Zertifizierungsrichtlinie der Public Key Infrastructure der Bundeswehr (PKIBw), Anteil Verwaltungs-PKI

Die Kennung (OID) dieser Zertifizierungsrichtlinie lautet:
1.3.6.1.4.1.14275.1.1.1

Version:	1.2.12.3
Datum:	15.07.2020

Änderungsnachweis

Datum	Version	Autor	Änderung und Änderungsgrund	Kapitel
08.03. - 14.03.2005	1.0.5	BAAINBw H1.4	Gemäß Mitprüfungsbemerkungen PMABw	1, 1.1, 1.2, 1.3.3, 1.3.5, 1.4.1, 4.1.2, 4.1.3
21.03.2005	1.0.6	BAAINBw H1.4	Beschluss der Koordinierungsgruppe IT-Sicherheit vom 15.03.05	1.3.5, 1.4.1
24.11.2005	1.0.7	BWI Systeme GmbH	Einarbeiten der Kommentierungen vom 9. und 14.11.2005	Deckblatt, 1.1, 2.9
28.11.2005	1.0.8	BAAINBw H1.4	Einarbeiten der offenen Kommentierungen vom 14.11.2005	1.3.2, 1.3.4
08.03.2007	1.0.8a	BAAINBw H1.4	Änderung der Kontaktdaten	1.4.2
08.04.2008	1.0.9	BAAINBw H1.4	Aufnahme Pseudonyme Aufnahme OCSP Überarbeitung Prozesse Schlüsselverantwortliche Überarbeitung aufgrund Änderung ZDV 54/100 und gesetzlicher Vorgaben Redaktionelle Änderungen	1.3.4, 3.1.8, 4.1.1 2.6.4, 4.4.11, 4.4.12 3.1.9, 3.1.10, 4.1.2, 4.1.3 1.3.5, 2.8.1, 2.8.2, 6.1.4 1.4.1, 2.6.1, 2.6.2, 2.6.3, 4.6.1
18.04.2008	1.1.0	BAAINBw H1.4	Einarbeitung Mitprüfungsbemerkungen	4.3.2, 6.2.3
23.10.2008	1.1.1	BAAINBw H1.4	Einarbeitung Prüfbemerkungen BSI	3.1.10
17.12.2008	1.1.2	BWI Systeme GmbH	Redaktionelle Änderungen Präzisierung Pseudonyme Überarbeitung der eingesetzten Algorithmen	Alle 1.3.4, 2.8.2, 3.1.1, 3.12 6.1.4
14.09.2009	1.1.3	BWI Systeme GmbH	Überarbeitung der eingesetzten Algorithmen	6.1.4
08.02.2010	1.1.3a	BAAINBw H1.4	Änderung der Kontaktdaten	1.4.2
21.06.2010	1.1.3b	BAAINBw H1.4	Änderung der Kontaktdaten	1.4.2
25.06.2010	1.1.4	BWI Systeme GmbH	Überarbeitung Einsatzgebiete Präzisierung Verweis zur Häufigkeit der Aktualisierung der Sperrlisten Überarbeitung der akzeptierten Ausweisdokument bei der Identifizierung von natürlichen Personen Überarbeitung der eingesetzten Algorithmen Überarbeitung des (verkürzten) Gültigkeitszeitraum der Zertifikate	1.3.5 2.6.2 3.1.8 6.1.4 6.3.2
03.09.2010	1.1.4a	BWI Systeme GmbH	Ablösung der PKIBw Nutzverwaltung durch Card Management System (CMS) Persönliches Erscheinen bei der Beantragung von Zertifikaten für OrgEinheiten entfällt (nur noch elektronische Beantragung) Überarbeitung Schutzbereiche für personenbezogene Daten aufgrund der geänderten Durchführungsbestimmungen zum BDSG im Geschäftsbereich BMVg	Alle 3.1.9 4.1.2
14.10.2010	1.1.5	BWI Systeme GmbH	Ergänzung Code-Signing Zertifikate	

Datum	Version	Autor	Änderung und Änderungsgrund	Kapitel
14.01.2011	1.1.6	BWI Systeme GmbH	Änderungen bei der Antragstellung von Zertifikaten für OrgEinheiten und technische Komponenten (Chipkarten-basierte Authentisierung am CMS anstelle des Antrages per signierter E-Mail) Archivierte Daten	3.1.93.1.10 4.1.2 4.1.3 4.6.1
11.07.2011	1.1.7	BWI Systeme GmbH	Anpassung der Evaluierungsanforderungen bei der Generierung und Speicherung von Schlüsseln Aktualisierung der Bezugsdokumente	6.1.7 6.2.1 9
12.01.2012	1.1.8	BWI Systeme GmbH	Anpassung bzgl. elektronischen Versand von PIN-Briefen für Schlüsseldateien Änderung der Einstufung von Sperrkennwörtern Regelungen zur Vernichtung von Chipkarten Änderungen nach Kommentierung durch TrustCenterBw	4.3.26.4.2.2 2.8.1 6.2.9 2.1.1 2.6.4 2.7.1 2.8.3 4.1.2 4.4.9 6.3.2 6.7
25.09.2012	1.1.9	BWI Systeme GmbH	Anpassung Ausstellungsintervall der Sperrlisten	4.4.9
28.12.2012	1.1.10	BWI Systeme GmbH	Änderungen bei der Archivierung von Antragsformular und Empfangsbestätigung für Personen-Zertifikate Änderungen der akzeptierten Ausweisdokument zur Identifizierung von Personen Änderung zu Message Recovery (keine Beschreibung im Organisationshandbuch) Anpassung Überprüfung de r Protokolldaten Anpassung Überprüfung des Personals Namensänderungen in der Bundeswehrorganisation (BAAINBw statt IT-AmtBw, BMVg AIN IV 2 statt BMVg M II / IT 3)	4.1.1 4.6.1 3.1.8 4.4.3 4.5.2 5.3.2 Diverse
07.02.2013	1.1.11	BAAINBw H1.4	Anpassung an aktualisiertes IT-Sicherheitskonzept (Sicherheitsüberprüfung Personal)	5.3.2
27.05.2013	1.1.12	BWI Systeme GmbH	Anpassung bzgl. elektronischem PIN/PUK-Brief für Chipkarten und elektronischer Archivierung von eingescannten Antragsformularen und Empfangsbestätigungen Verwendung von SHA-256 für Personen-Zertifikate zu eDA / eTA mit Gültigkeitszeitraum von 5 (statt bisher 3) Jahren Vereinheitlichung der Begriffe Kennwort -> Passwort, Einarbeitung der Namensänderung PKIBw Endanwenderhandbuch -> PKIBw Nutzerleitfaden für Chipkarten, Redaktionelle Änderungen	4.1.1, 4.3.1, 4.3.2, 4.6.1 6.1.4, 6.3.2, 6.4.1.2, 6.4.2.2 alle
28.06.2013	1.1.13	BWI Systeme GmbH	Einarbeitung Anmerkungen des BSI Änderung der Gültigkeitsdauer der Zertifikate für Zertifizierungsstellen von 4 auf 6 Jahre Redaktionelle Änderungen	 6.3.2

Datum	Version	Autor	Änderung und Änderungsgrund	Kapitel
28.02.2014	1.1.14	BWI Systeme GmbH	Einarbeitung Archivierung und Wiederherstellung von privaten Entschlüsselungsschlüsseln für Teilnehmer und funktionsbezogene PKI-Karten (FktPKI)	1.1, 1.2, 1.3.4, 1.3.5, 2.1.2, 2.4.1, 2.8.2, 3.1.2, 3.1.4, 3.1.7, 3.1.11, 4.1.4, 4.2.1, 4.3.3, 4.4.1, 4.4.2, 4.4.3.4, 4.7.2, 6.1.1.1, 6.1.2, 6.1.4, 6.1.5, 6.1.7, 6.2.3, 6.2.4, 6.2.5, 6.2.6, 6.2.7, 6.3.2, 6.4.1.2, 6.4.2.2, 9
06.03.2014	1.1.15	BAAINBw H1.4	Redaktionelle Änderungen	4.4.3, 4.8.2, 6.1.1.1, 6.1.5, 6.1.7
30.05.2014	1.2	BWI Systeme GmbH	Einarbeitung Ausstellung temporärer PKI-Karten	1.3.2, 1.3.3, 1.3.4, 2.1.3, 3.1.2, 3.1.7, 3.3, 4.1., 4.1.1,, 4.2.1, 4.3.1, 4.4.3, 4.4.4, 4.6.1, 6.1, 6.2, 6.3
18.06.2014	1.2.1	BAAINBw H1.4	QS, redaktionelle Änderungen	1.3.4, 2.1.3, 4.1.1, 4.2.1, 4.4.3, 6.2.3
13.03.2015	1.2.2	BWI Systeme GmbH	Einarbeitung geänderter Sperrwege	4.4
17.03.2015	1.2.3	BWI Systeme GmbH	QS	4.4
27.10.2015	1.2.4	BWI Systeme GmbH	Einarbeitung Compliance Prozess	2.8.7, 3.1.1.2, 4.1, 4.15, 4.3.3, 4.5.1, 6.2.3
30.10.2015	1.2.5	BWI Systeme GmbH	QS	
11.11.2015	1.2.6	BWI Systeme GmbH	QS	
24.11.2015	1.2.7	BWI Systeme GmbH	Einarbeitung QS	
04.12.2015	1.2.8	BWI Systeme GmbH	Aufnahme des HTTP-Sperrlistenverteilpunkts	2.6.4
11.12.2015	1.2.9	BWI Systeme GmbH	QS HTTPS-Sperrlistenverteilpunkt	2.6.4
04.11.2016	1.2.10	BWI Systeme GmbH	Einfügen des Zeitstempeldienstes	1.3.7, 2.6.4, 3.5, 4.6.4, 6.3.2
15.11.2016	1.2.11	BWI Systeme GmbH	QS	
19.12.2016	1.2.12	BWI Systeme GmbH	Einarbeitung Mitprüfungsbermerkungen	
15.07.2020	1.2.12.3	BWI GmbH	Redaktionelle Änderungen	1.4.2, 2.8.1, 2.8.2

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1. Einleitung

1.1. Überblick

Die Bundeswehr betreibt im Rahmen der Public Key Infrastructure der Bundeswehr (im Folgenden kurz PKIBw, genannt) eine Zertifizierungsinfrastruktur für die Verwendung im Bereich der Verwaltung (PKIBw, Anteil Verwaltungs-PKI).

Durch die Nutzung der PKIBw, Anteil Verwaltungs-PKI, werden die Sicherheitsziele Integrität, Vertraulichkeit, Authentizität und Nichtabstreitbarkeit erreicht. Zu diesem Zweck werden asymmetrische kryptographische Verfahren eingesetzt. Die Erstellung der dafür notwendigen Schlüssel, die Identifizierung der Benutzer, die Zuordnung der Schlüssel zu Benutzern und die Bereitstellung von Informationen über die Gültigkeit dieser Zuordnung gehören zu den grundlegenden Aufgaben der PKIBw.

Die PKIBw, Anteil Verwaltungs-PKI, betreibt eine einzige Zertifizierungsstelle; sie wird als „Bundeswehr Certification Authority“ (im Folgenden „BundeswehrCA“) bezeichnet.

Dieses Dokument ist die Zertifizierungsrichtlinie der BundeswehrCA. Es beschreibt die grundlegenden Abläufe und Regelungen zur Zertifikatserstellung und –verwaltung. Es ist daher wesentliches Dokument für Regelungen im Innenverhältnis (zwischen der BundeswehrCA (siehe Abs. 1.3.2) und den Teilnehmern) und im Außenverhältnis (zur Wurzelzertifizierungsinstanz der PKI-1-Verwaltung und zu externen Nutzern der PKIBw).

Die konkrete Umsetzung der in diesem Dokument beschriebenen Regelungen durch die BundeswehrCA wird in folgenden Dokumenten (nachfolgend Betriebsdokumente genannt) festgeschrieben:

- Organisationshandbuch für die Public Key Infrastructure der Bundeswehr (PKIBw), Anteil Verwaltungs-PKI [OrgHdb] (im Folgenden kurz „Organisationshandbuch“ genannt)
- Rollenkonzept für die Public Key Infrastructure der Bundeswehr (PKIBw) [Rollen] (im Folgenden kurz „Rollenkonzept“ genannt)
- Namenskonzept und Zertifikatsprofil für die Public Key Infrastructure der Bundeswehr (PKIBw) [Namen] (im Folgenden kurz „Namenskonzept“ genannt)
- Projektbezogenes IT-Sicherheitskonzept für die Public Key Infrastructure der Bundeswehr (PKIBw) [IT-SichhK] (im Folgenden „projektbezogenes IT-Sicherheitskonzept PKIBw“ genannt)

Sollten zwischen dieser Zertifizierungsrichtlinie und den vorstehenden Dokumenten Inkonsistenzen zu finden sein, haben die Bestimmungen dieser Zertifizierungsrichtlinie Vorrang.

Die Gliederung dieses Dokuments entspricht weitgehend dem Vorschlag des RFC 2527 [RFC2527] der Internet Engineering Task Force (IETF).

1.2. Dokumentidentifikation

Das Dokument trägt den Titel „Zertifizierungsrichtlinie der Public Key Infrastructure der Bundeswehr (PKIBw), Anteil Verwaltungs-PKI". Es gilt in der vorliegenden Version bis zur Herausgabe einer neuen Version oder bis zum Widerruf. Die Zertifizierungsrichtlinie wird von der PKI Management Authority der Bw (PMABw) herausgegeben.

Die BundeswehrCA trägt in den ausgestellten Zertifikaten eine Referenz auf diese Zertifizierungsrichtlinie ein. Dabei ist neben der eindeutigen Kennung dieser Zertifizierungsrichtlinie (Object Identifier - OID) auch die Webseite einzutragen, auf der diese Zertifizierungsrichtlinie im Internet öffentlich zugänglich hinterlegt ist.

Zusätzlich wird eine vom Schlüsselspeicher abhängige OID eingetragen, die vom BSI in der Zertifizierungsrichtlinie der Wurzelzertifizierungsstelle der Verwaltungs-PKI für die Bundeswehr festgelegt wurde.

1.3. Zertifizierungsinfrastruktur und Einsatzgebiete

1.3.1. PKI Management Authority der Bundeswehr (PMABw)

Das der PKIBw übergeordnete Gremium ist die PKI Management Authority der Bundeswehr (PMABw). Sie ist verantwortlich für die Steuerung, Einführung und Nutzung der PKIBw. Insbesondere hat sie folgende Aufgaben wahrzunehmen:

- Erstellen, Fortschreiben und Überwachen auf Einhaltung der Zertifizierungsrichtlinie der PKIBw, Anteil Verwaltungs-PKI, d.h. dieses Dokuments, sowie anderer Zertifizierungsrichtlinien, die im Rahmen der PKIBw noch erstellt werden,

- Adaptieren der PKIBw (z.B. Umsetzen neuer gesetzlicher Vorgaben, bzw. aufgrund technologischer Innovationszyklen),

- Herstellung notwendiger Vertrauensbeziehungen zwischen der PKIBw und ihren Nutzern,

- Zulassung von PKI-Produkten und Aufnahme in den IT-Standard Bw,

- Definition von Vorgaben für die Bw-interne und Bw-externe Interoperabilität in Zusammenarbeit mit nationalen und internationalen PKIs; diese Vorgaben sind für die PKIBw und für alle Vorhaben / Projekte der Bw mit verbindlich, in denen asymmetrische Schlüssel eingesetzt werden; Ausnahmen bedürfen der Genehmigung der PMABw,

- Treffen und Beenden von Vereinbarungen (z.B. Vertrauensbeziehungen) mit Bw-externen PKIs,

- Entwicklung und Genehmigung der Verfahren, Kontrollen und des Meldewesens für das Management der PKIBw,

- Festlegung, wann und unter welchen Voraussetzungen eine weitere Zertifizierungsstelle Mitglied der PKIBw werden kann bzw. wieder abgetrennt wird,

- Koordination aller Aspekte der Zusammenarbeit der PKIBw mit externen Stellen.

1.3.2. Zertifizierungsstelle

Die BundeswehrCA verwendet einen oder mehrere private Signaturschlüssel zum Erstellen von Signaturen für Zertifikate und Sperrlisten. Die korrespondierenden öffentlichen Prüfschlüssel werden von der Wurzelzertifizierungsstelle der Verwaltungs-PKI zertifiziert.

Für die Teilnahme an der Verwaltungs-PKI wird zwischen dem Bundesminister des Inneren, vertreten durch den Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik, und dem Bundesminister der Verteidigung, vertreten durch die Leitung der PKI Management Authority der Bundeswehr, derzeit wahrgenommen durch BMVg CIT II 2, eine Vereinbarung geschlossen.

Die öffentlichen Prüfschlüssel der BundeswehrCA werden auf Antrag von der Wurzelzertifizierungsstelle der Verwaltungs-PKI zertifiziert. Der Antrag auf Erteilung eines CA-Zertifikates zur Teilnahme an der Verwaltungs-PKI wird vom Leiter des TrustCenterBw als rechtlichem Vertreter der BundeswehrCA gestellt. Er bestätigt auch den Erhalt und die Akzeptanz des von der Wurzelzertifizierungsstelle ausgestellten CA-Zertifikates.

Die BundeswehrCA erhält von der PMABw und von der Wurzelzertifizierungsinstanz der Verwaltung das Recht, Zertifikate zu erstellen, zu signieren, herauszugeben und zu sperren. Die BundeswehrCA ist für alle Aspekte der Ausgabe und Verwaltung von Zertifikaten verantwortlich, einschließlich der Kontrolle von Registrierung, Identifikation, Rechtevergabe, Zertifikatserstellung, Veröffentlichung und Sperrung von Zertifikaten.

Es wird eine Referenzanlage betrieben, die die BundeswehrCA und das Card Management System umfasst. Die Referenzanlage übernimmt im Notfall die Sperrung von Zertifikaten, die Funktion der Sperrlistenerstellung und –veröffentlichung sowie die Funktionalität des Card Management Systems. Die dabei einzuhaltenden Sicherheitsbestimmungen sind im projektbezogenen IT-Sicherheitskonzept PKIBw [IT-SichhK] beschreiben.

1.3.3. Registrierungsstellen

In der PKIBw, Anteil Verwaltungs-PKI, sind eine zentrale Registrierungsstelle (CRA) und mehrere lokale Registrierungsstellen (LRAs) eingerichtet.

Die zentrale Registrierungsstelle ist Bestandteil des TrustCenterBw und ist dem Leiter TrustCenterBw unterstellt. Die lokalen Registrierungsstellen sind fachlich der zentralen Registrierungsstelle unterstellt.

Die zentrale Registrierungsstelle ist eine Einheit, die übergeordnete organisatorische Aufgaben für die lokalen Registrierungsstellen und die Teilnehmer übernimmt. Dazu gehören unter anderem

- die Bereitstellung des Teilnehmer-Service,
- die Bereitstellung der Sperrhotline,

- die Bearbeitung von Anträgen zum Aufbau einer LRA,
- die Überprüfung auf Einhaltung der Vorgaben durch die LRA,
- die Organisation von Schulungen für Mitarbeiter der LRA und
- die Verwaltung der Zugriffsrechte für das Card Management System (CMS) der PKIBw.

Die zentrale Registrierungsstelle übernimmt neben den o. g. übergeordneten Aufgaben auch die Bearbeitung der Zertifizierungsanträge für organisatorische Einheiten (OrgEinheiten) und technische Komponenten. Sie arbeitet gemäß dem Organisationshandbuch [OrgHdb], das von der PMABw genehmigt wurde und dessen Einhaltung von der BundeswehrCA überwacht wird.

Die lokalen Registrierungsstellen führen die Identitätsprüfung durch und übergeben die Schlüsselträger an die Teilnehmer. Die zentrale Registrierungsstelle veranlasst nach dem Erhalt einer Empfangsbestätigung, dass der elektronische PIN/PUK-Brief zum Download im CMS bereitgestellt wird bzw. der PIN/PUK-Brief im Ausnahmefall an den Teilnehmer versendet wird.

Die lokalen Registrierungsstellen werden grundsätzlich bei den personalbearbeitenden Stellen eingerichtet.

1.3.4. Teilnehmer

Unter Teilnehmern sind die Zertifikatsinhaber zu verstehen, die nach dieser Zertifizierungsrichtlinie ausgestellte Zertifikate von der BundeswehrCA erhalten.

Andere Personen, die diese Zertifikate nutzen und damit den Angaben in den Zertifikaten implizit vertrauen, werden als Zertifikatsnutzer bezeichnet.

Zertifikatsinhaber, für die Schlüssel nach dieser Zertifizierungsrichtlinie zertifiziert werden, können sein:

- Soldatinnen und Soldaten der Bundeswehr
- Zivile Mitarbeiterinnen und Mitarbeiter der Bundeswehr
- Technische Komponenten innerhalb der Kommunikationsinfrastruktur der Bundeswehr
- Organisatorische Einheiten (OrgEinheiten)
- Verschiedene Funktionen und Bereiche der Bundeswehr
- Auf Antrag für spezielle Zwecke Mitarbeiter externer Unternehmen. Die Zertifikate sind, nachdem der Auftraggeber (z.B. BAAINBw) der Zertifikatserstellung grundsätzlich zugestimmt hat, bei den Registrierungsstellen zu beantragen.

OrgEinheiten können Organisationsbriefkästen sein, die dazu dienen, Einheiten oder Dienststellen zu adressieren, es werden aber auch spezielle Funktionen oder Rollen, wie z. B. IT-

Sicherheitsbeauftragte (IT-SiBe), damit bezeichnet. Des Weiteren können Zertifikate für Funktionen bzw. Funktionsbereiche beantragt werden, wie z.B. Schulungsmaßnahmen (Schüler1, Schüler2, usw.), Konvois, Notfallbetrieb oder wachhabender Offizier.

Gemäß der vorstehenden Definition der Teilnehmer werden im Folgenden vier Teilnehmergruppen unterschieden:

- Natürliche Personen (inkl. Pseudonyme für natürliche Personen)
- OrgEinheiten
- Technische Komponenten
- Funktionen bzw. Funktionsbereiche.

Die öffentlichen Schlüssel aller Zertifikatsinhaber der PKIBw, Anteil Verwaltungs-PKI, werden nach dieser Zertifizierungsrichtlinie zertifiziert. Die Einrichtung weiterer Zertifizierungsstellen außerhalb der Hierarchie der PKIBw, Anteil Verwaltungs-PKI, die nicht dieser Zertifizierungsrichtlinie unterliegen, bleibt von dieser Regelung unberührt.

Für die Teilnehmergruppe „natürliche Personen“ werden die Zertifikate und Schlüssel auf Chipkarten gespeichert. Dabei wird zwischen den folgenden Ausprägungen unterschieden:

- **PKIBw-Karte**: „weiße“ Karte für eine Person (Bw-Angehöriger oder Externer), die vom TrustCenterBw mit PKIBw Logo, Name und Kartennummer bedruckt wird und einen Krypto-Chip enthält, auf dem Personen-Zertifikate und kryptographische Schlüssel der PKIBw gespeichert sind.
- **eDA / eTA**: Karte, die von der Bundesdruckerei optisch als Dienstausweis bzw. Truppenausweis für einen berechtigten Bw Angehörigen personalisiert und vom TrustCenterBw elektronisch personalisiert wird. Der eDA / eTA enthält ebenfalls einen Krypto-Chip, auf dem Personen-Zertifikate und kryptographische Schlüssel der PKIBw gespeichert sind.
- **Temporäre PKI-Karte:** Karte für eine Person, die bei Bedarf (z.B. Verlust / Defekt einer PKIBw-Karte oder eines eDA / eTA) in einer LRA dezentral elektronisch personalisiert und direkt an die Person ausgegeben wird. Temporäre PKI-Karten werden als Kartenrohlinge zentral im TrustCenterBw initialisiert sowie mit PKIBw Logo und Kartennummer bedruckt, bevor sie an eine LRA versendet werden. Die Personen-Zertifikate zu temporären PKI-Karten besitzen eine begrenzte Gültigkeit von einigen Wochen.
- **Funktionsbezogene Karte**: Karte für verschiedene Funktionen bzw. Funktionsbereiche, die analog zu den PKIBw-Karten zentral im TrustCenterBw erstellt werden. Funktionsbezogene Chipkarten werden analog zu Schlüsseldateien von einem Schlüsselverantwortlichen beantragt.

Im Folgenden wird generell von Chipkarten gesprochen. Aufgrund der unterschiedlichen Beantragungs- und Personalisierungsprozesse wird bei Bedarf eine Unterscheidung nach dem jeweiligen Chipkartentyp vorgenommen. Gleiches gilt für die zugehörigen Personen-Zertifikate und Zertifikate für Funktionen.

1.3.5. Einsatzgebiete

Die BundeswehrCA stellt Zertifikate für öffentliche Schlüssel im Bereich IT-BasisschutzBw und erweiterter IT-BasisschutzBw für folgende Aufgaben und Inhaber aus:

Aufgabe	Zertifikatsinhaber		
	Personen / Funktionen	**OrgEinheiten**	**Technische Komponenten**
Sicherstellung der Identität, Authentifizierung des Teilnehmers	x	x	x
Sicherstellung der Integrität und Authentizität von Informationen oder Nachrichten	x	-	x
Sicherstellung der Verbindlichkeit von Informationen oder Nachrichten	x	-	x
Sicherstellung der Vertraulichkeit von Informationen oder Kommunikationsverbindungen	x	x	x
Sicherstellung der Integrität und Authentizität von Programmen	-	x	-

Tabelle 1: Anwendbarkeit der Zertifikate

Die BundeswehrCA gibt grundsätzlich getrennte Schlüssel und Zertifikate für jede Aufgabe aus. Eine Zusammenfassung mehrerer Aufgaben ist bei technischer Notwendigkeit zulässig.

Einzelheiten zum Zertifikatsprofil, den in den Zertifikatserweiterungen „keyUsage“ und „extendedKeyUsage“ eingetragenen Verwendungszwecken sowie weiteren anwendungsspezifischen Einträgen in den Zertifikaten sind im Namenskonzept [Namen] beschrieben.

Die von der PKIBw, Anteil Verwaltungs-PKI, ausgegebenen Schlüssel und dazugehörige Zertifikate dürfen für die Verschlüsselung von Informationen in den Schutzbereichen:

- IT-BasisschutzBw[1] und
- Personenbezogene Daten des Schutzbereiches 3 (Erweiterter IT-BasisschutzBw)[2]

verwendet werden.

[1] Setzt die Zulassung der die Zertifikate der PKIBw nutzenden Anwendung für VS-NfD durch BMVg M II IT 3 bzw. durch das BSI voraus; der Einsatz für NATO RESTRICTED setzt die Zulassung der entsprechenden Anwendung durch das BSI voraus.

[2] Setzt die Zulassung der die Zertifikate der PKIBw nutzenden Anwendung für PersDat Schutzbereich 3 durch BMVg M II IT 3 voraus.

Für die Verschlüsselung von Verschlusssachen aus höheren Schutzbereichen ist es erforderlich, dass die Vorhaben / Projekte Produkte einsetzen, die für die jeweilige VS-Einstufung der Daten durch das BSI zugelassen sind.

Die von der PKIBw, Anteil Verwaltungs-PKI, ausgegebenen Schlüssel und dazugehörige Zertifikate dürfen für die elektronische Signatur von Informationen aller Kategorien und Schutzbereiche verwendet werden.

1.3.6. Zertifizierungsstellenhierarchie

Die BundeswehrCA ist eine nachgeordnete Zertifizierungsstelle der PKI der Verwaltung (PKI-1-Verwaltung).

Einen Überblick über den hierarchischen Aufbau der PKIBw und ihrer Einbindung in das nationale und internationale Umfeld gibt die folgende Abbildung.

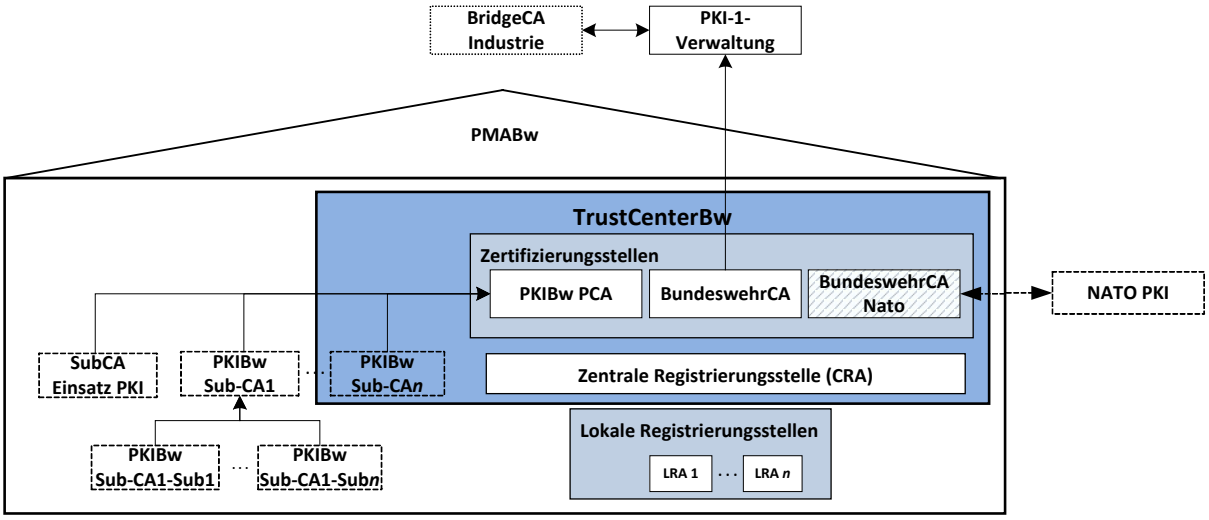

Abbildung 1: Beziehungen im nationalen und internationalen Umfeld

1.3.7. Zeitstempeldienst

Die PKIBw betreibt einen Zeitstempeldienst. Der Zeitstempeldienst liefert auf Anfrage einen signierten Zeitstempel zurück. Der Zeitstempel wird mit einem Zertifikat signiert, dass von der aktuell aktiven CA der Verwaltungs-PKIBw ausgestellt wurde. Mit den verwendeten Zertifikaten können Signaturen auf fortgeschrittenem Niveau erstellt werden. Der Zeitstempeldienst erstellt daher auch unter Berücksichtigung der eIDAS-Verordnung[1] fortgeschrittene Zeitstempel.

[1] Siehe Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, kurz auch als eIDAS-Verordnung bezeichnet

1.4. Ansprechpartner und Kontaktstellen

In diesem Abschnitt werden Ansprechpartner und Kontaktstellen genannt, die bei Fragen zum vorliegenden Dokument und dessen Auslegung kontaktiert werden können. Änderungsvorschläge sind über das in Kapitel 8 beschriebene Verfahren einzureichen.

1.4.1. Organisation zur Verwaltung dieses Dokuments

Die Zertifizierungsrichtlinie der BundeswehrCA wird von der PKI Management Authority der Bundeswehr (PMABw) genehmigt und herausgegeben. Die Aufgaben der PMABw werden durch BMVg CIT II 2 wahrgenommen.

1.4.2. Kontaktpersonen

Ansprechstelle der Zertifizierungsstelle:

TrustCenterBw
Zentrum für Cyber-Sicherheit der Bundeswehr
Abt Schutz und Prävention Dez TrustCenter PKIBw
Kommerner Straße 188
53879 Euskirchen

Tel.: 02251-953-2900
(Bw-Netz: 90-3461-2900)
Fax: 02251-953-2919
(Bw-Netz: 90-3461-2919)
E-Mail: PKIBwLeitung@bundeswehr.org

1.4.3. Verantwortlicher für die Prüfung der Eignung eines CPS

Ein Certification Practice Statement (CPS) enthält detaillierte Angaben über die Arbeitsabläufe bei der Registrierung und Zertifizierung eines Teilnehmers. In der PKIBw, Anteil Verwaltungs-PKI, werden solche Angaben im Dokument Organisationshandbuch [OrgHdb] aufgeführt. Ein zusätzliches CPS wird nicht erstellt.

Die PMABw prüft vor Erteilung der Genehmigung zur Inbetriebnahme der BundeswehrCA und der zentralen Registrierungsstelle, ob die in diesen Dokumenten, dem Sicherheitskonzept der Zertifizierungsstelle und der vorliegenden Zertifizierungsrichtlinie enthalten Vorgaben von der Zertifizierungsstelle und der zentralen Registrierungsstelle eingehalten werden.

2. Generelle Bestimmungen

2.1. Verpflichtungen

2.1.1. Verpflichtungen der Zertifizierungsstelle

Die BundeswehrCA verpflichtet sich zur Einhaltung der Vorgaben dieser Zertifizierungsrichtlinie und der Betriebsdokumente:

- Organisationshandbuch [OrgHdb]
- Rollenkonzept [Rollen]
- Namenskonzept [Namen]
- Projektbezogenes IT-Sicherheitskonzept PKIBw [IT-SichhK]

Insbesondere verpflichtet sie sich

- zur Einhaltung der in den Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung enthaltenen Vorgaben für eine Zertifizierungsstelle gemäß [BSIPolicy],
- zur Einhaltung der in der Selbsterklärung der Zertifizierungsstelle [BSIAnl1] vorgenommenen Zusagen,
- zur Erstellung, Einhaltung und Fortschreibung des projektbezogenen IT-Sicherheitskonzepts PKIBw [IT-SichhK],
- zum angemessenen Schutz aller privaten CA-Schlüssel durch organisatorische, personelle, infrastrukturelle und technische Maßnahmen gemäß [IT-SichhK], Abschnitt 7.1. „Maßnahmenbeschreibung spezifische Maßnahmen“.
- zur Veröffentlichung von Sperrlisten im zentralen Verzeichnisdienst der Bw gemäß Abschnitt 2.6.1 und
- zur Bereitstellung und Durchführung der in dieser Zertifizierungsrichtlinie definierten Prozesse und Dienstleistungen gemäß Abschnitt 4 „Betriebliche Abläufe“.

2.1.2. Verpflichtungen der Registrierungsstellen

Alle Registrierungsstellen der PKIBw, Anteil Verwaltungs-PKI, verpflichten sich zur Einhaltung der Vorgaben dieser Zertifizierungsrichtlinie und der Betriebsdokumente:

- Organisationshandbuch [OrgHdb]
- Projektbezogenes IT-Sicherheitskonzept PKIBw [IT-SichhK]

Insbesondere verpflichten sie sich

- bei der Registrierung die im Organisationshandbuch definierten Verfahrensanweisungen einzuhalten,
- die sichere Übergabe der Schlüsselmittelträger gemäß Abschnitt 4.3 “Übergabe von Zertifikaten“ zu gewährleisten und
- zur Belehrung der Teilnehmer gemäß Abschnitt 4.3 “Übergabe von Zertifikaten“.

2.1.3. Verpflichtungen der Zertifikatsinhaber

Die Zertifikatsinhaber verpflichten sich, die Richtlinien dieser Zertifizierungsrichtlinie einzuhalten.

Insbesondere verpflichten sie sich

- bei der Registrierung korrekte Angaben zu machen,
- bei der Registrierung mitzuwirken und benötigte Informationen zur Verfügung zu stellen,
- den Schlüsselträger mit den Schlüsseln für andere Personen unzugänglich aufzubewahren; Ausnahme: der Schlüsselverantwortliche für Funktionen darf diese den Nutzern der funktionsbezogenen Chipkarten nach Verpflichtung aushändigen,
- PIN und PUK bzw. Passwörter geheim zu halten; Ausnahme: der Schlüsselverantwortliche für Funktionen darf die PIN dem jeweiligen Nutzer der funktionsbezogenen Chipkarte nach Verpflichtung mitteilen,
- ihre Zertifikate auf einem der in Abschnitt 4.4.3 genannten Wege umgehend sperren zu lassen, wenn
  - ein Verdacht auf Kompromittierung des privaten Schlüssels besteht oder
  - Informationen im Zertifikat nicht mehr korrekt sind,
- temporäre PKI-Karten in der ausgebenden LRA zurückzugeben, wenn die begrenzt gültigen Zertifikate abgelaufen sind bzw. die temporäre PKI-Karte nicht mehr benötigt wird.

2.1.4. Empfehlungen für Zertifikatsnutzer

Den Zertifikatsnutzern wird empfohlen

- sich über diese Zertifizierungsrichtlinien zu informieren; dafür stehen ihnen diese Zertifizierungsrichtlinie und der PKIBw Nutzerleitfaden für Chipkarten [NutzerLF] zur Verfügung,
- Zertifikate nur für die gemäß dieser Zertifizierungsrichtlinie zulässigen Zwecke einzusetzen,

- die Gültigkeit von Zertifikaten und elektronischen Signaturen zu prüfen, insbesondere, ob das verwendete Zertifikat zwischenzeitlich widerrufen wurde und

- beim Einsatz automatisierter Verfahren zur Prüfung von Signaturen und Zertifikaten Systeme einzusetzen, die einen Prüfbericht erzeugen, und diesen zu kontrollieren.

Empfehlungen / Hinweise zur Nutzung der Zertifikate werden auf den Webseiten der PKIBw im IntraNetBw veröffentlicht.

2.1.5. Anforderungen an den Verzeichnisdienst

Der zentrale Verzeichnisdienst der Bw bestätigt im Rahmen der Mitzeichnung, die Richtlinien dieser Zertifizierungsrichtlinie bzgl. der Verfügbarkeit von Zertifikaten und Sperrlisten sowie bzgl. der Ausfallzeiten einzuhalten.

An die Zertifikate und Sperrlisten wird die Verfügbarkeitsanforderung „mittel“ gestellt. Die Verfügbarkeitsanforderung „mittel“ bedeutet:
Verfügbarkeit: min. 99% (entspricht ca. 87 Stunden Ausfall pro Jahr)

Dauer einer Störung: max. 1 Tag

2.2. Haftung

2.2.1. Haftung der Zertifizierungsstelle

Es gelten die allgemeinen Haftungsregelungen des Bundes.

2.2.2. Haftung der Registrierungsstelle

Es gelten die allgemeinen Haftungsregelungen des Bundes.

2.3. Finanzielle Verantwortung

Keine Regelungen.

2.3.1. Schadensersatz der beteiligten Parteien

Es gelten die allgemeinen Haftungsregelungen des Bundes.

2.3.2. Finanzielle Beziehungen

Keine Regelungen.

2.3.3. Verwaltung der Geschäftsbeziehungen

Keine Regelungen.

2.4. Auslegung und (gerichtliche) Durchsetzung (Vollzug)

2.4.1. Zugrunde liegende Gesetzesbestimmungen

Die BundeswehrCA stellt für Personen Zertifikate aus, mit denen sie fortgeschrittene Signaturen gemäß deutschem Signaturgesetz [SigG] erzeugen können, ist jedoch kein angezeigter oder akkreditierter Zertifizierungsdiensteanbieter.

Es gelten die allgemeinen gesetzlichen Bestimmungen.

Anmerkung: Signaturen von OrgEinheiten, technischen Komponenten und Funktionen bzw. Funktionsbereichen, sowie Verschlüsselungszertifikate sind vom SigG nicht abgedeckt.

2.4.2. Zugrunde liegende Erlasslage

Keine Regelungen.

2.4.3. Trennbarkeit der Bestimmungen, Fortbestehen von Ansprüchen, Vereinigung (Fusion), Kündigung von Verträgen

Keine Regelungen.

2.4.4. Schlichtungsverfahren

Keine Regelungen.

2.5. Gebühren

Es werden keine Gebühren erhoben.

2.6. Bereitstellung / Veröffentlichung von Informationen

2.6.1. Veröffentlichung von Informationen der Zertifizierungsstelle

Bekanntmachung von Dokumenten

Von der BundeswehrCA werden folgende Dokumente veröffentlicht:

- Zertifizierungsrichtlinie der BundeswehrCA (dieses Dokument),
- Organisationshandbuch [OrgHdb],
- Namenskonzept [Namen],
- PKIBw Nutzerleitfaden für Chipkarten [NutzerLF] und
- die Anschrift der zentralen Registrierungsstelle und eine Liste aller lokalen Registrierungsstellen mit Anschrift.

Die Veröffentlichung der Dokumente erfolgt in elektronischer Form auf der Webseite der PKIBw, die über das Portal (siehe Abschnitt 2.6.4) zu erreichen ist.

Kommunikation mit Teilnehmern

Die Zertifikatsinhaber und -nutzer werden informiert bei

- einem Wechsel eines Wurzelinstanzschlüssels oder eines CA-Schlüssels,
- der Sperrung eines Wurzelinstanzschlüssels oder eines CA-Schlüssels,
- der Kompromittierung oder Verdacht auf Kompromittierung eines Wurzelinstanzschlüssels oder eines CA-Schlüssels,
- sicherheitsrelevanten Änderungen dieser Zertifizierungsrichtlinie und
- der Einstellung der Tätigkeit einer Registrierungsstelle.

Diese Informationen werden auf der Webseite der PKIBw veröffentlicht. Zusätzlich erfolgt bei Sperrungen (Wurzelinstanz oder CA) sowie bei sicherheitsrelevanten Änderungen eine direkte Benachrichtigung der Zertifikatsinhaber per E-Mail. Eine Verteilerliste mit den E-Mail-Adressen aller Zertifikatsinhaber wird durch das Card Management System der zentralen Registrierungsstelle bereitgestellt.

Bereitstellung von Zertifikaten und Sperrinformationen

Die BundeswehrCA veröffentlicht folgende Zertifikate und Sperrlisten:

- ihre Signaturzertifikate,
- alle von ihr ausgestellten Sperrlisten und
- Verschlüsselungszertifikate der Teilnehmer.

Die Veröffentlichung von anderen Zertifikaten erfolgt bei Bedarf.

Die Sperrlisten werden über den zentralen Verzeichnisdienst der Bw (siehe Abschnitt 2.6.4) zum Abruf bereitgehalten. Weitere Möglichkeiten zum Erhalt von Sperrinformationen sind in den Abschnitten 4.4.11 und 4.4.13 beschrieben.

2.6.2. Häufigkeit der Aktualisierung

Die Sperrlisten werden entsprechend den Richtlinien aus Abschnitt 4.4.9 aktualisiert.

2.6.3. Zugriffsregelung

Alle unter dieser Zertifizierungsrichtlinie veröffentlichten Zertifikate und Sperrlisten sind innerhalb der Kommunikationsinfrastruktur der Bundeswehr abrufbar. Die in Abschnitt 2.6.1 aufgeführten Dokumente sind über die Webseite der PKIBw im IntraNetBw ebenfalls frei abrufbar.

Außerhalb der Kommunikationsinfrastruktur der Bw sind die Zertifizierungsrichtlinie der BundeswehrCA (dieses Dokument) sowie die Selbsterklärung über das Internet frei abrufbar. Zusätzlich sind die Sperrlisten über einen Verzeichnisdienst frei über das Internet abrufbar.

Der zentrale Verzeichnisdienst der Bw stellt sicher, dass die Änderung der vorstehend genannten Informationen nur durch die für diese Informationen zuständigen Stellen erfolgen kann.

2.6.4. Adressen von Verzeichnisdienst und Webseiten

Die BundeswehrCA veröffentlicht Sperrlisten und ggf. Zertifikate in den zentralen Verzeichnisdienst der Bw, der durch die Zentralen Dienste zur Verfügung gestellt wird. Zusätzlich werden Statusinformationen zu Zertifikaten über einen OCSP-Dienst abrufbar gehalten. Diese Informationen können über folgende Adressen und Mechanismen abgerufen werden:

Verzeichnisdienst:

a) Abrufen von Sperrlisten und CA-Zertifikaten (im IntraNetBw und von extern):

Adresse:	ldap.bundeswehr.org
Port:	389
Zugriffsprotokoll:	LDAP v3
Suchbasis:	ou=Bundeswehr, o=PKI-1-Verwaltung, c=DE

b) Abrufen von Teilnehmer-Zertifikaten (nur im IntraNetBw):

Adresse:	ldap.bundeswehr.org
Port:	389
Zugriffsprotokoll:	LDAP v3
Suchbasis:	ou=bmvg, o=bund, c=DE

c) Abrufen von Zeitstempeln mit Signatur

Adresse:	TSS.pkibw.bundeswehr.org
Port:	80
Zugriffsprotokoll:	HTTP

d) Online Statusabfrage (OCSP) (im IntraNetBw und von extern):

Adresse:	http://ocsp-v.bundeswehr.org/ocsp
Port:	80

Zugriffsprotokoll: HTTP

e) Abrufen von Sperrlisten per HTTP (im IntraNetBw und von extern):

Adresse: http://crl.bundeswehr.org/

Pfad: CN der CA mit Leerzeichen ersetzt durch Unterstriche + „.crl“

Port: 80

Zugriffsprotokoll: HTTP

Diese Zertifizierungsrichtlinie sowie weitere allgemeine Informationen können über folgende Webseiten abgerufen werden:

Bundeswehr intern (IntraNetBw): pkibw.bundeswehr.org (oder über das Portal von IntraNetBw – Homepage PKIBw)

Bundeswehr extern (Internet): pkibw.bundeswehr.org

2.7. Konformitätsprüfungen (Audits)

In internen Konformitätsprüfungen (im Folgenden Audits genannt) wird überprüft, ob die Zertifizierungsrichtlinie und das projektbezogene IT-Sicherheitskonzept PKIBw [IT-SichhK] von der BundeswehrCA und der zentralen Registrierungsstelle eingehalten werden und die Abläufe gemäß den Betriebsdokumenten umgesetzt sind.

2.7.1. Häufigkeit der Prüfung

Das erste Audit findet vor Genehmigung der Inbetriebnahme des TrustCenterBw statt.

Weitere Audits erfolgen bei sicherheitsrelevanten Änderungen in Abläufen oder Ausstattungen, mindestens jedoch einmal im Jahr analog den Grundsätzen für IT-Sicherheitsinspektionen von Dienststellen gemäß ZDV 54/100, Ziffer 137ff.

Ein Audit kann von folgenden Instanzen veranlasst bzw. beauftragt werden:

- der PMABw,
- dem IT-SiBe Projekt,
- dem Leiter TrustCenterBw und
- dem Leiter der zentralen Registrierungsstelle (nur für die zentrale Registrierungsstelle).

Einzelheiten sind im projektbezogenen IT-Sicherheitskonzept PKIBw [IT-SichhK] zu beschreiben.

2.7.2. Identität und Anforderungen des Prüfers

Der Prüfer (Auditor) ist ein unabhängiger Dritter, der über ausreichendes Fachwissen und Qualifikationen verfügt. Audits können von

- dem IT-Sicherheitsbeauftragten der Bw,
- einem externen Dienstleister mit entsprechender Erfahrung oder
- anderen Personen, die damit beauftragt werden,

durchgeführt werden.

2.7.3. Beziehungen zwischen Prüfer und zu untersuchender Partei

Das Audit wird von einer unabhängigen Drittinstanz vorgenommen. Insbesondere darf der Auditor nicht Mitarbeiter der überprüften Instanz sein.

2.7.4. Aspekte der Prüfung

In dem Audit können folgende Aspekte betrachtet werden:

- Die Umsetzung der Zertifizierungsrichtlinie der BundeswehrCA,
- Die Umsetzung des projektbezogenen IT-Sicherheitskonzepts PKIBw [IT-SichhK],
- Die Umsetzung der Abläufe gemäß den Betriebsdokumenten.

Die Ergebnisse werden beschrieben und erkannte Schwachstellen dokumentiert.

Die Ergebnisse werden

- der Instanz, die das Audit veranlasst hat,
- der PMABw,
- dem Leiter TrustCenterBw,
- dem IT-SiBe Projekt

bekannt gegeben.

2.7.5. Einzuleitende Handlungen nach unzureichendem Ergebnis

Bei gefundenen Mängeln muss eine Nachbesserung durch die Stelle, die das Audit veranlasst hat, gefordert und eine angemessene Frist zur Beseitigung gesetzt werden. Der Leiter der

auditierten Instanz hat Maßnahmen zur Beseitigung der Mängel einzuleiten und diese zu dokumentieren.

Der Auditor kann der PMABw empfehlen, den Betrieb der BundeswehrCA oder der zentralen Registrierungsstelle bis zur Beseitigung der Mängel einstellen zu lassen.

2.8. Vertraulichkeit

2.8.1. Vertraulich eingestufte Informationen

In der PKIBw, Anteil Verwaltungs-PKI, werden Daten erhoben und verarbeitet, die sowohl unter Aspekten der Sicherheit als auch unter Aspekten des Datenschutzes eine besondere Absicherung erfordern.

Diese Daten und ihre Einstufung sind in Tabelle 2 aufgeführt. Im projektbezogenen IT-Sicherheitskonzept PKIBw [IT-SichhK] sind die Einstufungen der Daten näher erläutert.

Daten	Kategorie und Schutzbereich
Antragsdaten: Persönliche Daten der Antragsteller, die nicht im Zertifikat eingetragen werden (z.B. dienstliche Anschrift, Ausweisnummer des Identifizierungsdokumentes).	PersDat Schutzbereich 2
Interne Daten des TrustCenterBw (z.B. private Schlüssel)	VS-NfD
Private Schlüssel und Aktivierungsdaten der Teilnehmer	VS-NfD
Sperrantragsdaten	PersDat Schutzbereich 1
Sperrkennwörter	OFFEN-AMTS & DIENSTGEHEIMNIS

Tabelle 2: Zuordnung vertraulicher PKI-Daten zu Schutzbereichen

Vertraulich eingestufte Daten werden ohne explizite Zustimmung der Betroffenen nicht an Dritte weitergegeben, es sei denn, die PKIBw, Anteil Verwaltungs-PKI, ist durch gesetzliche Bestimmungen dazu verpflichtet.

Die Antragsteller stimmen der internen Speicherung und Verarbeitung ihrer Antragsdaten durch die zentrale Registrierungsstelle bei der Registrierung zu. Die Antragsdaten werden in den Registrierungsstellen erhoben und im CMS gespeichert.

2.8.2. Nicht vertraulich eingestufte Informationen

Neben den in Abschnitt 2.8.1 aufgeführten Informationen, werden von der PKIBw auch Informationen verarbeitet, deren Integrität und Authentizität gewährleistet sein muss, die aber nicht vertraulich sind. Diese Informationen sind in Tabelle 3 aufgeführt.

Daten	Kategorie und Schutzbereich
Von der BundeswehrCA ausgestellte Teilnehmer-Zertifikate (Zertifizierungsdaten): Namen, ggf. Pseudonym und E-Mail-Adresse des Teilnehmers Bezeichnung und E-Mail-Adresse der OrgEinheit Bezeichnung und ggf. Netzwerkname (DNS-Name) der technischen Komponente	OFFEN-AMTS & DIENSTGEHEIMNIS (für OrgEinheiten, technische Komponenten, Funktionen bzw. Funktionsbereiche), PersDat Schutzbereich 1 (für Personen)
Von der BundeswehrCA ausgestellten Sperrlisten	OFFEN-AMTS & DIENSTGEHEIMNIS
Von der BundeswehrCA verwendete CA-Zertifikate	OFFEN-AMTS & DIENSTGEHEIMNIS

Tabelle 3: Zuordnung nicht vertraulicher PKI-Daten zu Schutzbereichen

Zum Inhalt von Sperrlisten siehe Abschnitt 2.8.3.

2.8.3. Offenlegung von Informationen über Zertifikatssperrungen

Die BundeswehrCA der PKIBw, Anteil Verwaltungs-PKI, stellt Informationen zu Zertifikatssperrungen über Sperrlisten und zusätzlich über den OCSP-Dienst zur Verfügung.

Ausgestellte Sperrlisten und OCSP-Antworten enthalten für jedes gesperrte Zertifikat

- die Seriennummer des Zertifikates und
- den Zeitpunkt der Sperrung.

2.8.4. Offenlegung an Behörden im Rahmen gesetzlicher Pflichten

Eine Weitergabe von in Abschnitt 2.8.1 genannten Informationen an Behörden erfolgt nur, wenn dies gesetzlich gefordert ist.

2.8.5. Offenlegung im Rahmen zivilrechtlicher Auskunftspflichten

Eine Weitergabe von in Abschnitt 2.8.1 genannten Informationen im Rahmen zivilrechtlicher Auskunftspflichten erfolgt nur, wenn dies gesetzlich gefordert ist.

2.8.6. Offenlegung auf Antrag des Zertifikatsinhabers

Ein Zertifikatsinhaber kann Einsicht in alle über ihn gespeicherten Informationen in elektronischer oder gedruckter Form beantragen. Sofern der Zertifikatsinhaber keine natürliche Person ist, kann der Antrag durch den Schlüsselverantwortlichen gestellt werden.

Der Antrag ist formlos, schriftlich oder elektronisch, an die ausstellende BundeswehrCA zu stellen. Elektronisch eingereichte Anträge müssen mit dem PKIBw-Signaturschlüssel des Antragstellers signiert werden.

2.8.7. Weitergabe des privaten Schlüssels an berechtigte Stellen

Berechtigte Stellen (CERTBw, CERT BWI und BWI IT Compliance Abteilung) können im Rahmen gesetzlicher Grundlagen die Wiederherstellung von privaten Schlüsseln der Nutzer beantragen. Die Wiederherstellung erfolgt ausschließlich auf nicht auslesbare Chipkarten („Compliance-Karten“), die immer von zwei unterschiedlichen besonders verpflichteten Personen (Compliance Manager) gehandhabt werden müssen.

Details regelt Abschnitt 6.2.3.

2.8.8. Weitere Gründe zur Freigabe von vertraulichen Informationen

Es liegen zurzeit keine weiteren Gründe vor.

2.9. Urheberrechte und Eigentumsrechte

Die von der PKIBw, Anteil Verwaltungs-PKI, an die Teilnehmer ausgegebenen Schlüssel und Schlüsselträger sind Eigentum der Bundeswehr, ebenso ausgestellte Zertifikate und Sperrlisten. 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 PMABw.

3. Identifizierung und Authentisierung

3.1. Erst-Registrierung

3.1.1. Namenstypen

Der Name bzw. das Pseudonym des Zertifikatsinhabers muss als *Distinguished Name* im Zertifikat in das Feld *Subject* eingetragen werden. Die Identität des Herausgebers des Zertifikates muss als *Distinguished Name* im Zertifikatsfeld *Issuer* enthalten sein.

Die Vergabe der *Distinguished Names* für Teilnehmer der PKIBw, Anteil Verwaltungs-PKI, d.h. natürliche Personen, Pseudonyme für natürliche Personen, technische Komponenten, OrgEinheiten und Funktionen bzw. Funktionsbereiche sowie Zertifizierungsstellen erfolgt nach den Vorgaben des Namenskonzeptes (vgl. [Namen]).

3.1.2. Aussagekraft von Namen

Der im Zertifikat eingetragene Name einer natürlichen Person, einer OrgEinheit oder einer Funktion bzw. Funktionsbereichs ist (zum Antragszeitpunkt) identisch mit dem im Verzeichnisdienst der Bw hinterlegten Namen dieses Teilnehmers. Entsprechendes gilt für Zertifikate, die Pseudonyme für natürliche Personen enthalten.

Pseudonyme, die anstelle des Namens einer natürlichen Person in ein Zertifikat eingetragen werden, sind entsprechend Namenskonzept (vgl. [Namen]) kenntlich gemacht.

Der im Zertifikat eingetragene Name einer technischen Komponente entspricht dem Netzwerknamen (DNS-Namen) der Komponente. Sofern ein solcher nicht existiert, muss der Antragsteller bei seiner lokalen DNS-Verwaltung einen Namen beantragen.

Neben dem Namen des Teilnehmers (siehe 3.1.4) enthält der Distinguished Name eines Zertifikates keine weiteren Angaben (wie beispielsweise den Dienstort oder die Dienststelle).

Zertifikate für natürliche Personen, OrgEinheiten und Funktionen bzw. Funktionsbereiche beinhalten zusätzlich im Feld *SubjectAltName* die E-Mail-Adresse der Person, OrgEinheit oder Funktion bzw. Funktionsbereichs, Zertifikate für technische Komponenten enthalten zusätzlich die Netzwerkadresse der Komponente.

Zur genauen Identifizierung einer Person, OrgEinheit oder Funktion bzw. Funktionsbereichs sind im Zweifelsfall weitere Informationen aus dem Verzeichnisdienst der Bw abzurufen.

3.1.3. Regeln zur Interpretation unterschiedlicher Namensformen

Keine Regelungen.

3.1.4. Eindeutigkeit der Namen

Durch den zentralen Verzeichnisdienst der Bw ist sichergestellt, dass die Namen von natürlichen Personen, OrgEinheiten und Funktionen bzw. Funktionsbereichen innerhalb des Namensraumes der PKIBw, Anteil Verwaltungs-PKI, eindeutig sind.

Die lokalen Registrierungsstellen entnehmen dem zentralen Verzeichnisdienst die benötigten Angaben und müssen prüfen, ob der Antragsteller berechtigt ist, für den ausgewählten Namen ein Zertifikat zu beantragen.

Dies beinhaltet insbesondere die Überprüfung, dass nicht verschiedene Personen oder Schlüsselverantwortliche Zertifikate auf den gleichen Namen beantragen.

Ein Zertifikatsinhaber kann jedoch gleichzeitig mehrere Zertifikate, die auf den gleichen Namen ausgestellt sind, besitzen.

Die Eindeutigkeit der Namen von technischen Komponenten wird durch die zentrale Registrierungsstelle überprüft.

3.1.5. Anspruch auf Namen und Beilegung von Streitigkeiten

Aus der Teilnahme an der PKIBw, Anteil Verwaltungs-PKI, ergibt sich kein Anspruch auf einen bestimmten Namen.

3.1.6. Anerkennung, Bestätigung und Bedeutung von Warenzeichen

Keine Regelungen.

3.1.7. Nachweis des Besitzes des privaten Schlüssels

Die Teilnehmer der PKIBw, Anteil Verwaltungs-PKI, werden von dieser mit Schlüsseln und Zertifikaten ausgestattet. An Personen und Funktionen bzw. Funktionsbereiche werden Chipkarten ausgegeben. Bei OrgEinheiten und technischen Komponenten erhält der Schlüsselverantwortliche (siehe 4.1) den Schlüssel in elektronischer Form (Schlüsseldatei).

Alle Teilnehmer-Schlüssel werden unter Kontrolle der BundeswehrCA im Rahmen der Personalisierung erzeugt.

In Ausnahmefällen, wenn eine technische Komponente keine Schlüssel der PKIBw, Anteil Verwaltungs-PKI, einlesen, sondern die Schlüssel nur selbst erzeugen kann, muss von der Komponente ein elektronischer Zertifizierungsantrag erstellt werden. Dieser ist mit dem privaten Schlüssel der Komponente zu signieren. Die CA-Systeme sind in der Lage, einen elektronischen Zertifizierungsantrag im PKCS#10-Format [PKCS10] einzulesen.

3.1.8. Authentisierung von natürlichen Personen

Für die Authentisierung von natürlichen Personen (inklusive bei der Beantragung von Pseudonym-Zertifikaten) ist folgender Ablauf einzuhalten:

Persönliches Erscheinen der zu registrierenden Person in einer für die BundeswehrCA arbeitenden lokalen Registrierungsstelle.

Vorlage eines gültigen Ausweisdokumentes der zu registrierenden Person. Als Ausweisdokumente werden akzeptiert:

- Dienst- oder Truppenausweis,

- Bundespersonalausweis,
- Deutscher Reisepass,
- Pässe und Personalausweise der Mitgliedstaaten der Europäischen Union, der anderen Vertragsstaaten der Abkommen über den Europäischen Wirtschaftsraum, und der Schweiz, sofern sie an Angehörige des Ausstellerstaates ausgestellt worden sind,
- ausländische Pässe und Passersatzpapiere, die das Bundesministerium des Innern zur Einreise in die Bundesrepublik Deutschland anerkennt[1],
- weitere Ausweisdokumente mit Lichtbild nach Ausnahmegenehmigung durch die PMABw.

3.1.9. Authentisierung von organisatorischen Einheiten

Für die Authentisierung von organisatorischen Einheiten ist folgender Ablauf einzuhalten:

- Der Antragsteller muss im Besitz einer PKIBw-Chipkarte sein und der zentralen Registrierungsstelle vor Antragstellung schriftlich als Schlüsselverantwortlicher benannt sein.
- Der Schlüsselverantwortliche verpflichtet sich zur Einhaltung der Richtlinien für Schlüsselverantwortliche. Die Verpflichtungserklärung ist zwei Jahre gültig.
- Liegt die Benennung mit gültiger Verpflichtungserklärung vor, erhält der Schlüsselverantwortliche spezielle Rechte zur Beantragung von Zertifikaten für organisatorische Einheiten.
- Zur Beantragung von Zertifikaten für organisatorische Einheiten muss sich der Schlüsselverantwortliche mit Hilfe seiner PKIBw-Chipkarte am Card Management System authentisieren. Dabei kommt der private PKIBw-Authentisierungsschlüssel des Schlüsselverantwortlichen zum Einsatz und die Gültigkeit des zugehörigen Authentisierungszertifikates wird vom System überprüft.

3.1.10. Authentisierung bei Beantragung von technischen Komponenten

Es gelten die Regelungen aus Abschnitt 3.1.9 analog für technische Komponenten.

3.1.11. Authentisierung von Funktionen bzw. Funktionsbereichen

Für die Authentisierung von Funktionen bzw. Funktionsbereichen ist folgender Ablauf einzuhalten:

- Der Antragsteller muss im Besitz einer PKIBw-Chipkarte sein und der zentralen Registrierungsstelle vor Antragstellung schriftlich als Schlüsselverantwortlicher benannt sein.

[1] Maßgeblich ist dafür eine im Bundesanzeiger bekannt gegebene Allgemeinverfügung auf Grund §3 Abs. 1 und § 71 Abs. 6 Aufenthaltsgesetz.

- Der Schlüsselverantwortliche verpflichtet sich zur Einhaltung der Richtlinien für Schlüsselverantwortliche. Die Verpflichtungserklärung ist zwei Jahre gültig.

- Liegt die Benennung mit gültiger Verpflichtungserklärung vor, erhält der Schlüsselverantwortliche spezielle Rechte zur Beantragung von Zertifikaten für Funktionen bzw. Funktionsbereiche.

- Zur Beantragung von Zertifikaten für Funktionen bzw. Funktionsbereiche muss sich der Schlüsselverantwortliche mit Hilfe seiner PKIBw-Chipkarte am Card Management System authentisieren. Dabei kommt der private PKIBw-Authentisierungsschlüssel des Schlüsselverantwortlichen zum Einsatz und die Gültigkeit des zugehörigen Authentisierungszertifikates wird vom System überprüft.

3.1.12. Authentisierung von Compliance Managern

Für die Authentisierung von Nutzern, die das Recht haben nach Abschnitt 2.8.7 Schlüsselträger mit privaten Schlüsseln anderer Personen zu erhalten, („Compliance Manager Karte“) oder die das Recht haben, den PIN/PUK-Brief zu einer Compliance-Karte zu erhalten („Compliance Manager PIN“), ist folgender Ablauf einzuhalten:

- Der Antragsteller muss im Besitz einer PKIBw-Chipkarte sein und der zentralen Registrierungsstelle vor Antragstellung schriftlich als Compliance Manager benannt sein.

- Der Compliance Manager verpflichtet sich zur Einhaltung der Richtlinien für Compliance Manager. Die Verpflichtungserklärung ist zwei Jahre gültig.

- Liegt die Benennung mit gültiger Verpflichtungserklärung vor, erhält der Compliance Manager spezielle Rechte zur Beantragung von Compliance-Karten.

- Zur Beantragung von Compliance-Karten muss sich der Compliance Manager mit Hilfe seiner PKIBw-Chipkarte am Card Management System authentisieren. Dabei kommt der private PKIBw-Authentisierungsschlüssel des Compliance Managers zum Einsatz und die Gültigkeit des zugehörigen Authentisierungszertifikates wird vom System überprüft.

- Das TrustCenterBw stellt sicher, dass die definierten Rollenausschlüsse der Rolle Compliance Manager eingehalten werden.

3.2. Erneute Registrierung / Re-Zertifizierung

Eine Re-Zertifizierung, d. h. die erneute Zertifizierung vorhandener Schlüssel ist nicht vorgesehen. Bei Ablauf eines Zertifikates ist ein neues Zertifikat zu beantragen. Bei jeder Zertifikatserzeugung werden neue Schlüssel generiert und zertifiziert.

Einzelheiten zur Schlüsselerzeugung sind in Abschnitt 6.1.1 beschrieben.

3.3. Erneute Registrierung nach Sperrung

Eine erneute Registrierung eines Teilnehmers, dessen vorheriges Zertifikat gesperrt wurde, geschieht nach den gleichen Richtlinien wie bei einer Erst-Registrierung (siehe Abschnitt 4.1). Personen können in der nächstgelegenen LRA eine temporäre PKI-Karte beantragen, die für

eine begrenzte Dauer verwendet werden kann (z.B. bis ein neuer eDA / eTA oder eine neue PKIBw-Karte abgeholt werden kann).

Eine erneute Zertifizierung eines öffentlichen Schlüssels nach einer Sperrung ist nicht zulässig.

3.4. Antrag auf Sperrung

Die Authentisierung bei einer Sperrung erfolgt gemäß Abschnitt 4.4.2.

3.5. Verwendung des Zeitstempeldienstes

Der Zeitstempeldienst liefert zu gelieferten Hash-Werten eine Signatur mit Zeitstempel zurück.

4. Betriebliche Abläufe

4.1. Antrag auf Zertifikate

Unter dieser Zertifizierungsrichtlinie werden Zertifikate für Personen, Funktionen, technische Komponenten und OrgEinheiten ausgestellt. Außerdem werden, wie in Kapitel 2.8.7 beschrieben, die privaten Schlüssel einer Person für eine berechtigte Stelle wiederhergestellt. Die genauen Abläufe bei der Registrierung sind im PKIBw Organisationshandbuch [OrgHdb] beschrieben.

4.1.1. Zertifikate für Personen

Jeder Teilnehmer, der ein Zertifikat erhalten soll, hat einen Antrag bei einer lokalen Registrierungsstelle zu stellen.

PKIBw-Karte und eDA / eTA:

Für jede beantragte Chipkarte (mit zugehörigen Personen-Zertifikaten) ist durch den Antragsteller und die lokale Registrierungsstelle der folgende Ablauf einzuhalten:

- Der Antragsteller muss sich gemäß 3.1.8 identifizieren und authentisieren.
- Persönliche Informationen über den Teilnehmer, die im Zertifikat eingetragen werden und zur Abwicklung des Geschäftsvorfalles notwendig sind, werden dem zentralen Verzeichnisdienst der Bw entnommen und auf dem Antrag eingetragen. Der Teilnehmer hat diese Daten auf Korrektheit zu prüfen und bestätigt dies mit seiner Unterschrift.
- Die Zertifizierungs- und Antragsdaten (siehe Abschnitt 2.8) werden durch den Mitarbeiter der lokalen Registrierungsstelle im CMS bestätigt. Das Original des PKIBw-Antrages wird
    - bei der Beantragung einer PKIBw-Karte an das TrustCenterBw (zentrale Registrierungsstelle) mit der Post gesandt und eine Kopie des PKIBw-Antrags wird dem Antragsteller einer PKIBw-Karte ausgehändigt,
    - bei der Beantragung eines eDA / eTA in der lokalen Registrierungsstelle eingescannt, in das CMS importiert, elektronisch signiert und archiviert und das Original dem Antragsteller übergeben.
- Bei der Beantragung von Pseudonym-Zertifikaten ist es zulässig, dass lokale Registrierungsstellen einen reduzierten Antrag (nur zertifikatsrelevante Daten) an die zentrale Registrierungsstelle senden. Dadurch kann sichergestellt werden, dass seitens PKIBw nur diese lokale Registrierungsstelle die Zuordnung Pseudonym – Person kennt. Der vollständige Antrag wird in der lokalen Registrierungsstelle aufbewahrt.
- Der Antrag wird für die Verarbeitung durch die BundeswehrCA freigegeben. Die Beantragung beinhaltet die Erzeugung neuer Schlüssel durch die BundeswehrCA. Eine Zertifizierung von selbst generierten Schlüsseln ist nicht zulässig.

Temporäre PKI-Karten:

Für jede temporäre PKI-Karte (mit zugehörigen, begrenzt-gültigen Personen-Zertifikaten) ist durch den Antragsteller und die lokale Registrierungsstelle der folgende Ablauf einzuhalten:

- Der Antragsteller muss sich gemäß 3.1.8 identifizieren und authentisieren.
- Persönliche Informationen über den Teilnehmer, die im Zertifikat eingetragen werden und zur Abwicklung des Geschäftsvorfalles notwendig sind, werden dem zentralen Verzeichnisdienst der Bw entnommen und auf dem Antrag eingetragen. Der Teilnehmer hat diese Daten auf Korrektheit zu prüfen und bestätigt dies mit seiner Unterschrift auf dem Antrag.
- Die Zertifizierungs- und Antragsdaten (siehe Abschnitt 2.8) werden durch den Mitarbeiter der lokalen Registrierungsstelle im CMS bestätigt. Dabei muss er sich mit Chipkarte und Eingabe der PIN authentisieren.
- Nach Bestätigung wird die elektronische Personalisierung eines Kartenrohlings am LRA Rechner durchgeführt. Dabei werden automatisiert neue Schlüssel erzeugt und ggf. Entschlüsselungsschlüssel vorheriger Chipkarten auf die temporäre PKI-Karte wiederhergestellt.
- Das Original des Antrages, der gleichzeitig Empfangsbestätigung für die temporare PKI-Karte ist, wird vom Antragsteller und vom Mitarbeiter der lokalen Registrierungsstelle unterschrieben, in der lokalen Registrierungsstelle eingescannt, in das CMS importiert, elektronisch signiert und archiviert und das Original dem Antragsteller übergeben.

4.1.2. Zertifikate für organisatorische Einheiten

Benötigt eine organisatorische Einheit Schlüssel und Zertifikate, muss für sie ein Schlüsselverantwortlicher benannt werden (siehe auch 3.1.9). Der Schlüsselverantwortliche beantragt und verwaltet die Schlüssel und Zertifikate für die organisatorische Einheit.

Der Schlüsselverantwortliche übernimmt die Verwaltung des Schlüssels der OrgEinheit auf unbestimmte Zeit. Er bleibt insbesondere auch bei einem Dienstort- oder Dienststellenwechsel gegenüber der PKIBw verantwortlich für die Verwaltung der ihm überlassenen Schlüssel, kann diese Verantwortung jedoch an eine andere Person übertragen.

Für diese andere Person ist ebenfalls eine Benennung zum Schlüsselverantwortlichen der entsprechenden OrgEinheit durchzuführen und der zentralen Registrierungsstelle bekannt zu geben (siehe auch 3.1.9).

Scheidet der Schlüsselverantwortliche aus dem Dienst aus, werden die von ihm verwalteten Zertifikate nach einem Monat gesperrt, wenn bis dahinkein Nachfolger benannt wurde.

Wechselt die PKIBw-Chipkarte, die der Schlüsselverantwortliche zur Authentisierung gegenüber dem CMS verwendet, so hat der Schlüsselverantwortliche die Kartennummer der neuen PKIBw-Chipkarte der zentralen Registrierungsstelle mitzuteilen.

Für jedes beantragte Zertifikat ist der folgende Ablauf einzuhalten (elektronische Beantragung):

- Der Antragsteller muss sich gemäß Abschnitt 3.1.9 am CMS mittels PKIBw-Chipkarte authentisieren.

- Der Schlüsselverantwortliche beantragt elektronisch über das Card Management System ein oder mehrere Zertifikate für OrgEinheiten.

- Die Zertifizierungsdaten und die Antragsdaten des Schlüsselverantwortlichen (siehe 2.8) werden durch den Mitarbeiter der zentralen Registrierungsstelle im CMS bestätigt.

- Der Antrag wird für die Verarbeitung durch die BundeswehrCA freigegeben. Die Beantragung beinhaltet die Erzeugung neuer Schlüssel durch die BundeswehrCA. Eine Zertifizierung von selbst generierten Schlüsseln ist nicht zulässig.

4.1.3. Zertifikate für technische Komponenten

Benötigt eine technische Komponente Schlüssel und Zertifikate, muss für sie ein Schlüsselverantwortlicher benannt werden (siehe auch 3.1.10). Der Schlüsselverantwortliche beantragt und verwaltet die Schlüssel und Zertifikate für die technische Komponente.

Der Schlüsselverantwortliche muss bereits Teilnehmer der PKIBw, Anteil Verwaltungs-PKI, und über elektronische Kommunikation erreichbar sein.

Der Schlüsselverantwortliche übernimmt die Verwaltung des Schlüssels der technischen Komponente bis zum Ablauf seiner Benennung oder bis zum Ende des Gültigkeitszeitraumes des von ihm verwalteten Zertifikates und Schlüssels. Er bleibt insbesondere auch bei einem Dienstort- oder Dienststellenwechsel gegenüber der PKIBw verantwortlich für die Verwaltung der ihm überlassenen Schlüssel, kann diese Verantwortung jedoch an eine andere Person übertragen.

Für diese andere Person ist ebenfalls eine Benennung zum Schlüsselverantwortlichen der entsprechenden technischen Komponente durchzuführen und der zentralen Registrierungsstelle bekannt zu geben (siehe auch 3.1.10).

Scheidet der Schlüsselverantwortliche aus dem Dienst aus, werden die von ihm verwalteten Zertifikate gesperrt, wenn vorher kein Nachfolger benannt wurde.

Für jedes beantragte Zertifikat ist durch den Antragsteller und die zentrale Registrierungsstelle der folgende Ablauf bei Beantragung mittels elektronischer Nachricht einzuhalten:

- Der Antragsteller muss sich gemäß Abschnitt 3.1.10 am CMS mittels PKIBw-Chipkarte authentisieren.

- Der Schlüsselverantwortliche beantragt elektronisch über das Card Management System ein oder mehrere technische Komponenten.

- Dabei ist ggf. die von der technischen Komponente erzeugte Zertifizierungsanfrage im CMS beizufügen (Hochladen der Datei). Eine Zertifizierung von selbst generierten Schlüsseln ist nur in den Fällen zulässig, bei denen eine Schlüsselerzeugung durch die BundeswehrCA aus technischen Gründen nicht möglich ist.

- Die Zertifizierungs- und die Antragsdaten des Schlüsselverantwortlichen (siehe 2.8) werden durch den Mitarbeiter der zentralen Registrierungsstelle im CMS bestätigt.

- Der Antrag wird für die Verarbeitung durch die BundeswehrCA freigegeben. Im Normalfall beinhaltet die Beantragung die Erzeugung neuer Schlüssel durch die BundeswehrCA. Nur im Ausnahmefall werden Requests von durch die Komponente selbst generierten Schlüsseln zertifiziert.

4.1.4. Zertifikate für Funktionen bzw. Funktionsbereiche

Benötigt eine Funktion bzw. Funktionsbereich Schlüssel und Zertifikate, muss für sie ein Schlüsselverantwortlicher benannt werden (siehe auch 3.1.9). Der Schlüsselverantwortliche beantragt und verwaltet die Schlüssel und Zertifikate für die Funktion bzw. Funktionsbereich.

Der Schlüsselverantwortliche übernimmt die Verwaltung des Schlüssels der Funktion bzw. Funktionsbereichs auf unbestimmte Zeit. Er bleibt insbesondere auch bei einem Dienstort- oder Dienststellenwechsel gegenüber der PKIBw verantwortlich für die Verwaltung der ihm überlassenen Schlüssel, kann diese Verantwortung jedoch an eine andere Person übertragen.

Für diese andere Person ist ebenfalls eine Benennung zum Schlüsselverantwortlichen der entsprechenden Funktion bzw. Funktionsbereichs durchzuführen und der zentralen Registrierungsstelle bekannt zu geben (siehe auch 3.1.9).

Scheidet der Schlüsselverantwortliche aus dem Dienst aus, werden die von ihm verwalteten Zertifikate gesperrt, wenn vorher kein Nachfolger benannt wurde.

Wechselt die PKIBw-Chipkarte, die der Schlüsselverantwortliche zur Authentisierung gegenüber dem CMS verwendet, so hat der Schlüsselverantwortliche die Kartennummer der neuen PKIBw-Chipkarte der zentralen Registrierungsstelle mitzuteilen.

Für jedes beantragte Zertifikat ist der folgende Ablauf einzuhalten (elektronische Beantragung):

- Der Antragsteller muss sich gemäß Abschnitt 3.1.9 am CMS mittels PKIBw-Chipkarte authentisieren.

- Der Schlüsselverantwortliche beantragt elektronisch über das Card Management System ein oder mehrere Zertifikate für die Funktion bzw. Funktionsbereich.

- Die Zertifizierungsdaten und die Antragsdaten des Schlüsselverantwortlichen (siehe 2.8) werden durch den Mitarbeiter der zentralen Registrierungsstelle im CMS bestätigt.

- Der Antrag wird für die Verarbeitung durch die BundeswehrCA freigegeben. Die Beantragung beinhaltet die Erzeugung neuer Schlüssel durch die BundeswehrCA. Eine Zertifizierung von selbst generierten Schlüsseln ist nicht zulässig.

4.1.5. Wiederherstellung von privaten Schlüsseln im Compliance Prozess

Im Auftrag einer berechtigten Stelle, die in Kapitel 6.2.3 abschließend genannt sind, kann ein nach Kapitel 3.1.12 benannter und verpflichteter Compliance Manager dieser Stelle, einen Antrag für die Wiederherstellung von privaten Schlüsseln stellen.

Der Compliance Manager trägt die Verantwortung für das sichere Handling der erstellten Karte. Er bleibt insbesondere auch bei einem Dienstort- oder Dienststellenwechsel gegenüber der PKIBw verantwortlich für die Verwaltung und Vernichtung der ihm überlassenen Schlüssel.

Wechselt die PKIBw-Chipkarte, die der Compliance Manager zur Authentisierung gegenüber dem CMS verwendet, so hat der Schlüsselverantwortliche die Kartennummer der neuen PKIBw-Chipkarte der zentralen Registrierungsstelle mitzuteilen.

Für jedes beantragte Zertifikat ist der folgende Ablauf einzuhalten (elektronische Beantragung):

- Der Antragsteller muss sich gemäß Abschnitt 3.1.9 am CMS mittels PKIBw-Chipkarte authentisieren.

- Der Schlüsselverantwortliche beantragt elektronisch über das Card Management System die Wiederherstellung aller privaten Schlüssel eines Nutzers. Dabei bestätigt er durch die Beantragung, dass die Voraussetzungen für die Wiederherstellung der Schlüssel gegeben sind und die Mitbestimmungsgremien korrekt eingebunden wurden.

- Die Antragsdaten werden durch den Leiter der zentralen Registrierung geprüft und im CMS bestätigt. Der Nutzer wird über die Antragsstellung und Bestätigung per E-Mail unterrichtet.

- Der Antrag wird für die Verarbeitung durch die BundeswehrCA freigegeben. Die Beantragung beinhaltet nur die Wiederherstellung einer festgelegten Liste privater Schlüssel. Die Erzeugung neuer Schlüssel und Zertifizierung von Schlüsseln findet nicht statt und ist nicht zulässig.

4.2. Ausstellung von Zertifikaten

Die Ausstellung eines Zertifikates durch die BundeswehrCA beinhaltet die vollständige und endgültige Überprüfung der Beantragung eines Zertifikates durch die lokale bzw. zentrale Registrierungsstelle.

Von den Registrierungsstellen im CMS freigegebene Zertifizierungsanträge werden von der BundeswehrCA ausgeführt. Einzelheiten sind in den nachfolgenden Abschnitten beschrieben.

4.2.1. Zertifikate von Personen und Funktionen bzw. Funktionsbereichen

PKIBw-Karten, eDA / eTA und funktionsbezogene Chipkarten:

Die Erzeugung von Schlüsseln und Zertifikaten der Personen und Funktionen bzw. Funktionsbereiche geschieht durch die BundeswehrCA gemäß den Sicherheitsrichtlinien aus Kapitel 5 und 6. Dieser Prozess beinhaltet die folgenden Funktionen:

- Erzeugung der Aktivierungsdaten, deren Speicherung in der Chipkarte und Ausdruck,
- Schlüsselgenerierung in der Chipkarte bzw. in einem Hardware Security Modul (HSM) im KeyExport Modus,
- Zertifizierung der öffentlichen Schlüssel und Speicherung der ausgestellten Zertifikate im Schlüsselträgermedium und
- Auslieferung der Schlüsselträger an die lokalen Registrierungsstellen bzw. an die Schlüsselverantwortlichen für Funktionen bzw. Funktionsbereiche.

Der gesamte Prozess findet in den Räumlichkeiten des TrustCenterBw statt.

Temporäre PKI-Karten:

Die Erzeugung von Schlüsseln und Zertifikaten für temporäre PKI-Karten für Personen geschieht gemäß den Sicherheitsrichtlinien aus Kapitel 5 und 6. Dieser Prozess beinhaltet die folgenden Funktionen:

- Prüfung anhand der Chipseriennummer, ob der in der LRA zu personalisierende Kartenrohling ein zuvor im TrustCenterBw initialisierter ist,
- Erzeugung der Aktivierungsdaten und Speicherung in der Chipkarte, verschlüsselte und authentisierte Übertragung der Aktivierungsdaten an das TrustCenterBw,
- Schlüsselgenerierung in der Chipkarte bzw. in einem Hardware Security Modul (HSM) im KeyExport Modus im TrustCenterBw,
- Zertifizierung der öffentlichen Schlüssel, verschlüsselte und authentisierte Übertragung der Zertifikate und Entschlüsselungsschlüssel zur Chipkarte und Speicherung auf der Chipkarte.

4.2.2. Zertifikate von organisatorischen Einheiten

Die Erzeugung von Schlüsseln und Zertifikaten der OrgEinheiten geschieht durch die BundeswehrCA gemäß den Sicherheitsrichtlinien aus Kapitel 5 und 6. Dieser Prozess beinhaltet die folgenden Funktionen:

- Schlüsselgenerierung,
- Zertifizierung der öffentlichen Schlüssel,
- Erzeugung und Speicherung der Aktivierungsdaten,
- Speicherung der Schlüssel und Zertifikate in einer Schlüsseldatei und

- Versand der Schlüsseldatei mittels signierter und verschlüsselter E-Mail direkt an den Antragsteller.

Der gesamte Prozess findet in den Räumlichkeiten des TrustCenterBw statt.

4.2.3. Zertifikate technischer Komponenten

Die Erzeugung von Schlüssel und Zertifikaten der technischen Komponenten erfolgt nach dem gleichen Prozess wie in Abschnitt 4.2.2 beschrieben.

Wird bei der Beantragung ein von einer technischen Komponente erzeugter Zertifizierungsantrag beigefügt, wird nur das ausgestellte Zertifikat direkt an den Antragsteller ausgeliefert.

4.3. Übergabe von Zertifikaten

4.3.1. Persönliche Übergabe

Bei der persönlichen Übergabe des Schlüsselträgers in der lokalen Registrierungsstelle wird der Antragsteller über seine Verpflichtungen und die ihm zur Verfügung stehenden Informationsmöglichkeiten belehrt. Die Belehrung kann entfallen, wenn durch die Registrierungsstelle zu einem früheren Zeitpunkt eine Belehrung erfolgte und seitdem keine geänderten Regelungen eingeführt wurden.

Der Antragsteller bestätigt den Erhalt des Schlüsselträgermediums mit zugehörigen Schlüsseln und Zertifikaten. Dazu unterzeichnet der Antragsteller handschriftlich eine Empfangsbestätigung.

Mit Ausstellung der Bestätigung quittiert der Antragsteller, dass

- er das Schlüsselträgermedium unbeschädigt erhalten hat und

- er über seine Verpflichtungen und die ihm zur Verfügung stehenden Informationsmöglichkeiten belehrt wurde.

Das Original der Empfangsbestätigung wird

- für die PKIBw-Karten an das TrustCenterBw (zentrale Registrierungsstelle) mit der Post versendet und dort archiviert. Der Antragsteller erhält eine Kopie der Empfangsbestätigung.

- für eDA / eTA und temporäre PKI-Karten in der lokalen Registrierungsstelle eingescannt und in das CMS importiert. Der Antragsteller erhält einen zusätzlichen Ausdruck der Empfangsbestätigung mit einem zufällig generierten Passwort zur Entschlüsselung des elektronischen PIN/PUK-Briefes.

PKIBw-Karte und eDA / eTA:

Im CMS wird die Empfangsbestätigung vermerkt, woraufhin von der zentralen Registrierungsstelle der elektronische Versand des PIN/PUK-Briefes bzw. des Passwortes für den Schlüsselträger initiiert wird.

Temporäre PKI-Karte:

Im CMS wird die Empfangsbestätigung vermerkt, woraufhin unmittelbar der elektronische Versand des PIN/PUK-Briefes bzw. des Passwortes für den Schlüsselträger initiiert wird.

4.3.2. Elektronische Übergabe

Die Schlüssel für OrgEinheiten und technische Komponenten werden auf elektronischem Wege ausgeliefert.

Dazu wird die mit einem Passwort geschützte Schlüsseldatei über das CMS zum Download bereit gestellt. Für den Download muss sich der Antragsteller mittels PKIBw-Chipkarten gegenüber dem CMS authentisieren.

Die Empfangsbestätigung durch den Antragsteller erfolgt über die Funktionalität des CMS. Für die Empfangsbestätigung muss sich der Antragsteller zuvor mittels PKIBw-Chipkarten gegenüber dem CMS authentisiert haben.

Daraufhin wird der elektronische PIN/PUK-Brief mit dem Passwort der Schlüsseldatei in verschlüsselter Form zum Download über das CMS bereitstellt. Der Antragsteller authentisiert sich am CMS und lädt den verschlüsselten PIN/PUK-Brief herunter. Die Entschlüsselung des PIN/PUK-Briefes ist nur mit dem zugehörigen privaten Schlüssel auf der PKIBw-Chipkarte des Antragstellers möglich.

Bei der elektronischen Übergabe von eindeutig für Testzwecke beantragten Zertifikaten für OrgEinheiten und technische Komponenten ist es zulässig, das Passwort der Schlüsseldatei mit einer verschlüsselten und signierten elektronischen Nachricht zu versenden. Hierzu ist es erforderlich, dass der Antragsteller das Trustcenter mit einer signierten Nachricht damit beauftragt.

Unmittelbar nach Ablauf des Tests und vor Aufnahme des produktiven Betriebes ist das Test-Zertifikat zu sperren und durch ein Zertifikat mit regelgerechter Übermittlung des elektronischen PIN/PUK-Briefes zu ersetzen.

Wurde für eine technische Komponente ein Zertifizierungsantrag gestellt, wobei der zu zertifizierende Schlüssel von der Komponente selbst erzeugt wurde, wird das ausgestellte Zertifikat über das CMS zum Download bereitgestellt. Zum Download muss sich der Antragsteller mittels PKIBw-Chipkarten gegenüber dem CMS authentisieren.

4.3.3. Auslieferung über den Postweg

Schlüssel (Chipkarten) für Funktionen und Compliance-Karten werden auf dem Postweg an den Antragsteller ausgeliefert.

Die Empfangsbestätigung durch den Antragsteller erfolgt über die Funktionalität des CMS. Für die Empfangsbestätigung muss sich der Antragsteller zuvor mittels PKIBw-Chipkarten gegenüber dem CMS authentisiert haben.

Für Compliance-Karten wählt der Antragsteller einen weiteren Compliance Manager („Compliance Manager PIN“) aus, der den elektronischen PIN/PUK-Brief für die Compliance-Karte erhalten soll.

Daraufhin wird der elektronische PIN/PUK-Brief in verschlüsselter Form zum Download über das CMS bereitstellt. Der Antragsteller authentisiert sich am CMS und lädt den verschlüsselten PIN/PUK-Brief herunter. Die Entschlüsselung des PIN/PUK-Briefes ist nur mit dem zugehörigen privaten Schlüssel auf der PKIBw-Chipkarte des Antragstellers möglich.

4.3.4. Prüfung der Zertifikate und Schlüssel

Der Antragsteller hat nach Erhalt des PIN/PUK-Briefes / des Passwortes und des Schlüsselträgers bzw. der Schlüsseldatei den Inhalt der darauf bzw. darin enthaltenen Zertifikate auf Korrektheit und die Verwendbarkeit der Schlüssel zu prüfen.

Bei Unstimmigkeiten ist die zentrale Registrierungsstelle zu informieren. Bis zur Klärung der Sachlage dürfen die Zertifikate und Schlüssel nicht weiter verwendet werden.

Sofern sich Registrierungsdaten als fehlerhaft herausstellen, ist eine erneute Beantragung erforderlich und die ausgestellten Zertifikate sind vom Antragsteller sperren zu lassen. Eine erneute Zertifizierung der ausgegebenen Schlüssel ist nicht vorgesehen.

4.4. Sperren und Suspendieren von Zertifikaten

4.4.1. Gründe für eine Sperrung

Die Zertifikate für Personen, technische Komponenten, OrgEinheiten oder Funktionen bzw. Funktionsbereiche sind umgehend zu sperren bzw. sperren zu lassen, falls einer der folgenden Gründe 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.
- Der zertifizierte Schlüssel oder die damit verwendeten Algorithmen entsprechen nicht mehr den aktuellen Anforderungen.
- Missbrauch oder Verdacht auf Missbrauch durch den Zertifikatsinhaber oder andere zur Nutzung des Schlüssels berechtigte Personen.

Es liegt im Ermessen des TrustCenterBw Karten zu sperren, die Zertifikate und Schlüssel beinhalten, die auf einer Compliance-Karte wiederhergestellt wurden. Der Grund für die Sperrung muss bei der Beantragung der Sperrung genannt werden, dieser wird jedoch nicht in die Sperrliste aufgenommen, sondern steht der BundeswehrCA zur statistischen Auswertung zur Verfügung.

4.4.2. Zum Sperrantrag berechtigte Personen

Die Sperrung von Zertifikaten natürlicher Personen kann vorgenommen werden

- vom Zertifikatsinhaber selbst,
- der Dienststelle des Zertifikatsinhabers,,
- von seiner personalbearbeitenden Stelle.

Die Sperrung von Zertifikaten organisatorischer Einheiten kann vorgenommen werden

- vom beauftragten Schlüsselverantwortlichen,
- von dem Vorgesetzten oder Dienststellenleiter des Schlüsselverantwortlichen,
- Sperrung bei Löschung des Eintrages im zentralen Verzeichnisdienst.

Die Sperrung von Zertifikaten für technische Komponenten kann vorgenommen werden

- vom beauftragten Schlüsselverantwortlichen der technischen Komponente,
- von dem Vorgesetzten oder Dienststellenleiter des Schlüsselverantwortlichen.

Die Sperrung von Zertifikaten für Funktionen bzw. Funktionsbereiche kann vorgenommen werden

- vom beauftragten Schlüsselverantwortlichen,
- von dem Vorgesetzten oder Dienststellenleiter des Schlüsselverantwortlichen
- Sperrung bei Löschung des Eintrages im zentralen Verzeichnisdienst.

Bei allen Zertifikaten kann eine Sperrung durch die Zertifizierungsstelle veranlasst werden.

4.4.3. Bestimmungen zur Durchführung einer Sperrung

Bei Vorliegen eines Sperrgrundes gemäß 4.4.1 muss durch eine berechtigte Person gemäß 4.4.2 eine Sperrung unverzüglich veranlasst werden.

Zertifikatsinhaber werden von der BundeswehrCA über eine durchgeführte Sperrung informiert, unabhängig von wem die Sperrung eingeleitet wurde, sofern der Betroffene noch im Dienst der Bundeswehr steht.

Im Einzelnen gelten folgende Regelungen:

4.4.3.1. Sperrung von Personenzertifikaten

Bei Sperrung eines Personen-Zertifikates werden alle auf der Chipkarte ausgegebenen Zertifikate des Zertifikatsinhabers gesperrt. Dabei werden auch historische Verschlüsselungszertifikate (d.h. Verschlüsselungszertifikate früherer Chipkarten, die wiederhergestellt wurden) gesperrt, sofern diese noch nicht abgelaufen sind. Die einzige Ausnahme bildet die Rückgabe einer temporären PKI-Karte. In diesem Fall werden nur die aktuellen begrenzt gültigen Personen-Zertifikate gesperrt (nicht aber historische Verschlüsselungszertifikate).

Die Verschlüsselungsschlüssel können abhängig von der eingesetzten Anwendung nach einer Sperrung des dazugehörigen Zertifikates noch zur Entschlüsselung von Daten genutzt werden. Sofern ein Zugriff auf den privaten Schlüssel noch möglich ist, hat der Zertifikatsinhaber vor der Rückgabe des Schlüsselträgers eine Umschlüsselung der Daten selbst vorzunehmen. Andernfalls kann, sofern für die jeweilige Anwendung verfügbar, der lokale Message Recovery Dienst zur Entschlüsselung von Daten in Anspruch genommen werden. Mit Einführung des Key Backup & Recovery Verfahrens kann der private Entschlüsselungsschlüssel von Chipkarten, die ab diesem Zeitpunkt ausgegeben worden sind, auf einer neuen Chipkarte wieder hergestellt werden. Damit kann auf Daten wieder zugegriffen werden, die mit diesem Schlüsselpaar verschlüsselt worden sind.

Sperrung durch den Zertifikatsinhaber

Zertifikatsinhaber können ihre Zertifikate auf einem der folgenden Wege sperren lassen:

- **elektronisch**: über den Self-Service im Card Management Systems unter Angabe des Sperrgrunds und des Sperrkennworts

- **telefonisch:** unter Angabe des Distinguished Name oder der Seriennummer im Zertifikat und ihres persönlichen Sperrkennwortes bei der Hotline der PKIBw (gilt nicht für Personen-Zertifikate zu temporären PKI-Karten),

- **persönlich:** bei der nächstgelegenen Registrierungsstelle, wobei eine Authentisierung über einen Dienst-, Truppen- oder Personalausweis erforderlich ist. Die Registrierungsstelle initiiert die Sperrung über das CMS. Dazu meldet sich der Registrierungsstellenmitarbeiter mit seiner Chipkarte am CMS an. Die Sperrung wird unmittelbar an die BundeswehrCA zur Ausführung weitergeleitet.

Sperrung durch die Dienststelle

Neben dem Zertifikatsinhaber selbst kann eine Sperrung seiner Zertifikate auch durch seine Dienststelle veranlasst werden, wenn ein Missbrauch oder ein Verdacht auf Missbrauch durch den Zertifikatsinhaber vorliegt.

Der Antrag auf Sperrung ist bei der nächstgelegenen Registrierungsstelle einzureichen. Dem Antrag ist die Begründung für die Sperrung beizufügen.

Die Registrierungsstelle initiiert die Sperrung über das CMS. Dazu meldet sich der Registrierungsstellenmitarbeiter mit seiner Chipkarte am CMS an. Die Sperrung wird unmittelbar an die BundeswehrCA zur Ausführung weitergeleitet

Sperrung durch die personalbearbeitende Stelle

Der Austritt eines Zertifikatsinhabers aus dem Dienstverhältnis wird durch seine personalbearbeitende Stelle in dem zuständigen IT-System vermerkt. Dies hat die Löschung seines Eintrages im zentralen Verzeichnisdienst zur Folge.

Die Löschung eines Benutzereintrages im zentralen Verzeichnisdienst löst eine automatische Mitteilung an die BundeswehrCA aus, die daraufhin das Zertifikat des Zertifikatsinhabers sperrt.

Sperrung durch die Zertifizierungsstelle

Neben den o. g. Personen und Stellen ist die BundeswehrCA berechtigt, eine Sperrung durchzuführen, wenn sie von einem der Sperrgründe gemäß Abschnitt 4.4.1 Kenntnis erlangt.

4.4.3.2. Sperrung von Zertifikaten organisatorischer Einheiten

Sperrung durch den Zertifikatsinhaber

Schlüsselverantwortliche (als Zertifikatsinhaber) können ihre Zertifikate auf einem der folgenden Wege sperren lassen:

- **elektronisch**: über den Self-Service im Card Management Systems unter Angabe des Sperrgrunds und des Sperrkennworts

- **telefonisch:** unter Angabe des eindeutigen Namens des Zertifikatsinhabers und der Seriennummer im Zertifikat und des Sperrkennwortes bzw. Antwort auf die Sperrfrage, bei der Hotline der PKIBw,

Der Nutzer des Schlüssels, d.h. die OrgEinheit selbst, ist nicht zur Sperrung des Zertifikates berechtigt. Bei Vorliegen eines der Sperrgründe gemäß Abschnitt 4.4.1 hat die OrgEinheit umgehend den Schlüsselverantwortlichen zu informieren-

Sperrung durch die Dienststelle

Neben dem Zertifikatsinhaber selbst kann eine Sperrung seiner Zertifikate auch durch seine Dienststelle veranlasst werden, wenn ein Missbrauch oder ein Verdacht auf Missbrauch durch den Zertifikatsinhaber vorliegt. Der Antrag erfolgt schriftlich per Brief an die zentrale Registrierungsstelle der PKIBw.

Sperrung bei Löschung des Eintrages im zentralen Verzeichnisdienst

Die Löschung des Eintrages der OrgEinheit im zentralen Verzeichnisdienst löst eine automatische Mitteilung an die BundeswehrCA aus, die daraufhin das zugehörige Zertifikat sperrt.

Sperrung durch die Zertifizierungsstelle

Neben den o. g. Personen und Stellen ist die BundeswehrCA berechtigt, eine Sperrung durchzuführen, wenn sie von einem der Sperrgründe gemäß Abschnitt 4.4.1 Kenntnis erlangt.

4.4.3.3. Sperrung von Zertifikaten technischer Komponenten

Es gelten die Regeln gemäß Abschnitt 4.4.3.1 mit folgender Abweichung:

- Die Regelung zur Sperrung bei Löschung des Eintrages im zentralen Verzeichnisdienst entfällt.

4.4.3.4. Sperrung von Zertifikaten für Funktionen bzw. Funktionsbereiche

Es gelten die Regeln gemäß Abschnitt 4.4.3.1.

4.4.4. Frist bis zur Bekanntgabe der Sperrung

Elektronische und persönliche Sperrungen werden unverzüglich durchgeführt (siehe auch Abschnitt 4.4.9).

Bei allen anderen Sperrungen, die von der BundeswehrCA im System veranlasst werden, wird die Durchführung der Sperrung ab Eingang des Antrages bei der BundeswehrCA bis spätestens zum nächsten Arbeitstag gewährleistet.

Eine durchgeführte Sperrung kann nicht rückgängig gemacht werden.

4.4.5. Gründe für eine Suspendierung

Suspendierungen werden im Zuständigkeitsbereich der PKIBw, Anteil Verwaltungs-PKI, nicht vorgenommen.

4.4.6. Zur Suspendierung berechtigte Personen

Entfällt.

4.4.7. Einreichung eines Antrags auf Suspendierung

Entfällt.

4.4.8. Dauer einer Suspendierung

Entfällt.

4.4.9. Aktualisierung der Sperrlisten

Die Sperrlisten der BundeswehrCA (Certificate Revocation Lists, kurz CRLs) werden regelmäßig und automatisiert ausgestellt und im zentralen Verzeichnisdienst der Bw sowie zusätzlich über den OCSP-Dienst gemäß 2.6.1 veröffentlicht. Sie enthalten den Zeitpunkt der Ausstellung und den Zeitpunkt, zu dem die nächste reguläre Sperrliste ausgestellt wird.

Die Sperrlisten werden regelmäßig alle 24 Stunden ausgestellt. Der eingetragene Gültigkeitszeitraum der Sperrlisten beträgt 48 Stunden.

Zusätzlich zur regelmäßigen Ausstellung werden Sperrlisten nach jeder Sperrung erzeugt und veröffentlicht. Dabei wird als Zeitpunkt des Endes der Gültigkeit der Zeitpunkt der nächsten regelmäßigen Aktualisierung eingetragen.

Bei der Veröffentlichung im Verzeichnis wird durch den Verzeichnisdienst und die BundeswehrCA sichergestellt, dass eine vorhandene Sperrliste durch die aktuellere ersetzt wird.

4.4.10. Anforderungen an die Überprüfung von Sperrlisten

Die Zertifikatsnutzer sind verantwortlich für die Prüfung der Gültigkeit eines übermittelten Zertifikats. In der Client-Umgebung gespeicherte Zertifikate sollten vor ihrer Nutzung gegen eine aktuelle Sperrliste geprüft werden.

An die Überprüfung des Gültigkeitsstatus mittels Sperrlisten werden die folgenden Anforderungen gestellt:

- Ein Zertifikatsnutzer sollte die Authentizität einer Sperrliste durch die Prüfung der in der Sperrliste enthaltenen Signatur verifizieren.
- Die Aktualität der Sperrliste sollte auf der Grundlage ihres Gültigkeitszeitraumes geprüft werden.
- Es sollte der vollständige Zertifizierungspfad auf Gültigkeit geprüft werden.

Sofern keine erfolgreiche Gültigkeitsprüfung vorgenommen werden kann (z. B. aus technischen Gründen), sollten keine Zertifikate akzeptiert werden. Jede Akzeptanz eines solchen Zertifikates erfolgt auf Risiko des Zertifikatsnutzers.

4.4.11. Online-Statusabfrage

Im Zuständigkeitsbereich der PKIBw, Anteil Verwaltungs-PKI, besteht die Möglichkeit einer Online-Statusabfrage mittels OCSP (Online Certificate Status Protocol).

In den von der BundeswehrCA ausgestellten Zertifikaten wird die Erweiterung „Authority Information Access“ mit dem Wert „http://ocsp-v.bundeswehr.org/ocsp“ gefüllt, wodurch Anwendungen, welche OCSP unterstützen, die URL des OCSP-Responders automatisch ermitteln können.

Der OCSP-Dienst antwortet für alle durch die BundeswehrCA, Anteil Verwaltungs-PKI, ausgestellten Zertifikate.

4.4.12. Verpflichtung zur Nutzung einer Online-Statusabfrage

Es existiert keine Verpflichtung zur Nutzung. Den Anwendungen ist die Art und Weise der Zertifikatsprüfung (Sperrliste oder Online-Abfrage) freigestellt.

4.4.13. Weitere Verfahren zur Bekanntgabe von Sperrungen

Keine Regelungen.

4.4.14. Spezielle Verfahren bei Kompromittierung von privaten Schlüsseln

Keine Regelungen.

4.5. Protokollierung sicherheitsrelevanter Ereignisse

4.5.1. Protokollierte Ereignisse

In der Zertifizierungsstelle werden u. a. die folgenden Ereignisse mit Datum, Uhrzeit und Verursacher protokolliert:

- Starten einer Komponente
- Anmeldung eines Rolleninhabers an einer Komponente
- Schlüsselerzeugung
- Personalisierung
- Erstellung von Zertifikaten
- Wiederherstellung von Schlüsseln
- Veröffentlichung von Zertifikaten
- Ausgeführte Sperrungen
- Erstellung von Sperrlisten
- Veröffentlichung von Sperrlisten.

Durch die zentrale Registrierungsstelle werden u. a. protokolliert:

- der Versand der Schlüsselträger bzw. Abruf von Schlüsseldateien,
- der Eingang der Empfangsbestätigung und
- der Abruf des elektronischen PIN/PUK-Briefes bzw. des Passwortes (zur Schlüsseldatei).

Zusätzlich sind folgende Ereignisse zu protokollieren:

- Änderungen der Hardwarekonfiguration
- Änderungen bei der Rollenaufteilung

- Änderung der Softwarekonfiguration
- Meldungen bzgl. des Verdachts auf Schlüsselkompromittierung.

Weitere Einzelheiten und der genaue Umfang der Protokollierung sind dem projektbezogenen IT-Sicherheitskonzept PKIBw [IT-SichhK] zu entnehmen.

4.5.2. Überprüfung der Protokolldateien

Die Protokolle der PKI-Anwendungssoftware werden regelmäßig auf sicherheitsrelevante Vorkommnisse hin untersucht, mindestens jedoch zweimal monatlich. Die Überprüfung wird vom Auditor der entsprechenden Dienststelle durchgeführt.

4.5.3. Aufbewahrungszeitraum der Protokolldateien

Die Protokolldateien werden mindestens bis zur nächsten Überprüfung im IT-System aufbewahrt. Anschließend werden die Protokolldateien gemäß Abschnitt 4.6 archiviert.

4.5.4. Schutz der Protokolldateien

Die Protokolldateien werden nur innerhalb der gesicherten Infrastruktur der BundeswehrCA und der zentralen Registrierungsstelle angefertigt und aufbewahrt. Kopien der Protokolldateien sind zusätzlich an einem gesicherten Standort aufzubewahren. Nur autorisiertes Personal der jeweiligen Stellen hat Zugriff auf die Protokolldateien. Archivierte Protokolldateien sind digital zu signieren.

4.5.5. Anfertigung von Sicherungen der Protokolldateien

Ein Backup der Protokolldateien findet in regelmäßigen Abständen statt. Die gesicherte Aufbewahrung der Backups ist sicherzustellen. Weitere Einzelheiten sind im projektbezogenen IT-Sicherheitskonzept PKIBw [IT-SichhK] festgelegt.

4.5.6. Protokollierungssystem

Die automatische Protokollierung findet durch die Komponenten des CA-Systems statt. Manuelle Protokolleinträge werden durch Eintrag in eine Protokolldatei festgehalten.

4.5.7. Benachrichtigung beim Auftreten sicherheitskritischer Ereignisse

Der IT-SiBe Projekt wird benachrichtigt, wenn die Überprüfung der Protokolldateien sicherheitskritische Ereignisse liefert und leitet die notwendigen Schritte (z. B. Benachrichtigung von Zertifikatsinhabern oder der PMABw) ein.

4.5.8. Gefährdungsabschätzung

Der Verantwortliche für die Überprüfung der Protokolldaten (Auditor) hat zu entscheiden, welche Ereignisse im Protokoll Hinweise auf sicherheitsgefährdende Handlungen oder Systemzustände sind. Er hat seine Erkenntnisse dem IT-SiBe Projekt mitzuteilen. Gegebenenfalls ist der IT-SiBe Dst für die Bewertung hinzuzuziehen.

4.6. Archivierung

In der PKIBw, Anteil Verwaltungs-PKI, werden Informationen und Dokumente archiviert, die bei der Durchführung der Prozesse Registrierung, Zertifizierung und Sperrung erzeugt werden.

4.6.1. Archivierte Daten

Von den lokalen Registrierungsstellen sind folgende Unterlagen zu archivieren:

- vollständige Originalanträge für Personen-Zertifikate, wenn bei Beantragung von Pseudonym-Zertifikaten nur reduzierte Anträge an die zentrale Registrierungsstelle gegeben werden,
- Sperranträge.

Von der zentralen Registrierungsstelle sind folgende Dokumente zu archivieren:

- vollständige Originalanträge für Personen-Zertifikate (bzw. reduzierte Antragsformulare bei Pseudonym-Zertifikaten) in Papierform, sofern sie nicht eingescannt und in der lokalen Registrierungsstelle archiviert werden (stattdessen erfolgt der Postversand zur Archivierung in der zentralen Registrierungsstelle),
- eingescannte PKIBw-Anträge und Empfangsbestätigungen für Personen-Zertifikate zu eTA / eDA und zu temporären PKI-Karten als signierte PDF-Dokumente (Speicherung im CMS),
- Sperranträge,
- alle Verpflichtungserklärungen für Mitarbeiter der PKIBw, Anteil Verwaltungs-PKI,
- Empfangsbestätigungen mit Verpflichtungserklärung für Personen-Zertifikate (bzw. reduzierte Empfangsbestätigungen bei Pseudonym-Zertifikaten), sofern sie nicht eingescannt und in der lokalen Registrierungsstelle archiviert werden,
- Einträge aus dem CMS von ausgeschiedenen Teilnehmern.

Die Antragsdaten für OrgEinheiten, technische Komponenten und Funktionen bzw. Funktionsbereiche werden als Teil des CMS Datenbestandes unverändert vorgehalten. Gleiches gilt für den Eingang der elektronischen Empfangsbestätigung in der zentralen Registrierungsstelle.

In der Zertifizierungsstelle werden folgende Dokumente archiviert:

- das Protokollbuch der BundeswehrCA in elektronischer Form,
- alle von der BundeswehrCA ausgestellten Zertifikate,
- alle von der BundeswehrCA ausgestellte Sperrlisten,
- alle von der BundeswehrCA verwendeten Zertifikate (dies beinhaltet auch die von der PCA der PKI-1-Verwaltung für die BundeswehrCA ausgestellten Zertifikate),

- in regelmäßigen Abständen die automatisch generierten Protokolldaten.

4.6.2. Aufbewahrungszeiten

Die Antragsdokumente werden mindestens 3 Jahre über den Gültigkeitszeitraum des beantragten Zertifikates hinaus aufbewahrt. Gleiches gilt für die Datensätze im CMS, die sich auf den Antragsprozess beziehen.

Die Anträge auf Sperrung bzw. mit der Sperrung angelegte elektronische Datensätze (z. B. im CMS), sowie ausgestellte Sperrlisten und alle Zertifikate werden mindestens bis 3 Jahre nach Ablauf des CA-Zertifikates aufbewahrt.

4.6.3. Schutzvorkehrungen

Archivierte elektronische Daten sind durch elektronische Signaturen vor Modifikation zu schützen. Der Zugriff auf archivierte Daten ist auf berechtigte Personen einzuschränken.

4.6.4. Backup-Prozeduren

Archivierte elektronische Daten unterliegen keinen Änderungen. Sie sind in regelmäßigen Abständen zu sichern. Dabei gelten die gleichen Anforderungen wie für die Datensicherung von Protokollen (siehe Abs. 4.5.5). Zusätzlich sind die archivierten Daten regelmäßig auf Lesbarkeit zu prüfen.

4.6.5. Anforderungen, die Daten mit Zeitstempeln zu versehen

Keine Bestimmungen.

4.6.6. System zur Erfassung der Archivierungsdaten

Das konkrete Archivierungssystem wird nach der Auswahl des CA-Systems ergänzt.

4.6.7. Handlungen zum Abrufen und Überprüfen von Daten

Das Bundesdatenschutzgesetz räumt zusätzlich jedem Teilnehmer das Recht ein, Auskunft über die von ihm gespeicherten Daten einzuholen (siehe Abs. 2.8.6).

4.7. Schlüsselwechsel

4.7.1. Schlüsselwechsel der Teilnehmer-Schlüssel

Der Wechsel der Schlüssel der Teilnehmer ist nur im Zusammenhang mit einer erneuten Registrierung und Zertifizierung möglich.

4.7.2. Schlüsselwechsel der Zertifizierungsstelle

Die BundeswehrCA erzeugt jährlich ein neues Signaturschlüsselpaar, dessen öffentlicher Schlüssel von der PCA der Verwaltung zertifiziert wird. Dieser neue Schlüssel (aktiver Schlüssel) wird bis zur Erzeugung des nächsten Signaturschlüssels zum Erstellen von Zertifikaten und Sperrlisten verwendet.

Eventuell vorhandene Schlüssel der BundeswehrCA werden mit der Nutzung eines neuen aktiven Schlüssels nur noch zum Signieren von Sperrlisten eingesetzt (passive Schlüssel). Abbildung 2 veranschaulicht die Gültigkeitsdauer von aktiven und passiven Schlüsseln über einen Zeitraum von 7 Jahren.

Der neue aktive öffentliche Schlüssel wird durch die PCA der Verwaltung neu zertifiziert und kann damit durch das Wurzelzertifikat der PCA der Verwaltung authentisch geprüft werden.

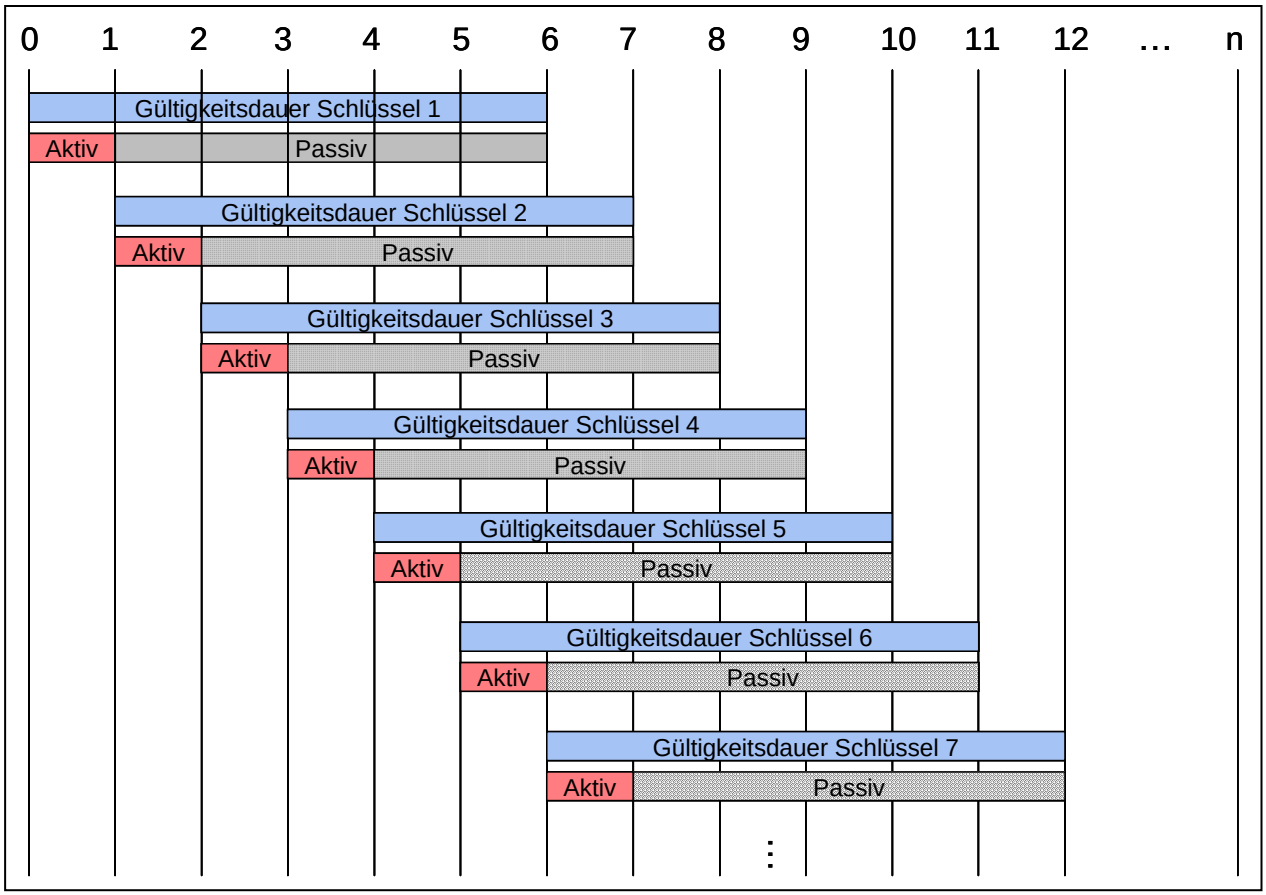

Abbildung 2: Nutzungsdauer aktiver und passiver Signaturschlüssel der BundeswehrCA

4.7.3. Außerplanmäßige Schlüsselwechsel

Die BundeswehrCA wechselt jedes Jahr ihren aktiven Signaturschlüssel. Zusätzlich können betriebsbedingt auch außerplanmäßige Wechsel notwendig sein. Ein außerplanmäßiger Wechsel des Schlüssels der BundeswehrCA kann u. a. durch folgende Ereignisse erforderlich werden:

- Kompromittierung eines Schlüssels,
- Schwachwerden von Algorithmen,
- Verlust von Schlüsseln oder

- Änderung von Zertifikatsinformationen.

In den vorab genannten Fällen ist eine Sperrung des Zertifikates der BundeswehrCA erforderlich.

4.8. Kompromittierung und Notfallplan

4.8.1. Rechner, Software und / oder Daten sind korrumpiert

Das Inkrafttreten des Notfallplans können folgende Personen anordnen:

- der Leiter TrustCenterBw oder dessen Vorgesetzte,
- der IT-SiBe der Dienststelle oder dessen Vorgesetzte,
- die PMABw.

Bei offensichtlicher Kompromittierung erfolgt die sofortige eigenverantwortliche Stilllegung durch den Leiter TrustCenterBw und sofortige Meldung an den IT-SiBe Dst. und den Vorgesetzten sowie an die PMABw.

Weitere Details sind im projektbezogenen IT-Sicherheitskonzept PKIBw [IT-SichhK] geregelt.

4.8.2. Sperrung von Zertifikaten zu CA- und Dienste-Schlüsseln

Bei Kompromittierung des privaten Schlüssels der BundeswehrCA wird umgehend das betroffene Zertifikat durch den Leiter TrustCenterBw bei der Wurzelzertifizierungsstelle gesperrt. Dies geschieht telefonisch unter Nennung des Sperrkennwortes.

Die BundeswehrCA informiert die Teilnehmer, dass ihre Zertifikate nicht mehr gültig sind, weil das Zertifikat der BundeswehrCA gesperrt wurde.

4.8.3. Schlüsselkompromittierung bzw. Verdacht auf Schlüsselkompromittierung

Siehe Abschnitt 4.8.2.

4.8.4. Sicherheitsvorkehrungen nach Katastrophen

Ein Wiederanlaufplan, der unter anderem die Wiederanlaufreihenfolge, Wiederbeschaf-fungsmöglichkeiten, Ausweichmöglichkeiten sowie die Möglichkeiten eines eingeschränkten Betriebs beschreibt, wurde definiert.

Abhängig vom Grad des eingetretenen Notfalls kann ein Wiederanlauf des IT-Systems notwendig sein. Um einen geregelten Ablauf im Zuge des Wiederanlaufs gewährleisten zu können, müssen bestimmte Informationen dokumentiert werden.

Einzelheiten sind im projektbezogenen Sicherheitskonzept PKIBw [IT-SichhK] beschrieben.

4.9. Einstellung des Betriebes der Zertifizierungsstelle

Die PMABw kann beschließen, den Betrieb der BundeswehrCA vorübergehend oder endgültig einzustellen. Eine vorübergehende Aussetzung kann beispielsweise notwendig werden, wenn ein durchgeführtes Audit (siehe Abs. 2.7) Mängel aufführt, die einen weiteren vertrauenswürdigen Betrieb nicht ermöglichen. Die Teilnehmer sind gemäß Abs. 2.6.1 zu informieren.

Die endgültige Einstellung des Betriebes der BundeswehrCA muss bei der PCA der Verwaltung angezeigt werden und hat die Sperrung aller aktiven und passiven Zertifikate der BundeswehrCA zur Folge. Die endgültige Einstellung des Betriebes ist den Teilnehmern gemäß Abs. 2.6.1 bekannt zu geben. Dabei ist eine angemessene Frist zu setzen, die es den Teilnehmern ermöglicht, auf alternative Dienste auszuweichen.

5. Sicherheitsvorkehrungen

5.1. Physische Sicherheitsvorkehrungen

Durch die PKIBw, Anteil Verwaltungs-PKI, werden Schlüssel und Zertifikate für die Verwendung im Bereich des IT-BasisschutzBw und Erweiterten IT-BasisschutzBw erstellt und ausgegeben. Diese dienen u.a. für die gesicherte Übermittlung oder Speicherung von Informationen der in Abschnitt 1.3.5 genannten Schutzbereiche.

Die Systeme zur Erstellung und Verwaltung von Schlüsseln und Zertifikaten sind besonders schützenswert, das Schutzniveau entspricht dem IT-BasisschutzBw, wie er in der ZDv 54/100 definiert wird.

Die einzelnen physischen Sicherheitsmaßnahmen müssen von der PKIBw in einem Sicherheitskonzept definiert und fortgeschrieben werden, das u.a. Regelungen für folgende Bereiche enthalten muss:

- Zutrittskontrolle,
- Sicherstellung der betrieblichen Infrastruktur (Strom, Klimatisierung, usw.),
- Schutz vor Umwelteinflüssen (Feuer, Wasser, Sturm, usw.),
- Maßnahmen zur Sicherstellung der Verfügbarkeit der Systeme.

Das Sicherheitskonzept und dessen Einhaltung werden gemäß Abschnitt 2.7 überprüft.

5.2. Verfahrensorientierte Sicherheitsvorkehrungen

Für die PKIBw, Anteil Verwaltungs-PKI, wurden Funktionsbereiche (Rollen) definiert, die beschreiben, welche Tätigkeiten für die Erfüllung der Aufgaben der PKIBw, Anteil Verwaltungs-PKI, durchzuführen sind. In der Zertifizierungsstelle sind Rollen mehrfach vorhanden und werden durch unterschiedliche Personen wahrgenommen. Aus Sicherheitsgründen sind bestimmte Rollen jedoch nicht kombinierbar.

Eine ausführliche Beschreibung der vorhandenen Rollen und den möglichen Zusammenfassungen von Rollen zu Stellen ist im Rollenkonzept [Rollen] enthalten.

Einzelheiten zu Sicherheitsvorkehrungen bei Ausübung von Rollen sind in das projektbezogene IT-Sicherheitskonzept PKIBw [IT-SichhK] und in die Betriebsdokumente aufzunehmen.

5.3. Personelle Sicherheitsvorkehrungen

5.3.1. Anforderungen an das Personal

Mitarbeiter der PKIBw, Anteil Verwaltungs-PKI, sind gemäß ZDv 54/100 auszuwählen. Dies beinhaltet, dass das Personal für die Ausübung einer Rolle entsprechendes Fachwissen besitzt. Andernfalls werden geeignete Schulungsmaßnahmen gemäß Abschnitt 5.3.3 veranlasst.

5.3.2. Überprüfung des Personals

Im TrustCenterBw wird ausschließlich Personal eingesetzt, das gemäß Sicherheitsüberprüfungs-Gesetz nach Ü3 überprüft ist.

5.3.3. Anforderungen an die Schulung und Ausbildung

Schulungen sind bei der Neubesetzung einer Stelle in fachlichen und technischen Bereichen durchzuführen.

Das technische Administrationspersonal für die IT-Systeme besitzt mindestens eine fundierte Ausbildung im Umfeld

- des Systemmanagements oder
- des Sicherheitsmanagements,
- der administrierten IT-Systeme.

Das Betriebspersonal der PKI-Anwendungen (Zertifizierungs- und Registrierungssystem) besitzt fundierte Kenntnisse in den Bereichen

- allgemeines EDV-Wissen,
- Grundlagen der IT-Sicherheit und
- Grundlagen der Kryptographie.

Darüber hinaus verfügen die eingesetzten Mitarbeiter über spezielles fachliches Wissen, das für die Ausübung ihrer jeweiligen Rolle notwendig ist.

Einzelheiten zu den erforderlichen Schulungsmaßnahmen sind im Ausbildungskonzept [AusbiKo] dargelegt.

5.3.4. Häufigkeit von Schulungswiederholungen

Einzelheiten zu den erforderlichen Schulungsmaßnahmen sind im Ausbildungskonzept [AusbiKo] dargelegt.

5.3.5. Ablauf und Häufigkeit von Tätigkeitswechseln

Der betriebliche Ablauf in der PKIBw, Anteil Verwaltungs-PKI, erfordert es, dass Rollen mehrfach besetzt sind. Dies betrifft insbesondere Regelungen im Falle von Krankheit, Urlaub und anders begründeter Abwesenheit von Mitarbeitern.

Diese und weitergehende Regelungen wie regelmäßige Tätigkeitswechsel können vom Leiter TrustCenterBw eigenverantwortlich getroffen werden, sofern die Anforderungen an Ausbildung und Rollentrennung eingehalten werden.

5.3.6. Sanktionen für unautorisierte Handlungen

Keine besonderen Regelungen im Rahmen der PKIBw.

5.3.7. Anforderungen an Vertragsvereinbarungen mit dem Personal

Keine besonderen Regelungen im Rahmen der PKIBw.

5.3.8. Dem Personal auszuhändigende Dokumente

Den Mitarbeitern der PKIBw, Anteil Verwaltungs-PKI, werden alle Dokumente und Handbücher ausgehändigt, die für die Ausübung ihrer Rollen relevant sind.

6. Technische Sicherheitsvorkehrungen

6.1. Schlüsselgenerierung und Installation

6.1.1. Schlüsselgenerierung

6.1.1.1. Schlüssel der Teilnehmer

PKIBw-Karte, eDA / eTA und Chipkarte für Funktionen bzw. Funktionsbereiche:

Die Schlüssel der Teilnehmer werden in den gesicherten Räumlichkeiten des TrustCenterBw auf einem dedizierten System erzeugt. Die Schlüssel zur Authentisierung und Signaturerstellung werden auf der Chipkarte des Teilnehmers erzeugt und gespeichert. Die Schlüssel für Ver- und Entschlüsselung werden außerhalb der Chipkarte in einem HSM im KeyExport Modus generiert und anschließend auf die Chipkarte aufgebracht. Damit wird die Erstellung eines Duplikats des privaten Schlüssels verhindert. Ferner ist eine Kenntnisnahme privater Schlüssel durch die BundeswehrCA dadurch ausgeschlossen.

Temporäre PKI-Karte:

Die Schlüssel zur Authentisierung und Signaturerstellung werden in der Chipkarte des Teilnehmers erzeugt und gespeichert. Die Schlüssel für Ver- und Entschlüsselung werden außerhalb der Chipkarte in einem HSM im KeyExport Modus generiert, das sich innerhalb des TrustCenterBw befindet. Die Schlüssel werden verschlüsselt über einen gesicherten Kanal an den Rechner in der LRA übermittelt und dann auf die Chipkarte aufgebracht. Damit wird die Erstellung eines Duplikats des privaten Schlüssels verhindert. Ferner ist eine Kenntnisnahme privater Schlüssel durch die BundeswehrCA dadurch ausgeschlossen.

Schlüsseldateien:

Schlüssel für OrgEinheiten und für technische Komponenten werden durch separate Prozesse erzeugt und als verschlüsselte Schlüsseldatei gespeichert.

Ausnahme für technische Komponenten (Schlüsselgenerierung durch die Komponente)

Technische Komponenten dürfen Schlüsselpaare innerhalb des Gerätes generieren, wenn keine fremderzeugten Schlüssel integrierbar sind, das Gerät einen elektronischen Zertifizierungsantrag erstellen kann, der den Vorgaben für die Namensvergabe gemäß Namenskonzept (vgl. Namen) entspricht und dabei die Vorgaben aus Abschnitt 6.1.7 erfüllt werden.

6.1.1.2. Schlüssel der Zertifizierungsstelle

Die Schlüsselpaare der BundeswehrCA werden innerhalb des kryptographischen Sicherheitsmoduls (siehe Abschnitt 6.2.1) erzeugt. Sie verlassen das Sicherheitsmodul nach der Erzeugung nur zum Zwecke der Datensicherung (siehe Abschnitt 6.2.4).

6.1.2. Auslieferung privater Schlüssel der Teilnehmer

Die privaten Schlüssel werden innerhalb der Chipkarte oder einer verschlüsselten Schlüsseldatei an den jeweiligen Antragsteller ausgeliefert bzw. übergeben. Sie sind dort vor dem Auslesen geschützt (siehe Abschnitt 6.2) und können nur nach Eingabe der Aktivierungsdaten (PIN, Passwort; siehe Abschnitt 6.2.7) benutzt werden.

Die Chipkarten werden dem Zertifikatsinhaber persönlich übergeben (siehe Abschnitt 4.3.1) bzw. mit der Post versendet (siehe Abschnitt 4.3.3). Die Schlüsseldateien werden dem Antragsteller elektronisch übermittelt (siehe Abschnitt 4.3.2).

6.1.3. Sichere Verteilung der Ausstellerzertifikate

Alle öffentlichen Schlüssel der BundeswehrCA werden in Form von Zertifikaten in ein Verzeichnis gestellt und können dort von Zertifikatsnutzern abgerufen werden (siehe Abschnitt 2.6.4).

Die Teilnehmer erhalten alle Ausstellerzertifikate im Zertifizierungspfad ihres eigenen Zertifikates auf ihrem Schlüsselträger (Chipkarte oder Schlüsseldatei).

Technische Komponenten, die keinen Schlüsselträger erhalten, da sie ihre Schlüsselpaare selbst erzeugen, erhalten ihr Zertifikat und alle Ausstellerzertifikate im Zertifizierungspfad in Dateiform übergeben.

Die Zertifikate der Wurzelzertifizierungsstelle (PCA) der Verwaltung können u. a. aus dem zentralen Verzeichnisdienst der Bw und dem Verzeichnisdienst der Verwaltung abgerufen werden. Je nach Anwendung muss dies durch den Teilnehmer selbst geschehen oder kann durch das Administrationspersonal zentral erfolgen.

Der Antragsteller ist verpflichtet, die Authentizität des Wurzelzertifikates anhand des sog. Fingerabdrucks mit einer vertrauenswürdigen Quelle abzugleichen.

6.1.4. Verwendete Schlüssellängen

Die Schlüssel zur Signatur von Zertifikaten und Sperrlisten, die von der BundeswehrCA verwendet werden, besitzen eine Schlüssellänge von 2048 Bit RSA Modulus.

Als Hash-Verfahren bei der Signatur von Zertifikaten und Sperrlisten wird ab dem 04.04.2014 SHA-256 verwendet. Bis vor diesem Zeitpunkt ausgestellte Zertifikate wurden mit SHA-1 signiert und sind bis zu ihrem Ablauf weiterhin gültig. Weitere Details sind im Namenskonzept [Namen] beschrieben.

Für die Signatur von OCSP-Antworten wurde vorübergehend (bis August 2014) SHA-1 verwendet, danach wird ebenfalls SHA-256.

Für die Signatur von Zeitstempeldienst-Antworten wird SHA-256 verwendet. Die Signaturen werden mit Zertifikaten mit 4096 Bit RSA Modulus ausgeführt, sobald die aktive CA der PKIBw ebenfalls ein Zertifikat mit 4096 Bit RSA Modulus nutzt. Bis zu diesem Zeitpunkt werden die Signaturen werden mit Zertifikaten mit 2048 Bit RSA Modulus ausgeführt.

Die von der PKIBw, Anteil Verwaltungs-PKI, ausgegebenen Schlüssel besitzen eine Schlüssellänge von 2048 Bit RSA Modulus. Gleiches gilt für Schlüssel, die in Ausnahmefällen durch technische Komponenten generiert werden (siehe Abschnitt 6.1.1.1).

Die Angaben zur Hashfunktion und zum Public Key Verfahren orientieren sich an den Vorgaben für geeignete Algorithmen aus [KrypAlgo14] zum Erstellungszeitpunkt des vorliegenden Dokumentes. Sie werden jährlich überarbeitet. Die Sicherheit und Eignung der Algorithmen wird überwacht.

6.1.5. Zur Schlüsselerzeugung berechtigte Personen

BundeswehrCA:

Zur Generierung von Schlüsseln für die BundeswehrCA ist die Rolle „Beauftragter zur Schlüsselgenerierung“ berechtigt.

PKIBw-Karte, eDA / eTA, Chipkarte für Funktionen:

Die Generierung von Schlüsseln zur Authentisierung und Signaturerstellung für natürliche Personen und Funktionen findet in einem automatisierten Prozess auf den Chipkarten statt. Die Schlüssel für Ver- und Entschlüsselung werden außerhalb der Chipkarten in einem HSM im KeyExport Modus generiert bzw. aus der Datenbank der BundeswehrCA abgerufen und anschließend auf die Chipkarten aufgebracht. Folgende Rollen sind zum Starten des automatisierten Prozesses berechtigt:

- „Beauftragter zur Schlüsselgenerierung“,
- „Personalisierer“ und
- „Zertifizierer“.

Temporäre PKI-Karte:

Die Generierung von Schlüsseln zur Authentisierung und Signaturerstellung für temporäre PKI-Karten findet in der LRA in einem automatisierten Prozess auf den Chipkarten statt. Die Schlüssel für Ver- und Entschlüsselung werden außerhalb der Chipkarten in einem HSM im KeyExport Modus generiert bzw. aus der Datenbank der BundeswehrCA abgerufen und über einen sicheren Kanal zum Rechner in der LRA auf die Chipkarten aufgebracht. Die Rolle „Registrator (lokal)“ ist berechtigt, den automatisch ablaufenden Prozess zu starten.

Schlüsseldateien:

Die Generierung von Schlüsseln für OrgEinheiten und technische Komponenten wird durchgeführt, nachdem die Prüfung durch die Rolle „Registrator“ erfolgt ist.

6.1.6. Überprüfung der Qualität der Schlüsselparameter

Keine Regelungen.

6.1.7. Hardware und Software zur Schlüsselerzeugung

Für kryptographische Schlüssel, die durch die PKIBw erzeugt werden, werden folgende Maßnahmen getroffen:

- Für die Generierung der CA-Schlüssel, der Zeitstempel- und der OCSP-Dienst-Schlüssel werden Hardware Security Module (HSM) eingesetzt, die nach Common Criteria Stufe mit Prüfstufe EAL4 oder nach ITSEC mit Prüfstufe E3 evaluiert sind.

- Für die Generierung der Schlüsseldateien für Teilnehmer kommen Komponenten nach dem aktuellen Stand der Technik zum Einsatz. Dabei wird ein Zufallszahlengenerator auf einem HSM verwendet.

- Die eingesetzten Chipkarten erzeugen die Teilnehmerschlüssel zur Authentisierung und Signaturerstellung auf dem Schlüsselgenerator „on board“, dieser ist nach ITSEC mit Prüfstufe E3 „hoch“ oder nach Common Criteria Stufe mit Prüfstufe EAL4+ „hohes Angriffspotential“ evaluiert.

- Für die Generierung von Teilnehmerschlüsseln zu Chipkarten mit Verwendungszweck Ver- bzw. Entschlüsselung wird ein HSM im KeyExport Modus eingesetzt. Die Hardware des HSMs ist nach FIPS 140-2 Level 3 zertifiziert.

Mit Ausnahme der Schlüssel zur Authentisierung und Signaturerstellung für temporäre PKI-Karten werden alle oben aufgeführten Schlüssel innerhalb des TrustCenterBw erzeugt.

In der Bw sind technische Komponenten im Einsatz, die das Einbringen der kryptographischen Schlüssel nicht ermöglichen. In diesem Ausnahmefall werden die Schlüssel durch technische Komponenten selbst und nicht durch die Zertifizierungsstelle generiert. Dafür ist eine Ausnahmeregelung erforderlich, die durch BAAINBw I3.3 erteilt wird.

6.1.8. Verwendungszwecke der Schlüssel

Von der PKIBw, Anteil Verwaltungs-PKI, ausgestellte Schlüssel dürfen nur für Zwecke gemäß Abschnitt 1.3.5 verwendet werden. Um die zugelassenen Verwendungszwecke kenntlich zu machen, werden in das Zertifikat Erweiterungen aufgenommen, die von Anwendungen ausgewertet werden können (vgl. [Namen]).

6.2. Schutz der privaten Schlüssel

6.2.1. Standards des kryptographischen Moduls

6.2.1.1. Regelungen für die Zertifizierungsstelle

Die privaten Schlüssel der BundeswehrCA zur Signatur von Zertifikaten, Sperrlisten, TSS-Zertifikate und OCSP-Auskünften werden nur innerhalb eines sicheren Hardware-Moduls (HSM) in der sicheren Umgebung der BundeswehrCA betrieben.

Die Schlüssel sind so in dem Sicherheitsmodul gespeichert, dass sie nur auf ein zweites HSM übertragen, nicht aber ausgelesen werden können (siehe Abschnitt 6.2.4).

Das Sicherheitsmodul ist so beschaffen, dass private Schlüssel nur innerhalb des Moduls verwendet werden können und Zugriffe nur nach entsprechender Authentifikation möglich sind. Bei Angriffen, die eine Zerstörung des Sicherheitsmoduls in Betracht ziehen, wird die Löschung der privaten Schlüssel initiiert.

Die in der PKIBw, Anteil Verwaltungs-PKI, eingesetzten HSMs müssen nach dem folgenden Standard überprüft sein:

- Common Criteria mind. Prüfstufe EAL4 oder ITSEC mind. Prüfstufe E3

6.2.1.2. Regelungen für die Teilnehmer

Die privaten Schlüssel von Personen und Funktionen werden in ISO 7816 konformen Chipkarten gespeichert. Die in der PKIBw, Anteil Verwaltungs-PKI, eingesetzten Chipkarten müssen nach dem folgenden Standard überprüft sein:

- Common Criteria mind. Stufe EAL4 „hohes Angriffspotential“, oder ITSEC mind. Sicherheitsniveau E3 „hoch“.

Es wird sichergestellt, dass alle Angaben, die auf dem Kartenkörper sichtbar aufgebracht sind, auch mit den elektronischen Daten übereinstimmen.

Die privaten Schlüssel sind auf diesen Karten gegen Auslesen geschützt und können erst nach Eingabe der Aktivierungsdaten eingesetzt werden.

Die an die Schlüsselverantwortlichen und das Administrationspersonal ausgegebenen Schlüsseldateien entsprechen dem Dateiformat gemäß PKCS #12 [PKCS12]. Die Verschlüsselung der darin gespeicherten privaten Schlüssel muss mit dem Algorithmus DES-EDE3-CBC (168 Bit Schlüssellänge) erfolgen. Andere starke Algorithmen mit einer Schlüssellänge von mindestens 168 Bit sind ebenfalls zulässig.

Zur zusätzlichen Absicherung der Schlüsseldateien werden diese über einen verschlüsselten Kanal vom Card Management System an den Antragsteller übertragen. Die Übertragung erfolgt erst nach Authentifizierung des Antragsstellers mittels PKIBw-Chipkarte.

6.2.2. Aufteilung privater Schlüssel auf mehrere Personen

Ein Teilnehmer-Schlüssel kann nicht auf mehrere Personen aufgeteilt werden.

Private Schlüssel der BundeswehrCA werden in einem Hardware-Sicherheitsmodul gespeichert. Eine Aufteilung auf mehrere Personen ist nicht vorgesehen.

Zur Aktivierung von privaten Schlüsseln siehe Abschnitt 6.2.7.

6.2.3. Hinterlegung privater Schlüssel

Private Entschlüsselungsschlüssel von natürlichen Personen und Funktionen werden nach der Generierung im HSM von der BundeswehrCA verschlüsselt in einer Datenbank gespeichert (siehe Abschnitt 6.2.5). Die privaten Entschlüsselungsschlüssel werden als historische Schlüssel bei der Personalisierung von Nachfolge-Chipkarten für die gleiche Person bzw. Funktion

wiederhergestellt, soweit der Speicherplatz auf der Chipkarte ausreichend ist. Es werden maximal 16 historische Schlüsselpaare wiedergestellt. Die Wiederherstellung erfolgt ausschließlich auf eine Nachfolge-Chipkarte derselben Person bzw. Funktion oder auf eine Chipkarte für eine berechtigte Stelle im Rahmen des Compliance Prozesses.

Eine Wiederherstellung von privaten Schlüsseln an eine berechtigte Stelle von Nutzern der Bundeswehr (Teilnehmer aus den Verzeichnisdienstzweigen Militär, Zivil, Extern) erfolgt ausschließlich für das CERTBw, für Teilnehmer der BWI-Systeme (Teilnehmer aus dem Verzeichnisdienstzweig BWI-Systeme) für das CERT BWI und für Teilnehmer der BWI-IT (Teilnehmer aus dem Verzeichnisdienstzweig BWI-IT) für die Compliance-Abteilung der BWI-IT. Außerdem erfolgt die Wiederherstellung ausschließlich auf nicht auslesbare Chipkarten („Compliance-Karten“), wobei das Aushändigen der Chipkarte und das Übermitteln der PIN an zwei verschiedene verpflichtete Personen erfolgen muss. 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. Eine Prüfung der PKIBw auf das Vorliegen dieser Bedingungen erfolgt nicht.

Private Schlüssel von natürlichen Personen und Funktionen, die zur Authentisierung oder Signatur dienen, dürfen von der BundeswehrCA nicht gespeichert werden. Die Speicherung ist durch die Verfahrensweise der Schlüsselgenerierung auf der Karte technisch ausgeschlossen.

Eine Speicherung von Schlüsseldateien organisatorischer Einheiten und technischer Komponenten ist durch die BundeswehrCA für den Zeitraum der Auslieferung (bis der Schlüsselverantwortliche den Erhalt bestätigt hat) zulässig.

Die Datensicherung (Kopie) des CA-Schlüssels und die Datensicherung der Schlüsselverantwortlichen bei „Gruppenzertifikaten“ fällt nicht unter Hinterlegung, siehe Abschnitt 6.2.4.

6.2.4. Backup privater Schlüssel

Die Schlüsselverantwortlichen von Schlüsseln organisatorischer Einheiten und technischer Komponenten sind berechtigt, Kopien der Schlüsseldateien für Zwecke der Datensicherung anzufertigen.

Die BundeswehrCA muss Kopien aller ihrer Schlüssel anfertigen. Dabei darf eine Kopie nur von einem Hardware-Sicherheitsmodul auf ein zweites erfolgen. Die Aufbewahrung eines privaten Schlüssels außerhalb eines Hardware-Sicherheitsmoduls ist nicht zulässig. Ausgenommen hiervon sind die Schlüssel des Zeitstempeldienstes und derOCSP-Responder, von denen kein Backup erstellt wird, sondern welche bei Bedarf neu generiert werden können.

6.2.5. Archivierung privater Schlüssel

Private Schlüssel von natürlichen Personen und Funktionen, die zur Entschlüsselung dienen, werden in der Datenbank der BundeswehrCA gespeichert. Darüber hinaus werden keine anderen privaten Schlüssel archiviert, insbesondere werden keine Authentisierungs- und Signaturschlüssel gespeichert.

Die Speicherung der o.g. Schlüssel erfolgt ausschließlich verschlüsselt mit einem symmetrischen Archivierungsschlüssel (AES 256 Bit). Der symmetrische Archivierungsschlüssel selbst

wird wiederum mit einem asymmetrischen Archivierungsschlüssel (RSA 2048 Bit) verschlüsselt in der Datenbank der BundeswehrCA gespeichert. Die Generierung des asymmetrischen Archivierungsschlüssel (RSA 2048 Bit) erfolgt in einem Hardware Security Module (HSM) und ist nicht exportierbar.

Private Schlüssel der BundeswehrCA sind nach Einstellung des Betriebes des jeweiligen CA-Systems noch mindestens ein (1) Jahr in einem Hardware-Sicherheitsmodul aufzubewahren.

Zur Archivierung von Zertifikaten siehe Abschnitt 4.6.

6.2.6. Einbringung privater Schlüssel in ein kryptographisches Modul

Schlüssel zur Authentisierung und Signaturerstellung, die auf einem kryptographischen Modul gespeichert werden, werden in der PKIBw, Anteil Verwaltungs-PKI, grundsätzlich auf diesem Modul erzeugt. Eine Erzeugung dieser Schlüssel außerhalb des Moduls mit anschließender Aufbringung findet nicht statt.

Die Schlüssel für Ver- und Entschlüsselung für Personen und Funktionen werden außerhalb der Chipkarte in einem HSM im KeyExport Modus generiert und anschließend auf die Chipkarte aufgebracht.

6.2.7. Methode zur Freischaltung / Aktivierung privater Schlüssel

Die Verwendung von privaten Schlüsseln der Teilnehmer erfordert eine Freischaltung des Schlüssels durch eine PIN (bei kryptographischen Hardware-Modulen) oder durch ein Passwort (bei Nutzung von Schlüsseldateien).

Die Nutzung von privaten Schlüsseln auf Chipkarten, die an Teilnehmer ausgegeben werden, muss die Eingabe einer PIN erfordern, die nur dem Teilnehmer bekannt ist (siehe Abschnitt 6.4). Ausnahme: der Schlüsselverantwortliche für Funktionen darf die PIN dem jeweiligen Nutzer der funktionsbezogenen Chipkarte nach Verpflichtung mitteilen,

Die Nutzung von privaten Schlüsseln, die als Schlüsseldatei ausgegeben wurden, muss durch die Anwendung, in die die Schlüsseldatei eingebracht wird, eingeschränkt werden. Dies ist anwendungsabhängig. Die PKIBw fordert,

- dass die Schlüssel in der Anwendung verschlüsselt abgespeichert werden, wobei der gleiche oder ein gleichwertiger Algorithmus zum Einsatz kommen muss, wie zur Verschlüsselung der Schlüsseldatei und

- der Schlüssel für die Verschlüsselung des von der PKIBw, Anteil Verwaltungs-PKI, ausgegebenen privaten Schlüssels aus einem Passwort abgeleitet wird, das zur Nutzung des Schlüssels einzugeben ist.

Zur Aktivierung von privaten Schlüsseln der BundeswehrCA müssen sich mehrere Operatoren (mindestens zwei) am Hardware-Sicherheitsmodul des CA-Systems anmelden. Weitere Details sind dem projektbezogenen IT-Sicherheitskonzept PKIBw [IT-SichhK] zu entnehmen.

6.2.8. Methode zur Deaktivierung privater Schlüssel

Die Teilnehmer sind verpflichtet, ihre privaten Schlüssel so aufzubewahren und zu verwenden, dass eine missbräuchliche Nutzung durch Dritte ausgeschlossen ist. Beim Verlassen des Arbeitsplatzes sind Schlüsselträger aus dem System zu entfernen, bei Software-Schlüsseln sind die Programme, die Zugriff auf die Schlüssel haben, zu beenden. Danach darf eine Nutzung ohne erneute Eingabe des Passwortes nicht mehr möglich sein.

6.2.9. Methode zur Vernichtung privater Schlüssel

Private Schlüssel, die in Hardware-Sicherheitsmodulen der CA-Systeme gespeichert sind, sind über eine geeignete Funktion des Moduls zu vernichten.

Die Vernichtung privater Schlüssel in Chipkarten erfolgt formlos durch die Zerstörung des kontaktbehafteten Chips.

Die Schlüsselverantwortlichen sind verpflichtet, nicht mehr benutzte Schlüsseldateien entsprechend den Vorschriften der ZDv 54/100 und der ZDv 2/30 zu vernichten.

6.3. Weitere Aspekte zum Schlüsselmanagement

6.3.1. Archivierung öffentlicher Schlüssel

Die PKIBw, Anteil Verwaltungs-PKI, gibt öffentliche Schlüssel in Form von Zertifikaten aus. Verschlüsselungszertifikate sind während ihres Gültigkeitszeitraumes im Zentralen Verzeichnisdienst der Bundeswehr abrufbar. Nach Ablauf ihrer Gültigkeit oder bei Sperrung werden sie aus dem Zentralen Verzeichnisdienst der Bundeswehr entfernt. Zur Archivierung von Zertifikaten siehe Abschnitt 4.6.

6.3.2. Verwendungszeitraum öffentlicher und privater Schlüssel

In der PKIBw, Anteil Verwaltungs-PKI, sind private Signatur- und Authentisierungsschlüssel ausschließlich im Gültigkeitszeitraum des dazugehörigen Zertifikates, und solange dieses nicht gesperrt ist, zu verwenden. Private Schlüssel zur Entschlüsselung von Daten dürfen auch nach Ablauf oder Sperrung des dazugehörigen Zertifikates zur Entschlüsselung von Daten verwendet werden.

Die regulären Gültigkeitszeiträume der einzelnen Typen von Teilnehmerzertifikaten sind Tabelle 4 zu entnehmen. Der Gültigkeitszeitraum kann von der BundeswehrCA aus besonderen Gründen, die dem Antragsteller offen zu legen sind, kürzer festgelegt werden.

Zertifikatstyp	**Gültigkeitszeitraum maximal**
Zertifizierungsstelle	6 Jahre
Personen (PKIBw-Karte, eDA / eTA)	5 Jahre
Personen (temporäre PKI-Karte)	8 Wochen
Funktionen	5 Jahre
OrgEinheiten	3 Jahre

Zertifikatstyp	Gültigkeitszeitraum maximal
Technische Komponenten	1 Jahr
OCSP-Responder	6 Monate
TSS-Signatur	5 Jahre

Tabelle 4: Gültigkeitszeiträume von Zertifikaten

Die BundeswehrCA stellt ausschließlich Zertifikate aus, deren Gültigkeitszeitraum innerhalb des Gültigkeitszeitraumes ihres aktuellen Zertifizierungsstellen-Zertifikates liegt.

Die von der BundeswehrCA ausgestellten Zertifikate sind für die Gültigkeitsprüfung nach dem sog. Schalenmodell ausgelegt, wie es in [MTTv2Prof], Abs. 5.3 definiert ist. Danach ist ein Zertifikat zu einem Zeitpunkt gültig, wenn u. a. für jedes im Zertifizierungspfad enthaltene Zertifikat gilt, dass

- die Signatur mathematisch korrekt ist,
- das Zertifikat für den vorgesehenen Verwendungszweck zugelassen ist (dies bedeutet, dass insbesondere alle kritischen Erweiterungen die für sie definierten Prüfungen bestanden haben müssen),
- das Zertifikat zum betrachteten Zeitpunkt nicht in einer Sperrliste des Ausstellers enthalten ist (ausgenommen hiervon ist das Root-Zertifikat) und
- der betrachtete Zeitpunkt innerhalb des Gültigkeitszeitraumes (der Zeitraum, der durch die Felder *notBefore* und *notAfter* angegeben wird) des Zertifikates liegt.

6.4. Aktivierungsdaten

6.4.1. Erzeugung und Installation der Aktivierungsdaten

6.4.1.1. Aktivierungsdaten für Schlüssel der Zertifizierungsstellen

Die Schlüssel der BundeswehrCA können nur nach der Aktivierung durch mehrere, mindestens jedoch zwei, berechtigte Personen am HSM verwendet werden.

Die zur Anmeldung am HSM benötigten Aktivierungsdaten werden bei der Inbetriebnahme erzeugt. Dabei ist jeder berechtigten Person eine individuelle PIN zuzuweisen.

6.4.1.2. Aktivierungsdaten für Schlüssel der Teilnehmer

Die PIN und der PUK der Chipkarten, die an Personen bzw. Schlüsselverantwortliche für Funktionen ausgegeben werden, werden bei der Personalisierung erzeugt und innerhalb der gesicherten Räumlichkeiten der BundeswehrCA in die Chipkarte eingebracht.

Die erzeugten PIN und PUK bestehen aus jeweils acht zufällig erzeugten Ziffern. Der Erzeugungsvorgang, das Einbringen von PIN und PUK auf die Karte und die Erzeugung des elektronischen PIN/PUK-Briefes (Regelfall) bzw. der Druck von papierbasierten PIN/PUK-Briefen

(Ausnahmefall) sind so ausgelegt, dass eine Kenntnisnahme der PIN bzw. des PUK durch unbefugte Personen unmöglich ist.

Für Chipkarten, die an Personen ausgegeben werden, werden die PIN/PUK-Briefe als Passwort-verschlüsselte PDF-Datei elektronisch bereitgestellt. Der Antragsteller authentisiert sich am CMS mittels ZVDBw Passwort und lädt den verschlüsselten PIN/PUK-Brief herunter. Die Entschlüsselung des PIN/PUK-Briefes ist nur mit dem auf der Empfangsbestätigung zufällig generierten Passwort möglich. Nachdem der LRA-Mitarbeiter die Übergabe der Chipkarte im CMS bestätigt hat, erfolgt der automatische Versand einer E-Mail an den Teilnehmer mit der Information, dass der elektronische PIN/PUK-Brief zum Download verfügbar ist. Nur in Ausnahmefällen, wenn der Antragsteller keinen Zugang zum CMS besitzt, werden die PIN/PUK-Briefe in Papierform an den Antragsteller versendet.

Für funktionsbezogene Chipkarten werden die PIN/PUK-Briefe mit dem Anmeldezertifikat des Schlüsselverantwortlichen verschlüsselt und elektronisch im CMS bereitgestellt. Die PIN/PUK-Briefe können nach Bestätigung des Karteneingangs vom SV im CMS direkt heruntergeladen werden.

Nach erfolgreichem Download bzw. Druck des PIN/PUK-Briefes werden PIN und PUK in den Systemen des TrustCenterBw gelöscht. Es findet keine weitere Speicherung von PIN und PUK statt.

Die Passwörter zur Verschlüsselung der Schlüsseldateien für OrgEinheiten und technische Komponenten werden während der Erzeugung der Schlüsseldateien ausgewählt.

Die Passwörter werden zufällig erzeugt und müssen aus einer Folge von Zahlen, Ziffern und Sonderzeichen bestehen. Sie werden bis zur Übermittlung an den Antragsteller verschlüsselt gespeichert. Einzelheiten regelt das projektbezogene IT-Sicherheitskonzept PKIBw [IT-SichhK].

6.4.2. Schutz der Aktivierungsdaten

6.4.2.1. Aktivierungsdaten für Schlüssel der Zertifizierungsstellen

Die Mitarbeiter der BundeswehrCA, die über Aktivierungsdaten verfügen, verpflichten sich, diese sicher aufzubewahren und niemand zugänglich zu machen.

6.4.2.2. Aktivierungsdaten für Schlüssel der Teilnehmer

Die PIN und der PUK sind auf der Chipkarte gegen Auslesen geschützt. Ein unbemerktes Lesen von PIN und PUK vor deren Übergabe an den Teilnehmer wird verhindert, weil

- der elektronische PIN/PUK-Brief als Passwort-geschützte PDF-Datei symmetrisch verschlüsselt ist bzw.

- der elektronische PIN/PUK-Brief für funktionsbezogene Chipkarten als PDF-Datei mit dem persönlichen Zertifikat des Schlüsselverantwortlichen verschlüsselt ist oder

- der papierbasierte PIN/PUK-Brief eine unbefugte Einsichtnahme verhindert. Stellt der Teilnehmer eine Beschädigung an seinem PIN/PUK-Brief fest, so hat er dies umgehend der zentralen Registrierungsstelle zu melden und die zugehörige Chipkarte nicht zu verwenden.

Die Passwörter für Schlüsseldateien werden bis zur Auslieferung an den Antragsteller verschlüsselt gespeichert. Die Übermittlung an den Antragsteller erfolgt mittels eines mit dessen PKIBw-Zertifikat verschlüsselten elektronischen PIN/PUK-Briefs. Der Antragsteller lädt den verschlüsselten, elektronischen PIN/PUK-Brief nach Authentifizierung über das CMS herunter.

Die Teilnehmer werden verpflichtet, ihre PIN/PUK bzw. das Passwort gegenüber anderen Personen geheim zu halten, Sperrkennwörter müssen zur Authentisierung einer Sperrung dem Personal der BundeswehrCA mitgeteilt werden.

6.4.3. Weitere Aspekte zu den Aktivierungsdaten

Der Inhaber einer Chipkarte hat die Möglichkeit seine PIN auf eine beliebige Zahlenkombination zu ändern. Dazu ist die Eingabe der alten PIN erforderlich.

6.5. Sicherheitsbestimmungen für IT-Systeme

Auf allen IT-Systemen, die in der BundeswehrCA und in den Registrierungsstellen zum Einsatz kommen, müssen die Sicherheitsmaßnahmen für IT-BasisschutzBw gemäß ZDv 54/100 umgesetzt sein. Weitergehende Maßnahmen sind in dem projektbezogenen Sicherheitskonzept PKIBw [IT-SichhK] beschrieben.

6.6. Sicherheitselemente im Produkt-Lebenszyklus

6.6.1. Systementwicklung

Die Bundeswehr IT-Standards müssen berücksichtigt werden.

6.6.2. Sicherheitsmanagement

Auf allen Systemen der Zertifizierungs- und der zentralen Registrierungsstelle darf nur Hard- und Software zum Einsatz kommen, die für die Erfüllung der Aufgabe des Systems notwendig ist. Für jedes IT-System ist ein Protokollbuch zu führen, in dem die eingesetzte Hard- und Software (inkl. Versionsständen) sowie Änderungen an diesen dokumentiert sind (siehe auch Abschnitt 4.6).

Zusätzlich muss ein System eingesetzt werden, dass unbefugte Änderungen an den Programmen, die zur Aufgabenerfüllung notwendig sind, erkennbar machen kann. Eine Überprüfung hat bei Systemstart und in regelmäßigen Abständen zu erfolgen.

Bei der Installation vom Hersteller gelieferter Software-Komponenten ist die Authentizität und Integrität der gelieferten Software vom Hersteller sicherzustellen.

6.7. Vorkehrungen zur Wahrung der Netzwerksicherheit

Durch die Automatisierung der Antrags- und Zertifizierungsprozesse sind die Systeme der Zertifizierungs- und der zentralen Registrierungsstelle vernetzt. Um die Systeme vor unberechtigtem Zugriff zu schützen, sind die Systeme der Zertifizierungsstelle und die Produk-tionsarbeitsplätze der zentralen Registrierungsstelle in einem vom restlichen Rechenzentrumsnetz getrennten Netz zu betreiben. Die Schnittstelle ist durch einen geeigneten Übergang abzusichern.

Ein direkter Zugriff auf die Systeme der BundeswehrCA darf von außerhalb der zentralen PKIBw Systeme nicht möglich sein. Der Zugriff auf die Systeme der zentralen Registrierungsstelle muss auf die Systeme und Personen beschränkt sein, die von außerhalb der zentralen Registrierungsstelle auf diese zugreifen müssen (z. B. auf Mitarbeiter der lokalen Registrierungsstellen). Gegebenenfalls ist der Zugriff netzwerkseitig zusätzlich abzusichern.

Weitere Einzelheiten sind im projektbezogenen IT-Sicherheitskonzept PKIBw [IT-SichhK] beschrieben.

6.8. Sicherheitsvorkehrungen bei der Entwicklung des kryptographischen Moduls

Siehe Abschnitt 6.6.1.

7. Zertifikats- und Sperrlisten-Profil

Der Aufbau und der Inhalt von Zertifikaten und Sperrlisten, die in der PKIBw, Anteil Verwaltungs-PKI, erstellt und ausgegeben werden, ist in dem Namenskonzept [Namen] dargestellt.

8. Verwaltung dieser Richtlinie

8.1. Verfahren zur Änderung dieses Dokuments

Die PMABw prüft dieses Dokument mindestens einmal jährlich auf Aktualität. Die PMABw stellt auf und veröffentlicht einen Änderungsplan, der beabsichtigte Änderungen an dieser Zertifizierungsrichtlinie beschreibt.

Das sonstige Änderungsmanagement wird wie folgt definiert:

- Alle Änderungen der Zertifizierungsrichtlinie, die von der PMABw erwogen werden, sind an einen Teilnehmerkreis, der von der PMABw festgelegt wird, mindestens einen Monat vor der Änderungsentscheidung zu verteilen.

- Änderungsvorschläge zu dieser Zertifizierungsrichtlinie sind in schriftlicher Form an die in Abschnitt 1.4.2 genannte(n) Person(en) zu richten. Diese Vorschläge müssen eine Beschreibung der Änderung, eine Änderungsbegründung und die Erreichbarkeitsdaten der vorschlagenden Person beinhalten. Die Vorschläge werden geprüft und ggf. an die PMABw weitergeleitet.

- Die PMABw prüft eingehende Änderungsvorschläge und entscheidet über deren Einbindung in die aktuelle Zertifizierungsrichtlinie.

- Eine aktualisierte Version der Zertifizierungsrichtlinie wird erstellt und von der PMABw verabschiedet.

- Die verabschiedete Zertifizierungsrichtlinie wird veröffentlicht.

Änderungen dürfen ohne Bekanntmachung erfolgen, wenn diese keine Auswirkungen auf die Sicherheit haben und keine Änderungen der Abläufe auf Seite der Teilnehmer (Registrierung, Prüfung von Zertifikaten, Sperrungen etc.) erfordern.

Änderungen, welche die Sicherheit oder die Abläufe der Teilnehmer betreffen, erfordern eine Veröffentlichung der Zertifizierungsrichtlinie. Insbesondere sind dies Änderungen bei Abläufen zur:

- Sperrung von Zertifikaten,

- Registrierung von Teilnehmern,

- Personalisierung von Schlüsselträgern

sowie

- dem Schlüssel- und Zertifikatsmanagement,

- dem Verzeichnis- und Auskunftsdienst,

- Verpflichtungen, Haftungsregelungen und der finanziellen Verantwortung.

Bei Änderungen, die eine Bekanntmachung erfordern, ist die Kennung (OID) der Zertifizierungsrichtlinie zu ändern. Zertifikate enthalten jeweils die Kennung (OID) der Zertifizierungsrichtlinie, die zum Zeitpunkt der Zertifikatserstellung gültig ist.

8.2. Verfahren zur Publizierung und Bekanntgabe

Die aktualisierte Fassung dieser Zertifizierungsrichtlinie wird über das in Abschnitt 2.6.1 beschriebene Verfahren veröffentlicht. Ältere Versionen sind weiter abrufbar zu halten.

Darüber hinaus sind die Zertifizierungs- und alle Registrierungsstellen darüber zu benachrichtigen, dass eine aktualisierte Fassung dieser Zertifizierungsrichtlinie vorliegt und anzuwenden bzw. umzusetzen ist.

Die PMABw ist verantwortlich für die Publizierung der jeweils aktuellen Version dieser Zertifizierungsrichtlinie.

8.3. Genehmigung und Eignung einer CPS

Bei Änderungen an dieser Zertifizierungsrichtlinie, ist die Verträglichkeit mit den nachfolgend genannten Dokumenten zu prüfen und ggf. eine Anpassung dieser einzuleiten.

- Organisationshandbuch [OrgHdb]
- Rollenkonzept [Rollen]
- Namenskonzept [Namen]
- Projektbezogenes IT-Sicherheitskonzept PKIBw [IT-SichhK]

Sollte diese Zertifizierungsrichtlinie und eines der vorstehenden Dokumente widersprüchliche Angaben enthalten, ist durch die PMABw eine Anpassung des betroffenen Dokumentes unverzüglich einzuleiten, ggf. ist eine vorübergehende Handlungsanweisung für Mitarbeiter der PKIBw, Anteil Verwaltungs-PKI, zu erlassen.

Die Zertifizierungs- und Registrierungsstellen der PKIBw, Anteil Verwaltungs-PKI, sind über Änderungen an diesen Dokumenten oder über vorübergehende Handlungsanweisungen umgehend zu informieren.

9. Referenzen

AusbiKo	Ausbildungskonzept; in der jeweils aktuellen Fassung
BSIAnl1	Selbsterklärung der Zertifizierungsstelle, Anlage 1 zum Vertrag über die Teilnahme an der PKI-1-Verwaltung; Version 3.00
BSIPolicy	Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung; Bundesamt für Sicherheit in der Informationstechnik; Version 3.2 vom 09.01.2003
NutzerLF	PKIBw Nutzerleitfaden für Chipkarten; in der jeweils aktuellen Fassung
KrypAlgo14	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen; 13. Januar 2014
MTTv2Prof	MailTrust Version 2; Profile für Zertifikate und Sperrlisten; J. Biester, F. Bauspiess, D. Fox; 16.03.1999
Namen	Namenskonzept und Zertifikatsprofil für die Public Key Infrastructure der Bundeswehr (PKIBw); in der jeweils aktuellen Fassung
OrgHdb	Organisationshandbuch für die Public Key Infrastructure der Bundeswehr (PKIBw), Anteil Verwaltungs-PKI; in der jeweils aktuellen Fassung
PKCS10	PKCS #10: Certification Request Syntax Standard; RSA Laboratories; Version 1.7, 26.05.2000
PKCS12	PKCS #12: Personal Information Exchange Syntax; RSA Laboratories; Version 1.0, 24.06.1999
RFC2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework; S. Chokhani, W. Ford; März 1999
Rollen	Rollenkonzept für die Public Key Infrastructure der Bundeswehr (PKIBw); in der jeweils aktuellen Fassung
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften; 16.05.2001
IT-SichhK	Projektbezogenes IT-Sicherheitskonzept für die Public Key Infrastructure der Bundeswehr (PKIBw); in der jeweils aktuellen Fassung

10. Abkürzungsverzeichnis

BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr
BMVg	Bundesministerium der Verteidigung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority, dt. Zertifizierungsstelle
CC	Common Criteria
CMS	Card Management System
CPS	Certification Practice Statement
CRA	Central Registration Authority, dt. zentrale Registrierungsstelle
CRL	Certificate Revocation List, dt. Sperrliste
DNS	Domain Name Server
Dst	Dienststelle
EAL	Evaluation Assurance Level
eDA / eTA	elektronischer Dienst- / Truppenausweis
HSM	Hardware Security Module
IT-SiBe	IT-Sicherheitsbeauftragte/r
KGS	Key Generation System
KoordGrp	Koordinierungsgruppe
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority, dt. lokale Registrierungsstelle
OCSP	Online Certificate Status Protocol, dt. Online-Statusabfrage
OID	Object Identifier, dt. Objektkennung
OrgEinheit	organisatorische Einheit
PCA	Policy Certification Authority
PersDat	Personenbezogene Daten

PIN	Persönliche Identifikationsnummer
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure, dt. Zertifizierungsinfrastruktur
PKIBw	Public Key Infrastructure der Bundeswehr
PMABw	PKI Management Authority der Bundeswehr
PUK	PIN Unblock Key
RA	Registration Authority, dt. Registrierungsstelle
RSA	Rivest, Shamir, Adleman
SchutzInfo	Sonstige schutzbedürftige Informationen
SHA-1	US Secure Hash Algorithm 1
SigG	Signaturgesetz
SigV	Signaturverordnung
SINA	Sichere Inter-Netzwerk Architektur
TSS	Timestampservice, dt. Zeitstempeldienst
VS	Verschlusssache
WBV	Wehrbereichsverwaltung