Certificate Policy (CP)

Sana Kliniken Berlin-Brandenburg Corporate PKI

OID: 1.3.6.1.4.1.36444.100.1.1.6
Version: 1.6

Inhalt

1 Einleitung

Die Sana Kliniken Berlin-Brandenburg GmbH stellt sowohl organisationsintern als auch -extern Dienste und Anwendungen bereit, die im Hinblick auf die Natur der verarbeiteten, genutzten und übertragen Daten einen zum Teil hohen Schutzbedarf aufweisen. Um diesen Schutzbedarf durch Maßnahmen angemessen zu adressieren, betreibt die Sana Kliniken Berlin-Brandenburg GmbH eine Public Key Infrastruktur.

1.1 Überblick

Die Gliederung des vorliegenden Dokuments orientiert sich an den in [RFC3647] getroffenen Empfehlungen zur Erstellung von Certificate Policies und Certification Practice Statements.

1.2 Identifikation des Dokuments

Bezeichnung:	Certificate Policy der Sana Kliniken BB PKI
Version:	1.6
Objekt Identifier:	1.3.6.1.4.1.36444.100.1.1.6

{ iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) Sana IT Services GmbH Berlin-Brandenburg(36444) pki(100) cp(1) major-version(1) minor-version(6) }

1.3 Bestandteile der Zertifizierungsinfrastruktur

1.3.1 Zertifizierungsstellen (CA)

Die Zertifizierungsstellen sind für das Ausstellen von Zertifikaten innerhalb der Sana Kliniken Berlin-Brandenburg Zertifizierungsinfrastruktur verantwortlich.

Root CA
Die Sana Kliniken Berlin-Brandenburg Root CA darf ausschließlich Zertifikate für untergeordnete Sub CAs ausstellen. End Entity Zertifikate dürfen durch sie hingegen nicht ausgestellt werden.

Sub CA
Sub CAs stellen Zertifikate für End Entities aus.

1.3.2 Registrierungsstellen (RA)

Registrierungsstellen sind für die Überprüfung der Identität von potentiellen Zertifikatnehmern verantwortlich. Jeder CA ist mindestens eine RA zugeordnet.

1.3.3 Zertifikatnehmer

Zertifikatnehmer repräsentieren natürliche oder juristische Personen für die Zertifikate nach den innerhalb dieses Dokuments definierten Vorgaben ausgestellt werden.

1.3.4 Zertifikatprüfer

Zertifikatprüfer repräsentieren natürliche oder juristische Personen die unter Zuhilfenahme ausgestellter Zertifikate, Zertifikatsperllisten und Zertifikatstatusinformationen die Identität und Authentizität eines Zertifikatnehmers prüfen.

1.3.5 Andere

Andere Teilnehmer (z. B. natürliche oder juristische Personen) können bei Bedarf als Dienstleister in die Abläufe innerhalb der Zertifizierungsinfrastruktur eingebunden werden.

1.4 Zertifikatnutzung

1.4.1 Zulässige Zertifikatnutzung

Die ausgestellten End Entity Zertifikate dürfen ausschließlich im Rahmen der Kommunikation mit der Sana Kliniken Berlin-Brandenburg GmbH für die im Zertifikat angegebenen Zwecke (KeyUsage, ExtendedKeyUsage) verwendet werden.

1.4.2 Nicht-zulässige Zertifikatnutzung

Eine Nutzung der Zertifikate außerhalb der in Abschnitt 1.4.1 definierten Kontexte ist nicht zulässig.

1.5 Policy Verwaltung

1.5.1 Verantwortliche Organisation

Die Verwaltung und Pflege dieser Certificate Policy erfolgt durch die Sana Kliniken Berlin-Brandenburg GmbH.

1.5.2 Ansprechpartner

Die Ansprechpartner für dieses Dokument können auf folgendem Wege erreicht werden:

Adresse: Sana Kliniken BB PKI
Matthias Grusdat
Fanningerstr. 32
10365 Berlin

Telefon: 030 / 5518-4545
E-Mail: pki@sana-bb.de

1.5.3 Prüfung von Certification Practice Statements (CPS)

Die Prüfung entsprechender CPS unterliegt den in Abschnitt 1.5.2 benannten Ansprechpartnern.

1.5.4 Genehmigungsverfahren für Certification Practice Statements (CPS)

Die Genehmigung entsprechender CPS unterliegt den in Abschnitt 1.5.2 benannten Ansprechpartnern.

1.6 Definitionen und Abkürzungen

Für das Verständnis dieses Dokuments relevante Definitionen und Abkürzungen können dem Glossar entnommen werden.

2 Veröffentlichungen und Informationsdienste

2.1 Informationsdienste

Jede Zertifizierungsstelle der Sana Kliniken BB PKI stellt mindestens einen Informationsdienst bereit, der folgende Informationen bereitstellt:

- Certificate Policy (CP) der Sana Kliniken BB PKI
- Certification Practice Statement (CPS) der CA
- Zertifikat der übergeordneten CA und dessen Fingerabdruck
- Zertifikat der CA und dessen Fingerabdruck
- Verweis auf Informationsdienste zum Abruf von Zertifikatsstatusinformationen und Sperrlisten der CA sowie der übergeordneten Root CA
- Kontaktinformationen für die Beantragung einer Zertifikatssperrung

2.2 Veröffentlichung von Zertifizierungsinformationen

Die Veröffentlichung der in Abschnitt 2.1 benannten Informationen erfolgt über die in dem entsprechenden CPS benannten Informationsdienste.

2.3 Aktualisierung von Zertifizierungsinformationen

Die Aktualisierung der Informationen in den entsprechenden Informationsdiensten erfolgt innerhalb der folgenden Fristen:

CP und CPS:	Eine Woche nach Erstellung einer neuen Version
Zertifikate:	Fünf Tage nach Erstellung
CRL:	vgl. Abschnitt 4.9

2.4 Zugriffssteuerung

Ein lesender Zugriff auf die entsprechenden Informationsdienste muss für alle an der PKI teilnehmenden Akteure ohne vorherige Zugriffskontrolle möglich sein.

Zugriffe die Veränderungen an den Inhalten der Informationsdienste vornehmen, dürfen durch entsprechende Zugriffssteuerungsmechanismen ausschließlich einem klar abgrenzbaren autorisierten Personenkreis möglich sein.

3 Identifizierung und Authentifizierung

3.1 Namenskonventionen

Die geltenden Namenskonventionen variieren je nach Art des ausgestellten Zertifikats. Entsprechende Vorgaben können den aktuellen Zertifikatsprofilen entnommen werden.

3.2 Identifizierung und Authentifizierung bei initialer Zertifikatsbeantragung

3.2.1 Besitzprüfung für private Schlüssel

Private Schlüssel dürfen ausschließlich zentral innerhalb der CA generiert werden. Eine Besitzprüfung ist daher nicht notwendig.

3.2.2 Identifizierung von Organisationen

Die Beantragung von Zertifikaten für Organisationen darf ausschließlich durch natürliche Personen erfolgen. Für diese gelten die in Abschnitt 3.2.3 formulierten Anforderungen. Die Zugehörigkeit der Person zur entsprechenden Organisation muss mithilfe aussagekräftiger Nachweise bescheinigt werden.

3.2.3 Identifizierung von natürlichen Personen

Natürliche Personen müssen durch einen angemessen vertrauenswerten Lichtbildausweis (Personalausweis, Reisepass, Führerschein, Kreditkarte mit Foto, Dienstpässe, zukünftig auch HBA etc.) identifiziert werden.

3.3 Identifizierung bei Zertifikatserneuerung

Die Authentifizierung einer Person bei einer Zertifikatserneuerung kann unter Zuhilfenahme eines gültigen dieser Person zugeordneten Zertifikats erfolgen. Gesperrte Zertifikate können nicht genutzt werden.

3.4 Identifizierung und Authentifizierung bei Zertifikatssperrung

Die einer Zertifikatssperrung vorausgehende Authentifizierung des Zertifikatsinhabers kann auf folgenden Wegen erfolgen:

- Mitteilung einer vereinbarten Authentisierungsinformation über beliebige Kommunikationswege (Telefon, schriftlich, elektronisch etc.)

- Persönliche Übergabe eines Sperrantrags

4 Ablauforganisation

4.1 Zertifikatantrag

4.1.1 Zertifikatbeantragung

Beliebige natürliche oder juristische Personen, die - insbesondere durch die Nutzung von bereitgestellten Dienste und Anwendungen - in einer direkten Beziehung zur Sana Kliniken Berlin-Brandenburg GmbH stehen, können Zertifikate beantragen. Der zulässige Personenkreis kann durch die Anforderungen spezifischer CPS weiter eingeschränkt werden.

4.1.2 Registrierungsprozess

Ausgangsbedingung für das Auslösen des Registrierungsprozesses ist das Einreichen eines Antrags bei der zuständigen Registrierungsstelle. Nach erfolgtem Eingang werden folgende Schritte durchlaufen und angemessen dokumentiert:

– Prüfung des Antrags hinsichtlich der Vollständigkeit und Korrektheit
– Festlegung eines eindeutigen DN

Die Übermittlung der entsprechenden Informationen an die Zertifizierungsstelle darf ausschließlich auf sicherem elektronischem Wege erfolgen.

4.2 Bearbeitung von Zertifikatanträgen

4.2.1 Durchführung der Identifizierung und Authentifizierung

Die Durchführung der Identifizierung und Authentifizierung ist nicht verpflichtende Grundlage für die Bearbeitung von Zertifikatsanträgen. Sie muss jedoch spätestens vor Veröffentlichung des Zertifikates bzw. der Weitergabe des zugehörigen Schlüsselmaterials verpflichtend erfolgen.

4.2.2 Annahme und Ablehnung von Zertifikatanträgen

Zertifikatanträge gelten nur dann als angenommen, wenn die in Abschnitt 4.1.2 definierten Prozessschritte erfolgreich durchlaufen wurden.

4.2.3 Bearbeitungsdauer

Die maximale Bearbeitungsdauer eines Zertifikatantrags darf den Zeitraum von einer Woche nicht überschreiten.

4.3 Zertifikatausstellung

4.3.1 Aktionen der Zertifizierungsstelle

Vor der Ausstellung muss die Zertifizierungsstelle die Berechtigung der RA, ein spezifisches Zertifikat zu genehmigen, in angemessener Form überprüfen.

4.3.2 Benachrichtigung des Zertifikatnehmers

Nach erfolgter Zertifikatsausstellung wird der Zertifikatnehmer informiert und das Zertifikat zusammen mit dem Schlüsselmaterial in geeigneter Weise an ihn übermittelt. Voraussetzung für die Übermittlung ist jedoch die in Abschnitt 3.2.3 beschriebene Identifizierung des Zertifikatnehmers.

4.4 Zertifikatakzeptanz

Es obliegt dem Zertifikatnehmer die im Zertifikat enthaltenen Informationen nach dessen Erhalt auf ihre Korrektheit zu überprüfen.

4.4.1 Annahme des Zertifikats

Ein Zertifikat gilt als angenommen oder akzeptiert, wenn der Zertifikatnehmer nach dessen Erhalt nicht innerhalb eines Zeitraums von 14 Tagen widersprochen hat. Mit der Annahme erklärt der Zertifikatnehmer die Korrektheit der im Zertifikat enthaltenen Informationen.

4.4.2 Veröffentlichung des Zertifikats durch die Zertifizierungsstelle

Wird der Veröffentlichung eines Zertifikats vorab nicht explizit durch den Zertifikatnehmer widersprochen, kann die Zertifizierungsstelle die Veröffentlichung in entsprechenden Informationsdiensten veranlassen.

4.4.3 Benachrichtigung zusätzlicher Instanzen durch die Zertifizierungsstelle

Die Benachrichtigung zusätzlicher Instanzen ist nicht vorgesehen. Abweichende Vorgaben können im CPS formuliert werden.

4.5 Verwendung von Schlüsselpaar und Zertifikat

4.5.1 Nutzung von privaten Schlüsseln und Zertifikaten durch Zertifikatnehmer

Der Zertifikatnehmer muss den angemessenen Schutz des dem Zertifikat zugeordneten privaten Schlüsselmaterials gewährleisten. Das Zertifikat darf ausschließlich für die in dieser Certificate Policy vorgesehenen Verwendungszwecke genutzt werden.

Der Zertifikatnehmer muss bei Verlust oder Kompromittierung des privaten Schlüssels sowie bei inkorrekten Zertifikatinhalten die Sperrung des Zertifikats veranlassen.

4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Zertifikatprüfer

Zertifikatprüfer müssen Sorge dafür tragen, dass sie vor Nutzung eines Zertifikats dessen Gültigkeit überprüfen.

4.6 Zertifikaterneuerung ohne Schlüsselwechsel

Eine Zertifikaterneuerung ohne Schlüsselwechsel ist nicht zulässig.

4.7 Zertifikaterneuerung mit Schlüsselwechsel

4.7.1 Gründe für eine Zertifikaterneuerung

Der Ablauf der Gültigkeit eines Zertifikats sowie die Kompromittierung eines Zertifikats stellen den einzigen Grund für eine Zertifikaterneuerung dar.

4.7.2 Wer kann eine Zertifikaterneuerung beantragen

Eine Zertifikaterneuerung kann durch den Zertifikatnehmer beantragt werden. Darüber hinaus sollte die entsprechende Zertifizierungsstelle eine aktive Zertifikaterneuerung unterstützen.

4.7.3 Ablauf der Zertifikaterneuerung

Die Zertifikaterneuerung orientiert sich an den in Abschnitt 4.3 beschriebenen Abläufen.

4.7.4 Benachrichtigung des Zertifikatnehmers

Es gelten die in Abschnitt 4.3.2 getroffenen Festlegungen.

4.7.5 Annahme einer Zertifikaterneuerung

Es gelten die in Abschnitt 4.4.1 getroffenen Festlegungen.

4.7.6 Veröffentlichung einer Zertifikaterneuerung

Es gelten die in Abschnitt 4.4.2 getroffenen Festlegungen.

4.7.7 Benachrichtigung zusätzlicher Instanzen bei einer Zertifikaterneuerung

Es gelten die in Abschnitt 4.4.3 getroffenen Festlegungen.

4.8 Zertifikatmodifikation

Eine Zertifikatmodifikation ist nicht vorgesehen. Es werden grundsätzlich nur neue Zertifikate mit neu generiertem Schlüsselmaterial ausgegeben.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Gründe für eine Zertifikatsperrung

Ist einer der nachfolgend genannten Umstände eingetreten, muss eine Zertifikatsperrung unverzüglich veranlasst werden:

- Verlust, Offenlegung oder anderweitige Kompromittierung des privaten Schlüsselmaterials
- Das Zertifikat enthält falsche oder nicht (mehr) gültige Informationen.
- Der Zertifikatnehmer ist nicht mehr zur Zertifikatnutzung berechtigt.
- Die Certificate Policy wird durch den Zertifikatnehmer nicht eingehalten.
- Der Zertifikatnehmer verlangt die Zertifikatsperrung.

– Die CA stellt ihren Betrieb ein

4.9.2 Wer kann eine Zertifikatsperrung beantragen

Eine Zertifikatsperrung kann durch den Zertifikatnehmer oder die Registrierungsstelle (RA) beantragt werden.

4.9.3 Ablauf einer Zertifikatssperrung

Nach erfolgreicher Authentifizierung des Zertifikatnehmers (vgl. Abschnitt 3.4) leitet die Registrierungsstelle den Sperrantrag an die zuständige Zertifizierungsstelle weiter. Dies gilt ebenfalls, wenn sie selbst den Sperrantrag stellt.

Die Zertifizierungsstelle prüft die Berechtigung der Registrierungsstelle einen entsprechenden Antrag einzureichen und führt nach erfolgreicher Überprüfung die Sperrung durch.

4.9.4 Fristen für die Stellung eines Sperrantrages

Ein Sperrantrag muss unverzüglich nach Eintreten einer der in Abschnitt 4.9.1 benannten Gründe gestellt werden.

4.9.5 Fristen für die Sperrung

Die Zertifizierungsstelle muss die Sperrung eines Zertifikates unverzüglich nach positiver Prüfung des entsprechenden Sperrantrages vornehmen.

4.9.6 Anforderungen zur Kontrolle der CRL durch den Zertifikatprüfer

Vgl. Abschnitt 4.5.2.

4.9.7 Häufigkeit von CRL-Veröffentlichungen

CRLs der Root CA müssen mindestens einmal pro Halbjahr erstellt und veröffentlicht werden. CRLs der Sub CAs müssen mindestens einmal pro Monat erstellt und veröffentlicht werden Erfolgt die Sperrung eines Zertifikats, muss eine entsprechend aktualisierte Sperrliste unverzüglich veröffentlicht werden.

4.9.8 Maximale Latenzzeit für die Veröffentlichung von CRLs

Zertifikatsperrlisten (CRL) müssen unverzüglich nach ihrer Erstellung veröffentlicht werden.

4.9.9 Verfügbarkeit von Online Sperr- und Statusüberprüfungsverfahren

In Ergänzung zur regelmäßigen Veröffentlichung von Zertifikatsperrlisten, muss ein Online Sperr- und Statusüberprüfungsverfahren implementiert sein.

4.9.10 Anforderungen an Online Sperr- und Statusüberprüfungsverfahren

Es gelten die in Abschnitt 4.9. formulierten Anforderungen.

4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrungen

Andere Formen der Bekanntmachung von Zertifikatsperrungen sind nicht vorgesehen.

4.9.12 Kompromittierung von privaten Schlüsseln

Wird die Kompromittierung eines privaten Schlüssels festgestellt, muss die Sperrung des assoziierten Zertifikats unverzüglich veranlasst werden.

4.9.13 Suspendierungsgründe

Das zeitliche Aussetzen der Gültigkeit von Zertifikaten ist nicht zulässig.

4.10 Dienst zur Statusabfrage von Zertifikaten

Die Verfahrensweise sowie die Ausprägung von Diensten zur Statusabfrage von Zertifikaten (z. B. über OCSP) sind dem entsprechenden Certification Practice Statement (CPS) zu entnehmen.

4.11 Beendigung der Zertifikatnutzung durch den Zertifikatnehmer

Die Zertifikatnutzung durch den Zertifikatnehmer gilt entweder nach Sperrung oder Ablauf der Gültigkeit des Zertifikats für beendet.

4.12 Schlüsselhinterlegung und -wiederherstellung

4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

Wird die Schlüsselhinterlegung durch die entsprechende Zertifizierungsstelle angeboten, so ist das zugrundeliegende Verfahren im CPS zu dokumentieren.

4.12.2 Richtlinien und Praktiken zum Schutz von Sitzungsschlüsseln und deren Wiederherstellung

n. a.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnamen

Geeignete infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen müssen gewährleisten, dass der Betrieb der Public Key Infrastruktur in einem angemessen sicheren Rahmen erfolgt. Die in dieser Certificate Policy (CP) sowie dem entsprechenden Certification Practice Statement (CPS) beschriebenen Aspekte beschreiben diese Maßnahmen in groben Zügen. Eine detaillierte Auseinandersetzung erfolgt in einem entsprechenden PKI-Konzept.

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Konkrete infrastrukturelle Sicherheitsmaßnahmen müssen im Certification Practice Statement beschrieben werden.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Sicherheitsrelevante Rollen

Um den ordnungsgemäßen Betrieb der Zertifizierungsstelle zu gewährleisten muss mindestens zwischen den folgenden funktionalen Rollen unterschieden werden:

Rolle	Funktion	Kürzel
Teilnehmerservice		TS
Registrator		RG
CA-Mitarbeiter		CAO1
PIN-Geber		CAO2
Systemadministrator		SA
Systemoperator		SO
Revision		R
Sicherheitsbeauftragter		ISO

5.2.2 Erforderliche Anzahl von Personen je Tätigkeit

Für folgende Tätigkeiten gilt das Vier-Augen-Prinzip:

Tätigkeit	**Rollen**
Erzeugen von Schlüsselpaaren für CA-Zertifikate	CAO1 + CAO2
Starten von Prozessen zur Ausstellung von Zertifikaten und Sperrlisten	CAO1 + CAO2
Austausch von Hard- und Softwarekomponenten für die Zertifizierung	SA + CAO1

5.2.3 Identifizieren und Authentifizieren von Rollen

Der Zutritt zu den IT-Systemen der Zertifizierungsstelle muss durch angemessene Sicherheitsmaßnahmen reglementiert werden. Der Zugang zu den Systemen der Zertifizierungsstelle muss durch angemessene Verfahren, jedoch mindestens Benutzername und Kennwort geschützt werden. Identifizierung und Authentifizierung müssen sich dabei nach den Anforderungen des in Abschnitt 5.2.1 beschriebenen Rollenmodells richten.

5.2.4 Trennung von Rollen

Die folgenden Rollen dürfen nicht in einer Person vereint werden.

	TS	RG	CAO1	CAO2	SA	S	R	ISO
TS - Teilnehmerservice	-				X	X	X	X
RG – Registrator		-			X	X	X	X
CAO1 – CA-Mitarbeiter			-	X	X	X	X	X
CAO2 – PIN Geber			X	-			X	X
SA – Systemadministrator	X	X	X		-		X	X
SO – Systemoperator	X	X	X			-	X	X
R – Revision	X	X	X	X	X	X	-	
ISO - SIcherheitsbeauftragter	X	X	X	X	X	X		-

5.3 Personelle Sicherheitsmaßnahmen

Konkrete personelle Sicherheitsmaßnahmen müssen im Certification Practice Statement beschrieben werden.

5.4 Sicherheitsüberwachung

Konkrete Maßnahmen zur Sicherheitsüberwachung müssen im Certification Practice Statement beschrieben werden.

5.5 Archivierung

Konkrete Maßnahmen zur Archivierung müssen im Certification Practice Statement beschrieben werden.

5.6 Schlüsselwechsel

Es gelten die an Kapitel 4.6 und 4.7 getroffen Aussagen.

5.7 Kompromittierung und Wiederherstellung

5.7.1 Prozeduren bei Sicherheitsvorfällen und Kompromittierung

Die Prozeduren und Abläufe bei Sicherheitsvorfällen während des PKI-Betriebs sind in gesonderten Dokumenten schriftlich zu fixieren. Eine Version dieses Dokuments ist an sämtliche Mitarbeiter der Zertifizierungsstelle auszuhändigen.

5.7.2 Prozeduren bei IT-Systemen

Der Betrieb fehlerhafter oder kompromittierter IT-Systeme, die direkten Einfluss auf den Betrieb der Zertifizierungsstelle besitzen, ist untersagt. Betroffene Systeme sind unverzüglich aus der Infrastruktur zu entfernen. Auf etwaige Auswirkungen der Kompromittierung ist unverzüglich mit den notwendigen Maßnahmen (Sperrung von Zertifikaten etc.) zu reagieren.

5.7.3 Kompromittierung von privaten Schlüsseln

Bei Kompromittierung des Schlüsselmaterials von Zertifikatnehmern muss eine Sperrung des mit dem Schlüsselmaterial assoziierten Zertifikats entsprechend Abschnitt 4.9 erfolgen.

Bei Kompromittierung des Schlüsselmaterials einer Zertifizierungsstelle muss eine Sperrung des Zertifizierungsstellenzertifikats sowie aller von dieser CA ausgestellten Zertifikate erfolgen. Betroffene Zertifikatnehmer sind zu informieren.

5.7.4 Betrieb nach einer Katastrophe

Entsprechende Maßnahmenkataloge für den Betrieb nach einer Katastrophe müssen Bestandteil eines Notfallkonzeptes sein.

5.8 Einstellung des Betriebs

Bei Einstellung des CA-Betriebs müssen folgende Maßnahmen ergriffen werden:

- Information aller Zertifikatnehmer, Registrierungsstellen und Kontaktpersonen
- Sperrung aller ausgegebenen Zertifikate
- Sichere Zerstörung des Schlüsselmaterials der Zertifizierungsstelle

6 Technische Sicherheitsmaßnahmen

Geeignete technische Sicherheitsmaßnahmen müssen gewährleisten, dass der Betrieb der Public Key Infrastruktur in einem angemessen sicheren Rahmen erfolgt. Die in dieser Certificate Policy (CP) sowie dem entsprechenden Certification Practice Statement (CPS) beschriebenen Aspekte beschreiben diese Maßnahmen in groben Zügen. Eine detaillierte Auseinandersetzung erfolgt in einem entsprechenden PKI-Konzept.

6.1 Schlüsselerzeugung und -installation

6.1.1 Schlüsselerzeugung

Die Schlüsselerzeugung muss in einem kryptografischen Modul der Zertifizierungsstelle erfolgen. Dieses Modul muss den Anforderungen entsprechend Abschnitt 6.2.1 genügen.

6.1.2 Übermittlung des privaten Schlüssels an den Zertifikatnehmer

Der private Schlüssel des Zertifikatnehmers ist während der Übermittlung angemessen zu schützen. Das Verfahren muss im CPS dargestellt werden.

6.1.3 Übermittlung des öffentlichen Schlüssels an den Zertifikatausssteller

n. a.

6.1.4 Übermittlung des öffentlichen CA-Schlüssels

Öffentliche Schlüssel der Zertifizierungsstelle können über die in Kapitel 2 beschriebenen Informationsdienste abgerufen werden.

6.1.5 Schlüssellängen

Die gültigen Mindestschlüssellängen sind den entsprechenden Zertifikatsprofilen zu entnehmen.

6.1.6 Parameter der öffentlichen Schlüssel und Qualitätssicherung.

n. a.

6.1.7 Verwendungszweck der Schlüssel und Beschränkung

n. a.

6.2 Schutz des privaten Schlüssels und Umgang mit kryptografischen Modulen

Zertifizierungsstellen, die auf vernetzten IT-Systemen betrieben werden, müssen das private Schlüsselmaterial in einem dedizierten kryptografischen Modul (Hardware Security Module) aufbewahren.

6.2.1 Standard des kryptografischen Moduls

Das zum Einsatz kommende kryptografische Modul muss einem der folgenden Standards genügen:

- Federal Information Processing Standard (FIPS) 140-2 Level 2
- Common Criteria (CC) EAL4+
- Information Technology Security Evaluation Criteria (ITSEC) E3

6.2.2 Kontrolle des privaten Schlüssels durch mehrere Personen

Sämtliche Zugriffe auf den privaten Schlüssel der Zertifizierungsstelle müssen dem Vier-Augen-Prinzip genügen.

6.2.3 Hinterlegung privater Schlüssel

Die Hinterlegung privater Schlüssel erfolgt nicht.

6.2.4 Backup privater Schlüssel

Das Backup privater Zertifizierungsstellenschlüssel darf ausschließlich in einer angemessen sicheren Umgebung aufbewahrt werden. (Tresor, Bankschließfach etc.) Das Schlüsselmaterial ist über eine auf mehrere Personen aufgeteilte PIN zu sichern. Kopien der einzelnen PIN Bestandteile sind getrennt voneinander in angemessen sicheren Umgebungen (Bankschließfach, Tresor, Notar etc.) zu verwahren.

Ein Backup privater Zertifikatnehmerschlüssel erfolgt nicht.

6.2.5 Archivierung privater Schlüssel

Vgl. Abschnitt 6.2.4

6.2.6 Transfer privater Schlüssel in ein kryptografisches Modul

Der nachträgliche Import von privatem Schlüsselmaterial - einer nicht an ein Netzwerk angeschlossenen Zertifizierungsstelle - in ein kryptografisches Modul entsprechend Abschnitt 6.2.1 ist zulässig.

6.2.7 Speicherung privater Schlüssel in einem kryptografischen Modul

Die Speicherung privater Schlüssel in kryptografischen Modulen muss verschlüsselt erfolgen.

6.2.8 Aktivierung privater Schlüssel

Die Aktivierung des privaten Schlüssels einer Zertifizierungsstelle muss nach dem Vier-Augen-Prinzip erfolgen. Die dafür notwendige PIN ist in zwei Hälften zu unterteilen.

6.2.9 Deaktivierung privater Schlüssel

n. a.

6.2.10 Vernichtung privater Schlüssel

Die Vernichtung des privaten Schlüssels einer Zertifizierungsstelle muss nach dem Vier-Augen-Prinzip erfolgen.

6.2.11 Güte des kryptografischen Moduls

Vgl. Abschnitt 6.2.1.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Vgl. Abschnitt 5.5.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Die Gültigkeit von Zertifikaten darf die in den Zertifikatprofilen angegebene Dauer nicht überschreiten. Die Gültigkeit des Schlüsselmaterials entspricht der Zertifikatgültigkeit.

6.4 Aktivierungsdaten

6.4.1 Aktivierungsdaten für Erzeugung und Installation

Folgende Anforderungen gelten für die zum Einsatz kommenden Aktivierungsdaten:

Root CA – Ausreichend komplexe Kombination aus alphanumerischen und Sonderzeichen – Mindestlänge = 15 Zeichen.

Sonstige - Ausreichend komplexe Kombination aus alphanumerischen und Sonderzeichen – Mindestlänge = 8 Zeichen.

6.4.2 Schutz der Aktivierungsdaten

Aktivierungsdaten müssen geheim gehalten werden. Sie dürfen ausschließlich Benutzern bekannt sein, die zertifizierungsstellen-relevante Funktionen entsprechend Abschnitt 5.2.1 ausüben.

6.4.3 Weitere Aspekte

n. a.

6.5 Sicherheitsmaßnahmen für Computer

6.5.1 Spezifische Anforderungen an technische Sicherheitsmaßnahmen

Ausschließlich speziell gehärtete IT-Systeme dürfen zum Einsatz kommen. Auf die Systeme zugreifende Nutzer müssen erfolgreich authentifiziert und autorisiert werden.

6.5.2 Güte und Qualität der Sicherheitsmaßnahmen

Die ausgewählten Sicherheitsmaßnahmen müssen angemessen sein und dem aktuellen Stand der Technik entsprechen.

6.6 Lebenszyklus der Sicherheitsmaßnahmen

Der Lebenszyklus von Sicherheitsmaßnahmen muss im Certification Practice Statement (CPS) beschrieben werden.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Die spezifischen Netzwerksicherheitsmaßnahmen der Zertifierungsstelle müssen im Certification Practice Statement (CPS) beschrieben werden.

7 Profilierung

7.1 Zertifikatprofil

Die Beschreibung der gültigen Zertifikatprofile erfolgt in einem gesonderten Dokument.

7.2 CRL-Profil

Die Beschreibung der gültigen Sperrlistenprofile erfolgt in einem gesonderten Dokument.

7.3 OCSP-Profil

Die Beschreibung der gültigen OCSP-Profile erfolgt in einem gesonderten Dokument.

8 Konformitätsprüfung

Es werden keine Vorgaben hinsichtlich der Konformitätsprüfung gestellt.

9 Allgemeine Festlegungen

9.1 Gebühren

n. a.

9.2 Finanzielle Verantwortung

Versicherungsschutz und Garantie für Sach- und Rechtsmängel sind nicht vorgesehen.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertraulich zu behandelnde Daten

Mit Ausnahme der in Abschnitt 9.3.2 benannten Informationen, werden sämtliche Teilnehmerdaten als vertraulich eingestuft.

9.3.2 Nicht-vertraulich zu behandelnde Daten

Sämtliche sich aus Teilnehmerzertifikaten, Zertifikatsperrlisten oder Zertifikatstatusinformationen direkt oder indirekt ableitenden Information, werden als nicht-vertraulich behandelt.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Die Zertifizierungsstelle trägt die Verantwortung für den Schutz vertraulicher Daten. Spezifische Sicherheitsmaßnahmen (Vertraulichkeitsverpflichtung von Mitarbeitern) müssen diese Anforderung angemessen adressieren.

9.4 Schutz personenbezogener Daten (Datenschutz)

9.4.1 Richtlinie zur Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten durch die Registrierungs- und Zertifizierungsstellen muss zwingend unter Einhaltung der geltenden Gesetze erfolgen.

9.4.2 Vertraulich zu behandelnde Daten

Vgl. Abschnitt 9.3.1.

9.4.3 Nicht-vertraulich zu behandelnde Daten

Vgl. Abschnitt 9.3.2.

9.4.4 Verantwortlicher Umgang mit personenbezogenen Daten

Vgl. Abschnitt 9.3.3.

9.4.5 Verwendung personenbezogener Daten

Der Zertifikatnehmer stimmt der Verwendung seiner personenbezogenen Daten im Rahmen der üblichen Funktionen und Aufgaben der Registrierungs- und Zertifizierungsstelle zu.

9.4.6 Offenlegung bei gerichtlicher Anordnung oder im Rahmen einer gerichtlichen Beweisführung

n. a.

9.4.7 Andere Umstände einer Veröffentlichung

n. a.

9.5 Urheberrechte

Die Weitergabe unveränderter Versionen dieses Dokuments an Dritte ist uneingeschränkt zulässig.

9.6 Verpflichtungen

9.6.1 Verpflichtungen der Zertifizierungsstellen

Sämtliche nach dieser Certificate Policy (CP) arbeitenden Zertifizierungsstellen verpflichten sich zur Einhaltung der in diesem Dokument definierten Anforderungen. Zusätzlich verpflichten sie sich zur Einhaltung der im zugehörigen Certification Practice Statement (CPS) formulierten Anforderungen.

9.6.2 Verpflichtungen der Registrierungsstellen

Sämtliche nach dieser Certificate Policy (CP) arbeitenden Registrierungsstellen verpflichten sich zur Einhaltung der in diesem Dokument definierten Anforderungen. Zusätzlich verpflichten sie sich zur Einhaltung der im zugehörigen Certification Practice Statement (CPS) formulierten Anforderungen.

9.6.3 Verpflichtungen der Zertifikatnehmer

Vgl. Abschnitt 4.5.1.

9.6.4 Verpflichtungen der Zertifikatprüfer

Vgl. Abschnitt 4.5.2.

9.7 Gewährleistung

Die Sana Kliniken Berlin-Brandenburg GmbH übernimmt keine Gewähr für die Verwendung und den Schutz des Zertifikats bzw. des zugehörigen Schlüsselpaares durch den Nutzer.

9.8 Haftungsbeschränkung

Die Sana Kliniken Berlin-Brandenburg GmbH haftet nicht für Schäden jeglicher Art, die durch die Verwendung des Zertifikats bzw. des zugehörigen Schlüsselpaares durch den Nutzer entstehen.

9.9 Haftungsfreistellung

Siehe 9.8.

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Sowohl die Certificate Policy (CP) als auch Certification Practice Statements (CPS) treten mit dem Moment ihrer Veröffentlichung im entsprechenden Informationsdienst (vgl. Kapitel 2) in Kraft.

9.10.2 Aufhebung

Die Gültigkeit dieses Dokuments erlischt mit Inkrafttreten einer neuen CP (vgl. Abschnitt 9.10.1) oder mit Einstellung des Betriebs der Zertifizierungsstellen.

9.10.3 Konsequenzen der Aufhebung

n. a.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

n. a.

9.12 Änderungen des Dokuments

Bei Änderungen des Dokuments, mit einem nachhaltigen Einfluss auf die Zertifikatnehmer oder die vorhandenen Abläufe und Sicherheitsmaßnahmen der Zertifizierungsstelle, muss eine Änderung der Dokumenten-OID erfolgen. Diese Änderung muss ggf. innerhalb der gültigen Zertifikatprofile sowie der bisher ausgestellten Zertifikate Berücksichtigung finden.

9.13 Konfliktbeilegung

Die in Abschnitt 1.5 benannten Ansprechpartner sind für die Konfliktbeilegung zuständig.

9.14 Geltendes Recht

Der Betrieb der Sana Kliniken Berlin-Brandenburg Corporate PKI unterliegt den Gesetzen der Bundesrepublik Deutschland.

9.15 Konformität mit geltendem Recht

n. a.

9.16 Weitere Regelungen

n. a.

9.17 Andere Regelungen

n. a.

10 Literaturverzeichnis

[RFC3647] Chokhani, S. et al.: RFC3647 – Internet X.509 Public Key Infrastructure – Certificate Policy and Certificatation Practice Framework. November 2003.

11 Glossar

CA	Certification Authority - Zertifizierungsstelle
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List (Zertifikatsperrliste)
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority – Registrierungsstelle