2.2 Annahme oder Ablehnung von Zertifikatsanfragen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.2.3 Bearbeitungsdauer bei Zertifikatsanfragen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.3 Zertifikatsausgabe

4.3.1 Aktionen durch die CA während der Zertifikatsausstellung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.3.2 Benachrichtigung des Teilnehmers

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme des Zertifikats

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Zertifikatsnehmer müssen die Annahme des Zertifikates der CA bestätigen. Ist die Prüfung nicht erfolgreich oder bleibt die Bestätigung aus, so muss die CA das Zertifikat nach Rückfrage sperren.

Die CA muss die Verfahren wie diese Bestätigung erfolgt im CPS in diesem Abschnitt beschreiben.

4.4.2 Veröffentlichung des Zertifikats durch die CAs

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.4.3 Benachrichtigung der Teilnehmer durch die (Root-)CA

Keine weiteren Vorgaben.

4.5 Verwendung des Schlüsselpaares

4.5.1 Nutzung durch den Zertifikatsinhaber

Für den Zertifikatsnehmer des Zertifikates der CA der Bundeswehr innerhalb der V-PKI gelten keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

Zertifikatsnehmer von ausgestellten Teilnehmerzertifikaten der CA der Bundeswehr innerhalb der V-PKI müssen bei der Nutzung ihres privaten Schlüssels die Anforderungen der von ihnen unterzeichneten Selbsterklärung erfüllen und dürfen diese nur für Zwecke gemäß Kapitel 1.4 verwenden.

4.5.2 Nutzung des Zertifikats durch Zertifikatsnutzer

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.6 Zertifikatserneuerung unter Verwendung des alten Schlüssels (Re-Zertifizierung)

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Die Re-Zertifizierung von Schlüsseln der Nutzer darf nicht erfolgen. Ausnahmen können in Rücksprache mit der BSI genehmigt werden. Die Genehmigung ist über die PMABw in Textform einzuholen.

4.6.1 Gründe für eine Zertifikatserneuerung

Keine weiteren Vorgaben.

4.6.2 Wer kann eine Zertifikatserneuerung anfragen

Keine weiteren Vorgaben.

4.6.3 Ablauf der Zertifikatserneuerung

Keine weiteren Vorgaben.

4.6.4 Benachrichtigung des Zertifikatsinhabers nach Zertifikatserneuerung

Keine weiteren Vorgaben.

4.6.5 Annahme einer Zertifikatserneuerung

Keine weiteren Vorgaben.

4.6.6 Veröffentlichung einer Zertifikatserneuerung durch die CA

Keine weiteren Vorgaben.

4.6.7 Benachrichtigung der Teilnehmer durch die CA

Keine weiteren Vorgaben.

4.7 Schlüssel- und Zertifikatserneuerung (Re-Key)

4.7.1 Gründe für eine Schlüssel- und Zertifikatserneuerung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.7.2 Wer kann eine Schlüssel- und Zertifikatserneuerung anfragen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.7.3 Ablauf der Schlüssel- und Zertifikatserneuerung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.7.4 Benachrichtigung des Zertifikatsnehmers

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.7.5 Annahme der Schlüssel- und Zertifikatserneuerung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.7.6 Veröffentlichung einer Zertifikatserneuerung durch die CA

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.7.7 Benachrichtigung der Teilnehmer durch die CA

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.8 Zertifikatsmodifizierung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.8.1 Gründe für eine Zertifikatsmodifizierung

Keine weiteren Vorgaben.

4.8.2 Wer kann eine Zertifikatsmodifizierung anfragen

Keine weiteren Vorgaben.

4.8.3 Ablauf der Zertifikatsmodifizierung

Keine weiteren Vorgaben.

4.8.4 Benachrichtigung des Zertifikatsinhabers

Keine weiteren Vorgaben.

4.8.5 Annahme der Zertifikatsmodifizierung

Keine weiteren Vorgaben.

4.8.6 Veröffentlichung einer Zertifikatsmodifizierung durch die CA

Keine weiteren Vorgaben.

4.8.7 Benachrichtigung der Teilnehmer durch die CA

Keine weiteren Vorgaben.

4.9 Sperrung und Suspendierung von Zertifikaten

Die CA darf ausgestellte Zertifikate nicht suspendieren.

4.9.1 Gründe für Sperrungen

Teilnehmerzertifikate müssen durch die CA gesperrt werden bzw. der Zertifikatsnehmer muss die Sperrung durch die CA veranlassen, sobald einer der in der „Certificate Policy Root-CA der PKI-1-Verwaltung“ genannten oder einer der im Folgenden genannten Sperrgründe vorliegt:

- Abhandenkommen des privaten Schlüssels (z.B. Verlust oder Diebstahl des Schlüsselträgers)
- Der Teilnehmer scheidet aus dem Dienst aus, der Betrieb der technischen Komponente wird eingestellt, die organisatorische Einheit oder Funktion bzw. Funktionsbereich wird aufgelöst oder der Schlüsselverantwortliche scheidet aus dem Dienst aus, ohne dass ein Nachfolger benannt wurde
- Eine Kompromittierung oder der Verdacht auf eine Kompromittierung des privaten Schlüssels liegt vor
- Angaben im Zertifikat sind nicht mehr korrekt
- Missbrauch oder Verdacht auf Missbrauch durch den Zertifikatsnehmer oder andere zur Nutzung des Schlüssels berechtigte Personen

4.9.2 Wer kann eine Sperrung initiieren

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Die Sperrung von Zertifikaten darf immer durch die folgenden Rollen und Stellen initiiert werden:

- Leitung des CA-Betreibers
- Der zuständige Informationssicherheitsbeauftragte des Zertifikatsnehmers
- Zertifikatseigentümer (Der Zertifikatsnehmer bei Zertifikaten für natürliche Personen und Schlüsselverantwortliche bei anderen Zertifikaten)

Zusätzlich darf die Sperrung von Zertifikaten natürlicher Personen durch die von der für den Zertifikatsnehmer zuständigen personalbearbeitenden Stelle initiiert werden.

Die Sperrung von anderen Zertifikaten kann zusätzlich von der Dienststellenleitung des Schlüsselverantwortlichen oder einer vorher gegenüber der CA benannten Stelle initiiert werden.

4.9.3 Ablauf von Sperrungen

Keine über die CP „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.9.4 Fristen für den Zertifikatsinhaber

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.9.5 Bearbeitungsfristen für die CA

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Nach durchgeführter Risikoabschätzung sollte die Bearbeitung eines Sperrantrages von Teilnehmerzertifikaten innerhalb eines Arbeitstages erfolgt sein.

4.9.6 Anforderung zu Zertifikatsprüfungen durch Zertifikatsnutzer (Relying Parties)

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.9.7 Häufigkeit der Sperrlistenveröffentlichung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.9.8 Maximale Latenzzeit für Sperrlisten

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.9.9 Orte für Online-Statusabfragen (OCSP/CRL)

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.9.10 Anforderungen an Online-Statusabfragen (OCSP/CRL)

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.9.11 Andere verfügbare Formen der Sperrungsbekanntmachung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.9.12 Anforderungen bei Kompromittierung von privaten Schlüsseln

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Bei Kompromittierung von privaten Schlüsseln oder bei Verdacht auf Kompromittierung muss eine Meldung gemäß dem in der Allgemeinen Reglung A-960/1 festgelegten Vorgehen erstattet werden

4.9.13 Gründe für eine Suspendierung

Keine - Siehe erster Absatz Kapitel 4.9.

4.9.14 Wer kann Suspendierung initiieren

Keiner - Siehe erster Absatz Kapitel 4.9.

4.9.15 Ablauf einer Suspendierung

Nicht zulässig - Siehe erster Absatz Kapitel 4.9.

4.9.16 Maximale Sperrdauer bei Suspendierung

Nicht zulässig - Siehe erster Absatz Kapitel 4.9.

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP/CRL)

4.10.1 Betriebsbedingte Eigenschaften

Die CA muss Informationen zum Zertifikatsstatus mindestens über Sperrlisten, siehe Kapitel 2, veröffentlichen.

Die CA sollte zusätzlich Informationen zum Zertifikatsstatus über OCSP-Funktionalitäten bereitstellen.

4.10.2 Verfügbarkeit des Dienstes

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Die Dienste zur Statusabfrage von Zertifikaten müssen 24/7 mit

- einer Verfügbarkeit von mindestens 99% (entspricht ca. 87 Stunden Gesamtausfall pro Jahr) und
- einer maximalen Einzelstörungsdauer von einem Tag

zur Verfügung stehen.

Abweichungen können in Rücksprache mit der PMABw genehmigt werden. Die Genehmigung ist in Textform einzuholen.

4.10.3 Weitere Merkmale

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

4.11 Beendigung des Vertragsverhältnisses

Für die Beendigung des Vertragsverhältnisses mit dem BSI gelten die Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“.

Für die Zertifikatsnehmer dieser CA gilt:

- Der Zertifikatsbezug durch natürliche Personen muss automatisch bei Ausscheiden aus dem Dienst beendet werden.
- Bei Funktionszertifikaten muss durch den Zertifikatsnehmer dargestellt werden, inwiefern die Einstellung aufgrund Ausscheiden/Versetzung des Schlüsselverantwortlichen, Aussonderung der Funktion zugrundeliegender Hard- und Software erfolgt, oder Zertifikate aus einer anderen Zertifizierungsstelle innerhalb der PKIBw bereitgestellt werden.

4.12 Schlüsselhinterlegung und -wiederherstellung (Key Escrow und Recovery)

4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und –wiederherstellung

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Die CA kann den Zertifikatsnehmern bzw. den zuständigen Schlüsselverantwortlichen treuhänderische Hinterlegung und Wiederherstellung ihrer privaten Schlüssel anbieten. Bei der Wiederherstellung muss der antragstellende Zertifikatsnehmer bzw. der zuständige Schlüsselverantwortliche eindeutig identifiziert werden. Die Schlüssel müssen auf einem Schlüsselträger mit mindestens dem gleichen Sicherheitsniveau wie bei der ursprünglichen Ausstellung übergeben werden.

Die Hinterlegung darf ausschließlich für Teilnehmerzertifikate, welche ausschließlich für eine Verschlüsselung verwendet werden, erfolgen. Die Hinterlegung von privaten Schlüsseln, die für Signatur- oder Authentifizierungszertifikate verwendet werden, ist nicht zulässig.

Die CA muss den Prozess zur Identifizierung des Zertifikatsnehmers, zur Wiederherstellung der Schlüssel und zur Übergabe des Schlüssels unter Berücksichtigung der Regelungen in der „Certificate Policy Root-CA der PKI-1-Verwaltung“ in ihrem CPS beschreiben.

Eine Wiederherstellung von durch die CA gespeicherten privaten Schlüsseln an eine andere Stelle als den Zertifikatsnehmer bzw. den zuständigen Schlüsselverantwortlichen darf

- für Zertifikatsnehmer der Bundeswehr (Zertifikatsnehmer aus den Verzeichnisdienstzweigen Militär, Zivil, Extern) ausschließlich auf Antrag der Leitung CSOCBw im ZCSBw oder
- für Zertifikatsnehmer der BWI (Zertifikatsnehmer aus dem Verzeichnisdienstzweig BWI) ausschließlich auf Antrag der Leitung CERT BWI

- erfolgen.

Die Wiederherstellung muss auf einem Hardware-Schlüsselträger erfolgen, bei der die privaten Schlüssel nicht aus dem geschützten Speicher des Hardware-Schlüsselträgers ausgelesen werden können. Für den Zugriff auf die Schlüssel muss durch getrennte Ausgabe von Hardware-Schlüsselträger und zugehöriger Aktivierungsdaten ein Vier-Augen-Prinzip eingehalten werden.

Die beantragende Stelle muss vor der Beantragung der Herausgabe privater Schlüssel sicherstellen, dass die rechtlichen Grundlagen für die Wiederherstellung vorliegen und die Mitbestimmungsgremien korrekt eingebunden wurden.

Die CA muss den Prozess zur Schlüsselwiederherstellung sowie zur Ausgabe der Hardware-Schlüsselträger und Aktivierungsdaten unter Berücksichtigung der Regelungen in der „Certificate Policy Root-CA der PKI-1-Verwaltung“ in ihrem CPS beschreiben.

4.12.2 Richtlinien und Praktiken zum Schutz und Wiederherstellung von Sitzungsschlüsseln

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Neben den Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“ müssen CA für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) zusätzlich die TR-03145-VS-NfD einhalten.

5.1.1 Einsatzort und Bauweise

Keine über die im ersten Absatz Kapitel 5.1 hinausgehenden Regelungen.

5.1.2 Räumlicher Zugang

Keine über die im ersten Absatz Kapitel 5.1 hinausgehenden Regelungen.

5.1.3 Stromversorgung und Klimaanlagen

Keine über die im ersten Absatz Kapitel 5.1 hinausgehenden Regelungen.

5.1.4 Gefährdung durch Wasser

Keine über die im ersten Absatz Kapitel 5.1 hinausgehenden Regelungen.

5.1.5 Brandschutz

Keine über die im ersten Absatz Kapitel 5.1 hinausgehenden Regelungen.

5.1.6 Aufbewahrung von Datenträgern

Keine über die im ersten Absatz Kapitel 5.1 hinausgehenden Regelungen.

5.1.7 Entsorgung

Keine über die im ersten Absatz Kapitel 5.1 hinausgehenden Regelungen.

5.1.8 Externes Notfall-Backup

Keine über die im ersten Absatz Kapitel 5.1 hinausgehenden Regelungen.

5.2 Organisatorische Sicherheitsmaßnahmen

Neben den Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“ muss die CA für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) zusätzlich die TR-03145-VS-NfD einhalten.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an Mitarbeiter

Neben den Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“ müssen CA für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) zusätzlich die TR-03145-VS-NfD einhalten.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Neben den Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“ müssen CA für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) zusätzlich die TR-03145-VS-NfD einhalten und das Personal der CA muss mindestens mit einer "erweiterten Sicherheitsüberprüfung“ Ü2/Sabotageschutz überprüft sein.

5.3.3 Anforderungen an Schulungen

Alle Mitarbeiter der CA müssen mindestens über fundierte Kenntnisse in den Bereichen

- allgemeines EDV-Wissen,
- Grundlagen der Info-Sicherheit und
- Grundlagen der Kryptografie,
- Grundlagen zu PKI

verfügen.

Die Mitarbeiter der CA, die mit der technischen und fachlichen Administration der Systeme und Software der CA oder RA betraut sind, müssen zusätzlich mindestens über eine fundierte Ausbildung im Umfeld

- des Systemmanagements und/oder
- des Sicherheitsmanagements

der administrierten Systeme und Software verfügen, die sie dazu befähigt die jeweiligen Systeme und Software zu installieren, zu konfigurieren und Fehlersituationen zu analysieren und Lösungsvorschläge zu entwickeln.

Darüber hinaus müssen die Mitarbeiter der CA, einschließlich der Mitarbeiter der RA, in die Bedienung der CA-Software und RA-Software Abhängigkeit der auszuübenden Rolle ausgebildet werden.

Die initiale Ausbildung der Mitarbeiter des CA, einschließlich der Mitarbeiter der RA, muss gemäß einem Ausbildungskonzept erfolgen oder die Mitarbeiter können einen Nachweis der erforderlichen Fachkenntnisse bzw. Ausbildungen vorweisen.

Bei Produkt-/Versionsänderungen von eingesetzten Systemen und Software muss ab diesem Zeitpunkt bei der initialen Ausbildung, die Ausbildung auf das neue Produkt bzw. auf die neue Version der Systeme und Software erfolgen und eine Anpassung des Ausbildungskonzeptes muss initiiert werden.

5.3.4 Häufigkeit und Anforderungen an Fortbildungen

Alle Mitarbeiter der CA, einschließlich der Mitarbeiter der RA, müssen jährlich eine Auffrischungsausbildung in den Bereichen

- Grundlagen der IT-/Cybersicherheit
- Grundlagen des Datenschutzes
- Grundlagen zum Brandschutz

durchführen.

Allen Mitarbeitern der CA, einschließlich der Mitarbeiter der CRA, sollten jährlich die Möglichkeit zur Durchführung von Weiterbildungsmaßnahmen angeboten werden, zur Vertiefung oder Auffrischung des allgemeinen EDV-Wissen, zur PKI und zur Kryptografie.

Allen Mitarbeitern der CA, die mit der technischen und fachlichen Administration der Systeme und Software der CA oder RA betraut sind, sollten jährlich die Möglichkeit zur Durchführung von Weiterbildungsmaßnahmen angeboten werden, zur Vertiefung oder Auffrischung der Kenntnisse im Umfeld des System- bzw. Sicherheitsmanagements der administrierten Systeme und Software.

Mitarbeiter von LRA sollten jährlich eine Auffrischungsausbildung in der Bedienung der RA-Software und der zugrundeliegenden Prozesse nachweisen.

Anlassbezogen oder bei Produkt- oder Versionsänderungen der eingesetzten Systeme und Software, müssen die Mitarbeiter der CA, einschließlich der Mitarbeiter der RA in Abhängigkeit der auszuübenden Rolle in die Bedienung/Administration ausgebildet und weitergebildet gebildet.

Die Fortbildungen der Mitarbeiter der CA, einschließlich Mitarbeiter der RA, muss gemäß eines Ausbildungskonzepts erfolgen und kann entweder als Ausbildung am Arbeitsplatz, Inhouseschulung bei der CA, an einer der Schulungseinrichtungen der Bundeswehr oder bei einem externen Bildungsträger erfolgen.

5.3.5 Häufigkeit und Ablauf von Arbeitsplatzwechseln

Neben den Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“ müssen CA für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) zusätzlich die TR-03145-VS-NfD einhalten.

5.3.6 Sanktionen für unerlaubte Handlungen

Keine weiteren Vorgaben.

5.3.7 Anforderungen an weitere Auftragnehmer

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

5.3.8 Dokumentation für Mitarbeiter

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Der Leitung der CA müssen alle Dokumente und Handbücher zum Betrieb der CA und CRA vorliegen. Allen Mitarbeitern der CA und RA müssen die zur Ausübung ihrer Rolle notwendigen Dokumente und Handbücher ausgehändigt werden.

5.4 Überwachung/Protokollierung

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Durch die CA müssen die zentrale Vorgaben der Informationssicherheit für die Protokollierung und deren Auswertung in der Informations- und Betriebstechnik für die Bundeswehr (Regelung der Bundeswehr A1-960/1-4532) umgesetzt werden.

CA für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) müssen zusätzlich die TR-03145-VS-NfD einhalten.

5.4.1 Überwachte Ereignisse

Keine über die im ersten Absatz Kapitel 5.4 hinausgehenden Regelungen.

5.4.2 Häufigkeit der Protokollanalyse

Keine über die im ersten Absatz Kapitel 5.4 hinausgehenden Regelungen.

5.4.3 Aufbewahrungsfrist für Protokolldaten

Keine über die im ersten Absatz Kapitel 5.4 hinausgehenden Regelungen.

5.4.4 Schutz von Protokolldaten

Keine über die im ersten Absatz Kapitel 5.4 hinausgehenden Regelungen.

5.4.5 Backup der Protokolldaten

Keine über die im ersten Absatz Kapitel 5.4 hinausgehenden Regelungen.

5.4.6 Überwachungssystem (intern oder extern)

Keine über die im ersten Absatz Kapitel 5.4 hinausgehenden Regelungen.

5.4.7 Benachrichtigung bei schwerwiegenden Ereignissen

Keine über die im ersten Absatz Kapitel 5.4 hinausgehenden Regelungen.

5.4.8 Schwachstellenanalyse

Keine über die im ersten Absatz Kapitel 5.4 hinausgehenden Regelungen.

5.5 Archivierung

5.5.1 Archivierte Daten

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

5.5.2 Aufbewahrungsfrist für archivierte Daten

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

5.5.3 Schutz der Archive

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

5.5.4 Backup der Archive (Datensicherungskonzept)

Keine weiteren Vorgaben.

5.5.5 Anforderungen an Zeitstempel

Keine weiteren Vorgaben.

5.5.6 Archivierungssystem (intern oder extern)

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

5.5.7 Prozeduren für Abruf und Überprüfung archivierter Daten

Keine weiteren Vorgaben.

5.6 Schlüsselwechsel der Zertifizierungsstelle

Die Nutzungsdauer des CA-Schlüssels darf maximal 6 Jahren (zuzüglich Karenzzeit) betragen. Es sollte regelmäßig ein Schlüsselwechsel (Neubeantragung einer CA bei dem BSI) erfolgen.

Dieser sollte grundsätzlich im einjährigen Rhythmus erfolgen. Der Fingerabdruck des neuen CA-Zertifikats sollte über einen sicheren Kanal, z.B. der HTTPS-Website der CA, für die Zertifikatsnutzer veröffentlicht werden. Es sollten mehrere gültige CA-Zertifikate zur Verfügung stehen.

5.7 Notfallmanagement

Neben den Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“ müssen CA für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) zusätzlich die TR-03145-VS-NfD einhalten.

5.7.1 Prozesse für Sicherheitsvorfälle und Kompromittierung

Es gelten die im ersten Absatz Kapitel 5.7 genannten Regelungen, die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

- Sicherheitsvorfälle müssen gemäß dem in der Allgemeinen Reglung A-960/1 festgelegten Vorgehen zum „Meldewesen für und Behandlung von Informationssicherheitsvorkommnissen“ gemeldet und behandelt werden.
- Der Verdacht oder die Feststellung der CA-Schlüsselkompromittierung ist ein Informationssicherheitsvorkommnis (InfoSichhVork) und muss gemäß dem in der Allgemeinen Reglung A-960/1 festgelegten Vorgehen zum „Meldewesen für und Behandlung von Informationssicherheitsvorkommnissen“ gemeldet und behandelt werden.
- Die im Rahmen der Behandlung des InfoSichhVork bei CA-Schlüsselkompromittierung durchzuführenden Maßnahmen müssen in einem Notfallhandbuch beschrieben und als kryptografischer Notfall behandelt werden.

5.7.2 Betriebsmittel, Software und/oder Daten sind korrumpiert

Es gelten die im ersten Absatz Kapitel 5.7 genannten Regelungen, die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Sind Betriebsmittel, Software und bzw. oder Daten korrumpiert oder besteht der Verdacht darauf, dass ein InfoSichVork vorliegt, muss dies gemäß dem in der Allgemeinen Reglung A-960/1 festgelegten Vorgehen zum „Meldewesen für und Behandlung von Informationssicherheitsvorkommnissen“ gemeldet und behandelt werden.

5.7.3 Kompromittierung des privaten Schlüssels

Es gelten die im ersten Absatz Kapitel 5.7 genannten Regelungen, die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Der Verdacht oder die Feststellung der Kompromittierung des privaten Schlüssels ist ein InfoSichhVork und muss gemäß dem in der Allgemeinen Reglung A-960/1 festgelegten Vorgehen zum „Meldewesen für und Behandlung von Informationssicherheitsvorkommnissen“ gemeldet und behandelt werden.

5.7.4 Wiederaufnahme des Betriebs nach einem Notfall

Es gelten die im ersten Absatz Kapitel 5.7 genannten Regelungen und die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung

5.8 Einstellung des Betriebs

Neben den Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“ müssen CA für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) zusätzlich die TR-03145-VS-NfD einhalten.

6 Technische Schutzmaßnahmen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.1 Schlüsselerzeugung und Installation

6.1.1 Schlüsselerzeugung

Neben den Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“ müssen CA für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) zusätzlich die TR-03145-VS-NfD einhalten.

6.1.2 Übermittlung privater Schlüssel an Zertifikatsinhaber

Es gelten die im ersten Absatz Abschnitt 5.7 genannten Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

CA, die zentral Schlüsselmaterial erzeugen und an den Zertifikatsnehmer bzw. Schlüsselverantwortlichen übermitteln, müssen die TR-03145-1 Abschnitt 5.4.2 und 5.4.3 einhalten. CA für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) müssen zusätzlich die TR-03145-VS-NfD einhalten.

6.1.3 Übermittlung öffentlicher Schlüssel an Zertifikatsaussteller

Zur Übermittlung des öffentlichen CA-Schlüssels an die Root-CA gelten die Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“. Das Verfahren des zuverlässigen Nachweises der CA-Schlüsselerzeugung für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 und 6.2.1 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) muss im CPS beschrieben werden.

Werden die Schlüssel bei den Zertifikatsnehmern der CA, außerhalb der gesicherten Umgebung der CA erzeugt, so muss der Zertifizierungsantrag in einem Format bei der CA eingereicht werden, in welchem der öffentliche Schlüssel gegen Manipulation gesichert wird. Hierfür sollte das PKCS#10-Format eingesetzt werden.

Die CA muss den Zertifizierungsantrag auf Manipulationen prüfen und ablehnen, wenn eine Manipulation nicht ausgeschlossen werden kann.

Das eingesetzte Verfahren und die Maßnahmen zur Prüfung müssen im CPS der CA beschrieben werden.

6.1.4 Übermittlung öffentlicher CA-Schlüssel an Zertifikatsnutzer (Relying Parties)

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.1.5 Schlüssellängen

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

CA-Schlüssel sollten bei Nutzung des Rivest-Shamir-Adleman-Algorithmus (RSA) eine Schlüssellänge von mindestens 4096 Bit besitzen.

Ausgestellte Zertifikate der CA sollten bei Nutzung von RSA eine Schlüssellänge von mindestens 4096 Bit besitzen.

Stellt die CA Zertifikate aus, die bei Nutzung von RSA nur die Mindestvorgabe aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“ für die Schlüssellänge erfüllen, muss die CA dies mit nachweisbarer technischer Begründung des Zertifikatsnehmers dokumentieren.

6.1.6 Erzeugung der Public-Key-Parameter und Qualitätssicherung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.1.7 Schlüsselverwendungszwecke (X.509v3 Key Usage)

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.2 Schutz privater Schlüssel und Einsatz kryptographischer Module

6.2.1 Standard kryptographischer Module

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.2.2 Kontrolle über den privaten Schlüssel durch zwei Personen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.2.3 Hinterlegung privater Schlüssel (Key Escrow)

Neben den Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“ müssen CA für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) zusätzlich die TR-03145-VS-NfD einhalten.

6.2.4 Backup privater Schlüssel

Neben den Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“ müssen CA für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) zusätzlich die TR-03145-VS-NfD einhalten.

6.2.5 Archivierung privater Schlüssel

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.2.6 Transfer privater Schlüssel in oder aus einem kryptographischen Modul

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.2.7 Speicherung privater Schlüssel in einem kryptographischen Modul

Neben den Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“ müssen CA für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) zusätzlich die TR-03145-VS-NfD einhalten.

6.2.8 Aktivierung (Nutzung) privater Schlüssel

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.2.9 Deaktivierung privater Schlüssel

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.2.10 Vernichtung privater Schlüssel

Es gelten die Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“. Die technische Leitlinie des BSI „Löschen und Vernichten von Verschlusssachen auf Datenträgern“ (BSI TL-M50) muss dabei berücksichtigt werden.

6.2.11 Güte kryptographischer Module

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation der Aktivierungsdaten

Aktivierungsdaten müssen den gültigen Vorgaben zur Erzeugung von Passwörtern/PINs in der Bundeswehr entsprechen.

6.4.2 Schutz der Aktivierungsdaten

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Wenn zutreffend, muss die CA Abschnitt 5.4.3 der BSI TR-03145-1 einhalten.

Die CA muss ihre Zertifikatsnehmer bzw. Schlüsselverantwortlichen verpflichten, dass der Schutz der Aktivierungsdaten vor dem weiteren Zugriff Dritter in deren Verantwortung liegt.

6.4.3 Weitere Aspekte

Keine weiteren Vorgaben.

6.5 Sicherheitsmaßnahmen für Computer

6.5.1 Spezifische Anforderungen an technische Sicherheitsmaßnahmen

Neben den Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“ müssen CA für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) zusätzlich die TR-03145-VS-NfD einhalten.

6.5.2 Güte der Sicherheitsmaßnahmen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.6 Technische Maßnahmen im Lebenszyklus

6.6.1 Systementwicklungskontrollen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.6.2 Sicherheitsverwaltungskontrollen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.6.3 Lebenszyklus-Sicherheitskontrollen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Die CA muss mindestens die Vorgaben aus Abschnitt 6.9 der TR-03145-1 einhalten.

Die CA sollte die Allgemeine Reglung der Bundeswehr A1-960/0-4514 „Absicherung von Netzübergängen“ einhalten.

Für den Anwendungsbereich mit Schutzniveau „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nach Abschnitt 1.4 der „Certificate Policy Root-CA der PKI-1-Verwaltung“) muss die CA zusätzlich die TR-03145-VS-NFD einhalten.

6.8 Zeitstempel

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

7 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen

7.1 Zertifikatsprofil

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

7.1.1 Versionsnummer

Für die CA gelten die für die Root-CA beschriebenen Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“.

7.1.2 Zertifikatserweiterungen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

7.1.3 Algorithmus-Bezeichner (OID)

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

7.1.4 Namensformen

Siehe Kapitel 3.1.

7.1.5 Namensbeschränkungen

Siehe Kapitel 3.1.

7.1.6 Bezeichner für CPs (OID)

Vom BSI wurden der CA der Bundeswehr die folgenden OID zugewiesen:

(1) 0.4.0.127.0.7.3.6.1.1.9.3 (Zertifikate ohne Zulassung für VS-NfD)

(2) 0.4.0.127.0.7.3.6.1.1.9.4 (Zertifikate mit Zulassung für VS-NfD)

Für die internen Zwecke der Bundeswehr wird außerdem die folgende OID aus dem privaten OID-Zweig der Bundeswehr der CA zugewiesen:

(3) 1.3.6.1.4.1.14275.1.1.1.1.1.1[2]

In Teilnehmerzertifikaten muss in das Feld „Policy Identifier“, abhängig von dem erreichten Schutzgrad, die OID (1) oder (2) an erster Stelle gesetzt werden.

Die OID (3) muss in jedem Teilnehmerzertifikat an zweiter Stelle gesetzt werden.

Die im Teilnehmerzertifikat gesetzte OID entspricht nicht den OID, welche in den CA-Zertifikaten der CA und der Root-CA gesetzt sind. Dies folgt der Vorgabe der „Certificate Policy Root-CA der PKI-1-Verwaltung“, widerspricht aber dem RFC 5280 und bricht die Prüfung der Zertifikatskette.

Die CA darf deshalb in den von ihr ausgestellten Teilnehmerzertifikaten das „Critical-Flag“ für die Erweiterung „certificatePolicies“ nicht auf „true“ setzen.

7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkungen (Policy Constraints)

Keine weiteren Vorgaben.

---

[2] Die OID ist wie folgt zusammengesetzt:

{Durch IANA zugewiesene OID der Deutschen Bundeswehr (1.3.6.1.4.1.14275) Übergreifende IT (1) PKIBW (1) Operativ (1) Policy (1) Policy RSA (1) Policy vPKI (1)}

7.1.8 Syntax und Semantik von Policy Qualifiern

Keine weiteren Vorgaben.

7.1.9 Verarbeitung von kritischen Erweiterungen für CPs

Keine weiteren Vorgaben.

7.2 Sperrlistenprofil

7.2.1 Versionsnummer

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

7.3 OCSP-Profil

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

7.3.1 Versionsnummer

Keine über die im ersten Absatz von Abschnitt 7.3 der „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehende Regelungen.

7.3.2 OCSP-Erweiterungen

Keine über die im ersten Absatz von Abschnitt 7.3 der „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehende Regelungen.

8 Konformitätsprüfung und andere Beurteilungskriterien

Es gelten die Regelungen der „Certificate Policy Root-CA der PKI-1-Verwaltung“ und darüber hinaus die folgenden Festlegungen.

Der Betreiber einer CA muss diese CP einhalten.

8.1 Häufigkeit und Umstände der Überprüfung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

8.2 Identität und Qualifikation des Überprüfers

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

8.3 Verhältnis von Prüfer zu Überprüftem

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

8.4 Überprüfte Bereiche

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

8.5 Mängelbeseitigung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

8.6 Veröffentlichung der Ergebnisse

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

9 Andere geschäftliche und rechtliche Angelegenheiten

9.1 Gebühren und Auslagen

9.1.1 Gebühren für Zertifikatserstellung oder -erneuerung

Keine weiteren Vorgaben.

9.1.2 Gebühren für Zugriff auf Zertifikate

Keine weiteren Vorgaben.

9.1.3 Gebühren für Sperrung oder Statusabfragen

Keine weiteren Vorgaben.

9.1.4 Andere Gebühren und Auslagen

Keine weiteren Vorgaben.

9.1.5 Gebührenerstattung

Keine weiteren Vorgaben.

9.2 Finanzielle Verantwortung

9.2.1 Versicherungsschutz

Die CA darf keine Versicherungen zugunsten der PKI-Teilnehmer abschließen.

9.2.2 Sonstige Vermögenswerte

PKI-Teilnehmer müssen keine Erklärung abgeben, dass diese Zugang zu anderen Vermögenswerten haben, um den Betrieb zu unterstützen und um Schadensersatz für mögliche Haftung zu zahlen.

9.2.3 Versicherung oder Garantie für Endteilnehmer

Die CA darf keine Versicherungen zugunsten der Endteilnehmer abschließen. Gewährleistungsansprüche müssen ausgeschlossen werden.

9.3 Vertraulichkeit von Informationen

9.3.1 Vertraulich zu behandelnde Informationen

Informationen der CA, die nicht in Kapitel 9.3.2 aufgeführt sind, unterliegen mindestens der allgemeinen Amtsverschwiegenheit (Einstufung: OFFEN – Amts- und Dienstgeheimnis).

9.3.2 Nicht vertraulich zu behandelnde Informationen

Als nicht vertraulich zu behandelnde Informationen gelten für die CA mindestens folgende Informationen:

- Von der CA genutzte öffentliche Schlüssel
- Sperrlisten
- Die zugrundeliegenden CP

Die CA kann weitere Informationen als nicht vertraulich zu behandelnde Informationen festlegen.

9.3.3 Schutz vertraulicher Informationen

Die CA muss vertraulich zu behandelnde Informationen gemäß ihrer Einstufung und Schutzbedürftigkeit schützen.

9.4 Schutz personenbezogener Daten

Die CA muss die Vorgaben zur Verarbeitung, Einstufung, Nutzung und Schutz personenbezogener Daten in der Bundeswehr berücksichtigen.

9.4.1 Vorgabe zur Verarbeitung personenbezogener Daten

Siehe erster Absatz vom Kapitel 9.4.

9.4.2 Vertraulich zu behandelnde personenbezogene Daten

Siehe erster Absatz vom Kapitel 9.4.

9.4.3 Nicht vertraulich zu behandelnde personenbezogene Daten

Siehe erster Absatz vom Kapitel 9.4.

9.4.4 Schutz personenbezogener Daten

Siehe erster Absatz vom Kapitel 9.4.

9.4.5 Einwilligung und Nutzung personenbezogener Daten

Siehe erster Absatz vom Kapitel 9.4.

9.4.6 Offenlegung bei gerichtlicher Anordnung oder im Rahmen gerichtlicher Beweisführung

Offenlegung bei gerichtlicher Anordnung oder im Rahmen gerichtlicher Beweisführung muss durch die CA nachgekommen werden.

9.4.7 Andere Umstände einer Veröffentlichung

Das Bundesdatenschutzgesetz (BDSG) und die europäische Datenschutzgrundverordnung (EU-DSGVO) räumen jedem das Recht ein, Auskunft über die von ihm gespeicherten Daten einzuholen. Die CA muss diesem Auskunftsersuchen nachkommen. Die CA sollte nur Auskunftsersuchen nachkommen, bei denen eine eindeutige Identifizierung des Auskunftsersuchenden gewährleistet ist.

9.5 Urheberrechte

Die von der CA ausgegebenen Zertifikate und Sperrlisten sind Eigentum der Bundeswehr. Zertifikate und Sperrlisten dürfen, sofern sie in einem öffentlichen Verzeichnis hinterlegt sind, durch Teilnehmer der PKIBw uneingeschränkt abgerufen und genutzt werden. Die Weiterverbreitung, insbesondere die Bereitstellung in einem durch Dritte betriebenen Verzeichnis, erfordert die ausdrückliche Genehmigung der PMA.

9.6 Verpflichtungen

9.6.1 Verpflichtung der CAs

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

9.6.2 Verpflichtung der RAs

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

9.6.3 Verpflichtung des Zertifikatsinhabers

Siehe Kapitel 4.5.1.

9.6.4 Verpflichtung der Zertifikatsnutzer

Siehe Kapitel 4.5.2.

9.6.5 Verpflichtung anderer Teilnehmer

Keine weiteren Vorgaben.

9.7 Gewährleistung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

9.8 Haftungsbeschränkung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

9.9 Haftungsfreistellung/Schadenersatz

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

9.10 Gültigkeit und Aufhebung

9.10.1 Gültigkeit

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

9.10.2 Aufhebung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

9.10.3 Konsequenzen der Aufhebung

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

Keine weiteren Vorgaben.

9.12 Änderungen der CP

9.12.1 Vorgehen bei Änderungen

Ändert sich die „Certificate Policy Root-CA der PKI-1-Verwaltung“ muss dieses Dokument und die CPS der CA auf Aktualität überprüft werden.

Für Änderungen dieses CP siehe Kapitel 1.5.1.

Nach Änderung dieser CP muss das CPS der CA auf Aktualität geprüft werden.

9.12.2 Benachrichtigungsmechanismus und Fristen

Jede aktualisierte und genehmigte Version dieser CP muss den Zertifikatsnutzern unverzüglich über die Veröffentlichungspunkte der CA bereitgestellt werden.

9.12.3 Umstände, die eine Änderung des CP-Bezeichners (OID) erfordern

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

9.13 Konfliktbeilegung

Neben den Regelungen in der „Certificate Policy Root-CA der PKI-1-Verwaltung“ kann eine Konfliktbeilegung unter Vermittlung der PMABw zwischen der CA und seinen Zertifikatsnehmern stattfinden.

9.14 Geltendes Recht

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

9.15 Konformität mit geltendem Recht

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

9.16 Weitere Regelungen

9.16.1 Vollständigkeit

Keine weiteren Vorgaben.

9.16.2 Abtretung der Rechte

Für die CA gelten gegenüber der Root-CA die Regelungen aus der „Certificate Policy Root-CA der PKI-1-Verwaltung“.

Darüber hinaus gelten keine weiteren Regelungen für die Zertifikatsnehmer gegenüber der CA.

9.16.3 Salvatorische Klausel

Keine weiteren Vorgaben.

9.16.4 Rechtliche Auseinandersetzungen/Erfüllungsort

Keine über die „Certificate Policy Root-CA der PKI-1-Verwaltung“ hinausgehenden Regelungen.

9.16.5 Höhere Gewalt

Keine weiteren Vorgaben.

9.16.6 Andere Regelungen

Keine weiteren Vorgaben.