Certification Practice Statement (CPS)

Root CA - Service CA - User CA – Admin CA

Sana Kliniken Berlin-Brandenburg Corporate PKI

OID: 1.3.6.1.4.1.36444.100.2.1.5
Version: 1.5

Inhalt

1 Einleitung

Die Sana Kliniken Berlin-Brandenburg GmbH betreibt innerhalb der Sana Kliniken Berlin-Brandenburg Corporate PKI insgesamt vier Zertifizierungsstellen:

- Sana Kliniken Berlin-Brandenburg Root CA
- Sana Kliniken Berlin-Brandenburg User CA
- Sana Kliniken Berlin-Brandenburg Service CA
- Sana Kliniken Berlin-Brandenburg Admin CA

Für jede einzelne dieser Zertifizierungsstellen gelten die Vorgaben dieses Dokuments.

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: Certification Practice Statement – Root CA – Service CA – User CA – Admin CA - Sana Kliniken Berlin-Brandenburg Corporate PKI
Version: 1.5
Objekt Identifier: 1.3.6.1.4.1.36444.100.2.1.5

{ iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) Sana IT Services GmbH Berlin-Brandenburg(36444) pki(100) cps(2) major-version(1) minor-version(5) }

1.3 Bestandteile der Zertifizierungsinfrastruktur

1.3.1 Zertifizierungsstellen (CA)

Vgl. Certificate Policy.

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

Vgl. Certificate Policy.

1.3.4 Zertifikatprüfer

Vgl. Certificate Policy.

1.3.5 Andere

Vgl. Certificate Policy.

1.4 Zertifikatnutzung

Vgl. Certificate Policy.

1.5 Policy Verwaltung

Vgl. Certificate Policy.

1.6 Definitionen und Abkürzungen

Vgl. Certificate Policy.

2 Veröffentlichungen und Informationsdienste

2.1 Informationsdienste

Vgl. Certificate Policy.

2.2 Veröffentlichung von Zertifizierungsinformationen

Erforderliche Informationen werden unter der folgenden Adresse zur Verfügung gestellt: http://pki.sana-bb.de/info

2.3 Aktualisierung von Zertifizierungsinformationen

Vgl. Certificate Policy.

2.4 Zugriffssteuerung

Vgl. Certificate Policy.

3 Identifizierung und Authentifizierung

Vgl. Certificate Policy.

4 Ablauforganisation

Vgl. Certificate Policy.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnamen

5.1 Infrastrukturelle Sicherheitsmaßnahmen

5.1.1 Lage und Konstruktion

Die verwendete Technik befindet sich in 3 separaten Rechenzentren auf dem Gelände des Sana Klinikum Lichtenberg.

5.1.2 Zutrittskontrolle

Alle 3 Rechenzentren haben eine Zutrittskontrolle.

5.1.3 Stromversorgung und Klimatisierung

Alle 3 Rechenzentren sind mit USV gegen kurzfristigen Stromausfall, Notstromaggregat gegen langfristigen Stromausfall und Klimaanlagen gegen Überhitzung abgesichert.

5.1.4 Abwehr von Wasserschäden

In allen 3 Rechenzentren wurden Vorkehrungen für die Abwehr von Wasserschäden getroffen.

5.1.5 Feuer

Alle 3 Rechenzentren sind mit Rauchmeldern ausgestattet.

5.1.6 Lagerung der Datenträger

Datenträger werden in einem gesicherten Bereich gelagert.

5.1.7 Abfallentsorgung

Die Löschung ausgesonderter Datenträger erfolgt durch 7-faches Überschreiben gemäß den Vorgaben des BSI.

5.1.8 Externes Backup

Backups werden räumlich getrennt von den Originaldaten an einem gesicherten Ort aufbewahrt.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Sicherheitsrelevante Rollen

Vgl. Certificate Policy.

5.2.2 Erforderliche Anzahl von Personen je Tätigkeit

Vgl. Certificate Policy.

5.2.3 Identifizieren und Authentifizieren von Rollen

Vgl. Certificate Policy.

5.2.4 Trennung von Rollen

Vgl. Certificate Policy.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an die Mitarbeiter

Die Mitarbeiter verfügen über Kenntnisse über die eingesetzten Betriebssysteme und die eingesetzte Anwendungssoftware verfügen.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Keine

5.3.3 Anforderungen an die Schulung

Keine

5.3.4 Häufigkeit der Schulungen

Keine

5.3.5 Job Rotation

Keine

5.3.6 Sanktionen für unautorisierte Handlungen

Sowohl bei Mitarbeitern als auch bei Support-Partnern werden Sanktionen für unautorisierte Handlungen durchgeführt.

5.3.7 Anforderungen an die Arbeitsverträge

In den Arbeitsverträgen wird eine Verpflichtung zur Verschwiegenheit und Geheimhaltung vereinbart.

5.3.8 Dokumente für die Mitarbeiter

Keine

5.4 Sicherheitsüberwachung

5.4.1 Überwachte Ereignisse

Folgende Ereignisse werden überwacht:
- Verfügbarkeit der IT-Systeme (Ping)
- Verfügbarkeit der Schnittstellen (HL7)
- Füllstände der Festplatten

– Verstöße gegen Firewall Policies

5.4.2 Häufigkeit der Protokollanalyse

Die Protokolle der unter 5.4.1 definierten überwachten Ereignisse werden Montag bis Freitag von 8:00 Uhr bis 17:00 Uhr stündlich ausgewertet.

5.4.3 Aufbewahrungsdauer von Protokolldaten

Protokolldaten werden 3 Monate aufbewahrt.

5.4.4 Schutz von Protokolldaten

Der Zugriff auf Protokolldaten ist nur Administratoren möglich.

5.4.5 Backup von Protokolldaten

Protokolldaten werden täglich gesichert.

5.4.6 Überwachungssystem

Das Überwachungssystem wird mittel crontab und syslog realisiert.

5.4.7 Benachrichtigung bei schwerwiegenden Ereignissen

Bei schwerwiegenden Ereignissen werden der Betriebsleiter und die verantwortlichen Mitarbeiter informiert.

5.4.8 Schwachstellenanalyse

Es wird eine reaktive Schwachstellenanalyse durch die Überwachung bekannt werdender Schwachstellen der Produkte Solaris, Oracle, Linux, Jboss, EJBCA und Java durchgeführt.

5.5 Archivierung

5.5.1 Archivierte Daten

Keine

5.5.2 Aufbewahrungszeitraum für archivierte Daten

n.a.

5.5.3 Schutz der Archive

n.a.

5.5.4 Datensicherungskonzept

Es wird eine tägliche Datensicherung durchgeführt.

5.5.5 Anforderungen für Zeitstempel

5.5.6 Archivierungssystem

n.a.

5.5.7 Prozeduren zum Abrufen und Überprüfen von archivierten Daten

5.6 Schlüsselwechsel

Vgl. Certificate Policy.

5.7 Kompromittierung und Wiederherstellung

Vgl. Certificate Policy.

5.8 Einstellung des Betriebs

Vgl. Certificate Policy.

6 Technische Sicherheitsmaßnahmen

6.1 Schlüsselerzeugung und –installation

Vgl. Certificate Policy.

6.2 Schutz des privaten Schlüssels und Umgang mit kryptografischen Modulen

Vgl. Certificate Policy.

6.3 Weitere Aspekte des Schlüsselmanagements

Vgl. Certificate Policy.

6.4 Aktivierungsdaten

Vgl. Certificate Policy.

6.5 Sicherheitsmaßnahmen für Computer

Vgl. Certificate Policy.

6.6 Lebenszyklus der Sicherheitsmaßnahmen

6.6.1 Softwareentwicklung

n.a.

6.6.2 Sicherheitsmanagement

Ein Management bezüglich des Lebenszyklus der Sicherheitsmaßnahmen wurde instanziiert. Eine Revision der getroffenen Sicherheitsmaßnahmen erfolgt in regelmäßigen Abständen.

6.6.3 Sicherheitseinstufung

n. a.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Die eingesetzten Produkte im Netzwerkbereich wurden im Hinblick auf die Sicherheitsanforderungen überprüft und getestet.

7 Profilierung

Vgl. Certificate Policy.

8 Konformitätsprüfung

Vgl. Certificate Policy.

9 Allgemeine Festlegungen

Vgl. Certificate Policy.

10 Literaturverzeichnis

Vgl. Certificate Policy.

11 Glossar

Vgl. Certificate Policy.