ITDZ BERLIN

PKI Policy und CPS Berlin Class2 Typ2 CA

PKI Policy und Practice Statement des Basisdienstes Land Berlin PKI

Name

PKI-Team

Version 1.0

05.02.2025

Inhaltsverzeichnis

Änderungshistorie

Datum	Version	Grund	Author/Editor	
23.10.2023	0.1	Erstellung	Jörg Schmidtke (Computacenter)	Gesamtes Dokument
13.02.2024	0.2	Überarbeitung	Jörg Schmidtke (Computacenter)	Gesamtes Dokument
12.04.2024	0.3	Überarbeitung	Jörg Schmidtke (Computacenter)	Gesamtes Dokument
14.05.2024	0.4	Überarbeitung	Jörg Schmidtke (Computacenter)	Gesamtes Dokument
30.07.2023	0.5	Überarbeitung	Jörg Schmidtke (Computacenter)	Gesamtes Dokument
03.02.2025	0.6	Überarbeitung	Andreas Koch (ITDZ Berlin)	Gesamtes Dokument
05.02.2025	1.0	Finalisierung	Andreas Koch (ITDZ Berlin)	Gesamtes Dokument

1 Einleitung

Das IT-Dienstleistungszentrum Berlin (ITDZ Berlin) betreibt einen zentralen PKI-Dienst. Dieses Dokument beschreibt die PKI Richtline (Certificate Policy - CP) und die praktischen Verfahrensregeln (Certificate Practice Statement - CPS) der Berlin Class2 Typ2 CA.

Die Wurzelzertifizierungsstelle (Root CA - Certification Authority), wie auch die darunterliegenden Zertifizierungsstellen (Sub CAs – Intermediate Certification Authorities) – hier die Berlin Class2 Typ2 CA – bilden die Vertrauensanker des PKI-Dienstes.

Die in diesem Dokument getroffenen Aussagen sind für die Zertifizierungsstelle (CA) bindend. Die CA zertifizieren die Zertifikatsnehmer ausschließlich nach den Richtlinien dieser Policy.

2 Überblick

2.1 Aufbau der PKI und ihrer Schnittstellen

Das ITDZ Berlin erweitert die hierarchisch strukturierte interne PKI für die zertifikatbasierte Sicherung folgender Anwendungsfälle:

- E-Mail Verschlüsselung (Inhaltsbasierter Schutz von E-Mail Nachrichten)
- E-Mail Signaturen (Authentizitätsnachweise für die Absender von E-Mails)
- Client-Zertifikate für stationäre und mobile Geräte zur Authentifizierung via EAP (Extensible Authentication Protocol) über 802.1x sowie an Infrastruktur-Diensten wie VPN)
- SSL-Zertifikate für Web-Server und Gateways
- Zertifikate für VPN-Gateways (IPSec), Server und Client
- Kerberos/LDAPs Zertifikate für Domänencontroller
- Code-Signierung von Skripten und Makros
- Key Recovery Möglichkeit für User Zertifikate
- Datenbankverschlüsselung
- Zertifikate mit qualifizierter elektronischer Signatur (Signatur, Siegelung und Archivierung von Dokumenten, unterschriftsersetzend)

Die Infrastruktur des PKI-Dienstes basiert auf dem Standard X.509 v3, sowie Microsoft Windows Server (Version 2022) mit den Active Directory Certificate Services (ADCS) sowie zwei nCipher Hardware Security Modulen (HSMs).

Mit Zertifikaten wird die elektronische Kommunikation vor unberechtigter Einsichtnahme durch Verschlüsselung gesichert (Vertraulichkeit). Die Authentizität des angegebenen Kommunikationspartners und die Integrität der Daten ist durch die elektronische Signatur gewährleistet. Die erweiterte Vertrauensinfrastruktur wird die Gültigkeit des öffentlichen Schlüssels eines Zertifikatnehmers, mit den dazugehörenden Identifikationsmerkmalen (wie Schlüsselinhaber, beglaubigende Stelle, Gültigkeitszeitraum, usw.), durch die elektronische Signatur der Zertifizierungsinstanz (Sub CA) beglaubigt.

Bei der verschlüsselten Kommunikation mit einem Server, der sich mittels Zertifikats ausweist ist gewährleistet, dass es sich wirklich um den angegebenen Server handelt. Gleiches gilt auch bei den gesicherten Daten und Informationsübertragung über öffentliche Netze durch Zertifikate (IPSec) zum Aufbau von virtuellen privaten Netzen. Durch die Zertifikate lassen sich verschlüsselte und authentisierte Kommunikationskanäle (sogenannte Tunnel) zwischen einem Arbeitsplatz-PC

und einem Anwendungsserver an verschiedenen Standorten aufbauen. E-Mail-Zertifikate reduzieren die Risiken der ungesicherten Nachrichtenübertragung, die darin liegen, dass Fremde die elektronischen Inhalte lesen und ändern können. Eine gültig signierte E-Mail gibt zusätzlich die Sicherheit, dass die Nachricht wirklich vom angegebenen Absender kommt und der Inhalt nach dem Absenden nicht verändert wurde.

Es werden zwei HSMs zur Redundanz eingesetzt, um eine Ausfallsicherheit zu gewährleisten. Diese Geräte garantieren die Generierung und Speicherung von hardwarebasierenden Schlüssel für Zertifikate, mit einem eigenen mitgelieferten Cryptographic Service Provider (CSP). Der Zugriff auf diese HSM-Module ist nur über eine HSM-Software und einen gesicherten Tunnel zwischen den Clients (CAs) möglich und Änderungen können nur mit Hilfe der Administrator bzw. Operator Card Sets erfolgen. Die HSMs übernehmen auch die Signierung der für die Sub CA bereitgestellten Sperrlisten.

Der private Schlüssel der Zertifizierungsstellen wird durch das HSM selbst erzeugt und kann aus dem HSM nicht durch unberechtigte Dritte ausgelesen werden. Die Zertifizierungsstellen-Software sendet lediglich die zu signierenden Zertifikate an das HSM, welches die signierten Zertifikate wieder zurück an die Zertifizierungsstellen-Software sendet.

Die Kommunikation zwischen dem HSM und den angeschlossenen CA erfolgt über eine konfigurierte Security World und ist über einen gesicherten Tunnel verschlüsselt, so dass eine Beeinflussung der Kommunikation ausgeschlossen ist. Des Weiteren ist es nicht möglich, ohne die Administrator Cards weitere CAs bzw. Server, auch innerhalb eines VLANs, zu einer Kommunikationsverbindung mit dem HSM hinzuzufügen, da diese über die Security World geschützt ist.

Die Zertifikate des PKI-Dienstes dienen der Absicherung der online Kommunikation durch sichere elektronische Signatur (nach dem Signatur-Gesetz [2]) und der Verschlüsselung.

2.2 Zertifizierungshierarchie

Das ITDZ Berlin betreibt eine zentrale Registrierungsstelle zur Antragstellung und Registrierung aller von ihr unterstützten Zertifikate. Die Abbildung 1 veranschaulicht den Aufbau. Die Root CA (Berlin Class2 Root CA) des Basisdienstes Land Berlin PKI erstellt als oberste CA der Hierarchie ein selbstsigniertes Wurzelzertifikat und signiert die Zertifikate der angeschlossenen Sub CA (Berlin Class2 Typ2 CA). Die von der Root CA zertifizierten Sub CAs bilden die zweite Stufe der PKI-Hierarchie. Die Zertifikatnehmer wiederum werden durch die ihnen zugeordnete Zertifizierungsstelle eingebunden und bilden die unterste Stufe der Zertifizierungshierarchie.

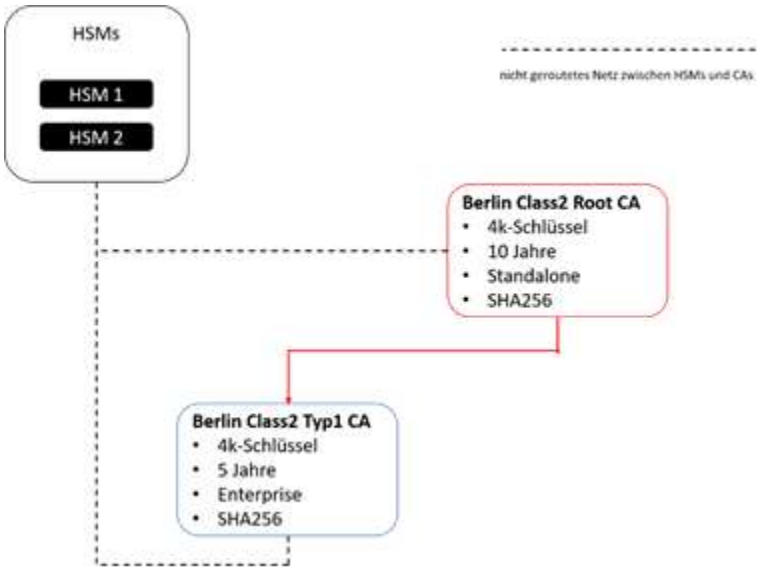

Abbildung 1: Architektur der PKI mit angeschlossenen CAs

Zertifikatnehmer sind Fachverfahren (Applikationen), Personen und Maschinen (Server, Clients und Netzwerkkomponenten). Zertifikatnehmer von E-Mail-Zertifikaten sind natürliche oder juristische Personen für namensbezogene Zertifikate sowie Personengruppen, Funktionen oder Dienste (IT-Prozesse), die im Rahmen der PKI Schlüssel und Zertifikate erhalten. Für natürliche Personen werden Pseudonyme zugelassen. Maschinenzertifikate werden grundsätzlich vom Systemadministrator der Maschine bzw. der Maschine selbst beantragt (Sonderfall MS Autoenrollment). PKI-Informationen werden über die Verzeichnis- und Validierungsdienste des Basisdienst Land Berlin PKI abgerufen.

Unterhalb der Root CA besteht die Unterstruktur im PKI-Dienst aus verschiedenen Ebenen:

- Zertifizierungsinstanz CA
- Registrierungsinstanz RA
- Zertifikatnehmer (ZN) für folgende IT-Anwendungen:
  - AD-Nutzer und Komponenten für Verschlüsselung; Signatur, Authentication
  - IPSec-Verbindungen
  - externe Nutzer und Komponenten für Verschlüsselung, Signatur, Authentication
  - Client Authentication
  - Kerberos/LDAPs Authentication

Die bestehende PKI Struktur kann um weitere CAs mit oder ohne lokale Registrierungsstellen erweitert werden.

2.3 Registrierungsstellen

Das ITDZ hat eine hierarchisch strukturierte PKI für die zertifikatbasierte Absicherung der IT-Anwendungen:

- Personen- und Maschinen-Zertifikate werden von der **Berlin Class2 Typ2 CA** ausgestellt und signiert.

Im ITDZ Berlin ist eine zentrale Registrierungsstelle eingerichtet. Bei Behörden kann auf Anforderungen auch eine lokale Registrierungsstelle eingerichtet werden.

2.4 Validierungsdienste

Der Typ des Zertifikats entscheidet beim Zertifikatsantrag darüber, ob und wo (intern und/oder extern) das Zertifikat veröffentlicht wird. Die von der Sub CA signierte Zertifikate sowie die Sperrlisten (CRL internen sowie externen Validierungsdienste veröffentlicht. Die Daten werden auf Web-Servern bereitgestellt, welche redundant und hochverfügbar erreichbar sind.

Folgende Web-Veröffentlichungsorte sind vorgesehen:

Datei/CRL	Pfad
CP/CPS	https://www.class2.pki.verwalt-berlin.de/www/Berlin-Class2-Typ2-CA-2022/
CRLs (http-CDP)	**Root CA:** http://cdp.class2.pki.verwalt-berlin.de/cdp/Berlin%20Class2%20Root%20CA%202022.crl **Berlin Class2 Typ2 CA:** http://cdp.class2.pki.verwalt-berlin.de/cdp/Berlin%20Class2%20Typ2%20CA%202022.crl
CA-Zertifikate (http-AIA)	**Root CA:** http://aia.class2.pki.verwalt-berlin.de/aia/Berlin%Class2%Root%CA%2022.crt **Berlin Class2 Typ2 CA:** http://aia.class2.pki.verwalt-berlin.de/cdp/Berlin%20Class2%20Typ2%20CA%202022.crt

Tabelle 1: Web-Veröffentlichungsorte der CA-Zertifikate und Sperrlisten

2.5 Anwendungsbereich

Auf Antrag erzeugt die Root CA durch ein HSM X.509v3-Zertifikate für die Zertifizierungsstelle (CAs), die wiederum auf Antrag verschiedene Zertifikate für die Zertifikatsnehmer*innen (ZN) erzeugen. Darüber hinaus können die jeweiligen CAs für weitere Registrierungs- und Zertifizierungsinstanzen (RAs) Zertifikate ausstellen.

Der Zuständigkeitsbereich der Root CA und der angeschlossenen Sub CA umfasst alle Einrichtungen der Berliner Verwaltung. Diese Policy unterstützt das Zertifikat-Format X.509 v3, das in aktuellen Standard-Browsern für unterschiedliche Anwendungen eingesetzt wird. Die X.509 v3 ist ein Standardformat der ITU-T für Zertifikate (International Telecommunications Union-Telecommunication) [3]. Es enthält den Namen sowie Angaben über die Identität des Zertifikatnehmers, die durch eine elektronische Signatur des Ausstellers (CA) bestätigt werden. Aufgrund der Zertifikatserweiterungsmöglichkeit nach X.509 v3 gibt es bei der CA für E-Mail-Zertifikate eine Trennung von Signatur- und Verschlüsselungsschlüssel. Diese Trennung beinhaltet, dass jeder Zertifikatnehmer zwei E-Mail-Zertifikate mit den dazugehörigen Schlüsseln erhält.

2.6 Personelle Unterstützung

2.6.1 Organisationsstruktur

Dieser Abschnitt enthält die wichtigsten Informationen und Adressen um PKI-Dienst. Der PKI-Dienst wird vom ITDZ für das Land Berlin betrieben.

2.6.2 Ansprechstelle der Zertifizierungsstelle

Der PKI-Dienst wird von Mitarbeitern aus dem entsprechenden Fachgebiet des ITDZ betrieben. Diese Informationen werden im Betriebskonzept erarbeitet und im Betriebshandbuch fortgeschrieben. Erreichbar sind die Mitarbeiter des PKI-Teams unter folgender Adresse:

IT-Dienstleistungszentrum Berlin
Berliner Straße 112-115
10713 Berlin
Telefax: +49 30 9028 3048
E-Mail: pki@itdz-berlin.de

3 Allgemeine Bestimmungen

3.1 Verpflichtungen der untergeordneten Zertifizierungsstelle

- Jeder Sub CA wird ein eindeutiger Name zugeteilt, der innerhalb der gesamten PKI gilt. Damit wird sichergestellt, dass die vereinbarten Namensbestandteile in ihrem Zuständigkeitsbereich verwendet werden.
- Jede Sub CA ist an die Einhaltung des durch die Root CA festgelegten Namensraumes gebunden (auf HSM basierender Aufbau).
- Die Einhaltung der Sicherheitsrichtlinien ist durch die Nutzung des HSM vorgegeben.
- Über die Sub CAs ist jederzeit der Nachweis zur Zertifikatsbeantragung, -ausstellung und -sperrung möglich.
- Die Schlüssel der veröffentlichten Zertifikate werden durch die HSMs gesichert.
- Die HSMs stellen sicher, dass die Sub CA-Schlüsselpaare in einer gesicherten Umgebung kryptografisch geeignet erzeugt wird. Darüber hinaus stellt es sicher, dass der geheime Schlüssel nur zur Bestätigung von Zertifikaten verwendet wird.
- Jede Sub CA stellt einen Sperrliste zur Verfügung. Die Sperrliste kann über die Validierungsdienste (siehe 2.4) abgerufen werden.

3.2 Verpflichtungen der Registrierungsstelle (RA)

- Zu den Aufgaben und Pflichten der Mitarbeiter der RA gehört, dass Zertifikatnehmer durch persönliches Erscheinen in der RA identifiziert, Post-Ident Verfahren und anhand eines gültigen amtlichen Ausweises oder bei Verwaltungsbeschäftigten durch einen gültigen Dienstausweis authentisiert werden. Optional kann für die festangestellten Mitarbeiter des Land Berlin die Überprüfung über die gültigen Mitarbeiterverzeichnisse der Verwaltung oder durch Anfrage bei den dafür zuständigen Personalstellen erfolgen. Dies gilt auch bei Pseudonymzertifikaten, damit die RA in der Lage ist, das verwendete Pseudonym dem realen Namen des Zertifikatnehmers zuzuordnen. Die Zuordnung wird von der RA vertraulich verwahrt.
- Bei Maschinenzertifikaten (für Fachverfahren, Server und Netzwerkkomponenten) wird die Identität des Geräts im Verzeichnisdienst überprüft. Bei nicht-Mitgliedern des Verzeichnisdienstes wird die Identität des entsprechenden Administrators der Maschine bzw. des Fachverfahrens/der Applikation überprüft.
- Die RA informiert die Zertifikatnehmer (bei Maschinenzertifikaten den jeweiligen Administrator) über die Notwendigkeit der Einhaltung der Sicherheitsrichtlinien.

- Die Mitarbeiter der RA sind über die Aufgaben und Pflichten einer RA informiert und sind daran gebunden.
- Die Mitarbeiter sind einer Sicherheitsüberprüfung SÜ 2 nach Berliner Sicherheitsüberprüfungsgesetz (BSÜD) zu unterziehen.

3.3 Verpflichtungen von lokalen Registrierungsstellen

Die RA des ITDZ Berlin kann lokale Registrierungsoperatoren - Local Registration Authority (LRA) - zur Beantragung von Zertifikaten für Mitarbeiter oder Maschinen einer Einrichtung benennen. Dies hat den Vorteil, dass nicht alle Mitarbeiter einer Einrichtung wegen der Identifizierung Kontakt mit der RA im ITDZ aufnehmen müssen. Bei festangestellten Mitarbeitern des ITDZ Berlin ist das Vorhandensein des Accounts im Active Directory ausreichend.

- Die Mitarbeiter der von der RA eingesetzten LRA sind über die Aufgaben und Pflichten einer LRA informiert und halten sich an die Sicherheitsrichtlinien der Root CA und der zuständigen Sub CAs.
- Die LRA Mitarbeiter haben dieselben Aufgaben und Pflichten wie die Mitarbeiter der RA.

3.4 Verpflichtungen der Endanwender

- Der Zertifikatnehmer erklärt sich bereit den geheimen Schlüssel ausreichend zu schützen, den Zugriff anderer Personen zu verhindern und ihn nicht weiterzugeben.
- Der Zertifikatnehmer erklärt sich bereit, die Sperrung seines Zertifikats bei Kompromittierung oder Verdacht darauf zu veranlassen.
- Die Weitergabe des geheimen Schlüssels oder der PSE mit PIN des Zertifikatnehmers ist untersagt.
- Bei der Beantragung von Gruppenzertifikaten muss sich eine berechtigte Person als Gruppenverantwortlicher ausweisen. Erst danach erhält der Gruppenverantwortliche die entsprechenden Schlüssel und Zertifikate zur Weiterverteilung in der Gruppe. Jedes Gruppenmitglied ist Zertifikatnehmer.
- Für Nutzer innerhalb des zentralen AD..

3.5 Gültigkeitsdauer der Zertifikate

Die Gültigkeitsdauer von Zertifikaten für die Sub CA beträgt maximal fünf Jahre. Ein regelmäßiger Schlüsselwechsel des Zertifikats der CA ist spätestens nach drei Jahren vorgesehen.

Dementsprechend gibt es mehrere gültige CA-Zertifikate, die sich im Gültigkeitsdatum unterscheiden.

Die Gültigkeitsdauer von Endzertifikaten beträgt maximal zwei Jahre.

4 Identifizierung und Authentisierung

4.1 Erstmalige Registrierung

4.1.1 Identifizierung und Authentisierung einer natürlichen Person

Alle ausgestellten Zertifikate der CAs entsprechen dieser Policy und erfüllen eine einheitliche Vertrauensstufe, die sich auf die Identitätsfeststellung und die Überprüfung der Inhalte bezieht. Die Sicherheit der Verschlüsselung ist u.a. von den eingesetzten Algorithmen, Zertifikaten, Produkten und bei Gruppenzertifikaten von organisatorischen Randbedingungen abhängig. Für die Vertrauensstufe in den CAs ist die Verbindlichkeit der durch die Zertifikate gemachten Aussagen bedeutsam. Der Zuordnung des Zertifikats zum Zertifikatnehmer bzw. zu einer Referenzperson bei Gruppenzertifikaten kommt somit entscheidende Bedeutung zu. Für die erstmalige Registrierung und Ausstellung von Zertifikaten durch die CAs bestehen besondere Anforderungen an die Identifizierung der Zertifikatnehmer, die im folgenden Abschnitt dargelegt werden. Bei der Ausstellung weiterer Zertifikate für bereits registrierte Zertifikatnehmer gelten vereinfachte Verfahren.

Personen, die ein Zertifikat beantragen, werden durch persönliches Erscheinen in der RA, Post-Ident-Verfahren identifiziert und anhand eines gültigen amtlichen Ausweises authentisiert. Verwaltungsbeschäftigten können durch einen gültigen Dienstausweis authentisiert oder über die gültigen Mitarbeiterverzeichnisse der jeweiligen Verwaltung ggf. durch Anfrage bei den zuständigen Personalstellen überprüft werden.

Sofern ein LRA-Operator eingesetzt wurde, erfolgen die Identifizierung und Authentisierung der Zertifikatnehmer auf die gleiche Weise über ihn.

4.1.2 Identifizierung und Authentisierung bei Maschinenzertifikaten

Maschinenzertifikate für Fachverfahren sind von einer natürlichen Person zu beantragen, die als Systemadministrator der Maschine fungiert. Diese Person muss gemäß Abschnitt 4.1 ein entsprechendes Zertifikat beantragen und die in Abschnitt 4.1.1 geforderten Identitäts- und Authentisierungsnachweise erbringen. Zusätzlich ist die Angabe des Maschinennamens (z. B. DNS Namen) obligatorisch.

Im Sonderfall des MS Autoenrollment werden Maschinenzertifikate direkt durch die Maschinen selbst automatisiert beantragt. Einen Authentisierungsnachweis hat die Maschine durch die Mitgliedschaft im Verzeichnisdienst bereits erbracht.

4.1.3 Namensregeln

Der Namensraum der Root CA wird durch diese bestimmt und legt den Namensraum der Sub CAs fest. Für die Eindeutigkeit der verwendeten Namen für Zertifikatnehmer trägt die zuständige CA die Verantwortung.

4.1.4 Zertifizierungsinstanzen

- Der Namensraum der Root CA lautet: *CN=Berlin Class2 Root CA 2022, O=Landesverwaltung Berlin, C=DE*
- Der Namensraum der Sub CAs lautet:
  - *CN=Berlin Class2 Typ2 CA 2022, O=Landesverwaltung Berlin, C=DE*

4.1.5 User-Zertifikate

Allen Zertifikatnehmern der Zertifizierungshierarchie vom Typ User wird ein eindeutiger Distinguished Name (DN) nach X.500 zugeordnet, welcher bei der Ausstellung eines Zertifikats für einen Zertifikatnehmer als dessen Subjektname zu verwenden ist. Ein DN enthält eine eindeutig kennzeichnende Folge von Namensbestandteilen, durch die alle Zertifikatnehmer einer Hierarchie referenziert werden können. Die korrekte Wahl von DNs ermöglicht daher die effiziente Speicherung und Suche von Zertifikaten innerhalb eines Verzeichnisses.

Die Berlin Class2 Typ2 CA 2022 ist für die Einheitlichkeit und Eindeutigkeit der vergebenen Namen (DNs) für User-Zertifikate verantwortlich.

Die DNs aller Zertifikatnehmer, deren Zertifikate von der Berlin Class2 Typ2 CA 2022 generiert wurden, enthalten die in Tabelle 2 festen Attribute:

Attribut	Kürzel	Wert
Country	C	DE
Organization	O	Landesverwaltung Berlin
Organizational Unit	OU	<Behördenkürzel>

Tabelle 2: Feste Attribute von DNs aller Zertifikatnehmer

und die in Tabelle 3 spezifischen Attribute:

Attribut	Kürzel	Wert
Organizational Unit	OU (kann mehrfach vorkommen)	<Verfahren> oder <Bereich>
Common Name	CN	<Nachname Vorname> oder <Login-Name>
E-Mail	E	<E-Mail-Adresse>

Tabelle 3: Spezifische Attribute von DNs aller Zertifikatnehmer

Über den Subject Alternate Name (SAN) können auch weitere Namen, wie z. B. die E-Mail-Adresse oder der User Principal Name (UPN), angegeben werden.

4.1.6 Maschinen-Zertifikate

Allen Zertifikatnehmern der Zertifizierungshierarchie vom Typ Maschine wird ebenfalls ein eindeutiger Distinguished Name (DN) nach X.500 zugeordnet, welcher bei der Ausstellung eines Zertifikats für Maschinen als dessen Subjektname zu verwenden ist. Die zuständige Berlin Class2 Typ2 CA 2022 ist für die Einheitlichkeit und Eindeutigkeit der vergebenen Namen (DNs) verantwortlich.

Die DNs aller Maschinen, deren Zertifikate von der Berlin Class2 Typ2 CA 2022 generiert wurden, enthalten die in den folgenden Tabellen dargestellten Attribute.

4.1.6.1 Manuelles Enrollment

Die festen Attribute für Maschinenzertifikate, die nicht über MS-Autoenrollment erzeugt werden sind wie folgt:

Attribut	Kürzel	Wert
Country	C	DE
Organization	O	Landesverwaltung Berlin
Organizational Unit	OU	<Behördenkürzel>

Tabelle 4: Feste Attribute von DNs aller Maschinenzertifikate (manuelles Enrollment)

und die in Tabelle 5 spezifischen Attribute:

Attribut	Kürzel	Wert
Organizational Unit	OU (kann mehrfach vorkommen)	<Verfahren> oder <Bereich>
Common Name	CN	<Nachname Vorname> oder <Login-Name>
E-Mail	E	<E-Mail-Adresse>

Tabelle 5: Spezifische Attribute von DNs der Maschinenzertifikate (manuelles Enrollment)

4.1.6.2 MS-Autoenrollment

Maschinenzertifikate, die über MS-Autoenrollment ausgestellt werden, haben die folgenden spezifischen Attribute:

Attribut	Kürzel	Wert
Common Name	CN	< Maschinenname>

Tabelle 6: Spezifische Attribute von DNs der Maschinenzertifikate (MS-Autoenrollment Variante 1)

Für den Fall, dass die abzusichernde Anwendung weitere Informationen über das Zertifikat erhalten muss, kann der DN auch über die folgenden spezifischen

Attribut	Kürzel	Wert
Country	C	<TLD der AD-Domäne>
Domain Component	DC (kann mehrfach vorkommen)	<Domänenteile der AD-Domäne>
Organizational Unit	OU (kann mehrfach vorkommen)	<OU in der AD-Domäne>
Common Name	CN (kann mehrfach vorkommen)	<CN in der AD-Domäne>
Common Name	CN	< Maschinenname>

Tabelle 7: Spezifische Attribute von DNs der Maschinenzertifikate (MS-Autoenrollment Variante 2)

Über den Subject Alternate Name (SAN) können auch weitere Namen, wie z. B. weitere DNS-Namen angegeben werden.

4.2 Regelmäßiges Wiederausstellen

Folgezertifikate müssen entweder wie bei der erstmaligen Registrierung auf der RA oder als elektronisch signierter Verlängerungsantrag bei der RA beantragt werden. Es gibt dabei keine Rezertifizierung, sondern die Folgezertifikate haben neue Schlüssel. Ausnahmen bestehen bei den Zertifikatnehmern, die selbst einen Certificate Request an der Maschine erzeugen und diesen mit dem Zertifikatsantrag zur RA senden oder bei automatisch ausgerollten Zertifikaten, die Maschinen im AD zugeordnet sind. Ein einmal erzeugter Request kann auch bei Folgezertifikaten verwendet werden.

4.3 Wiederausstellung nach Sperrungen

Nach einer Sperrung des Zertifikats ist wie bei einer erstmaligen Registrierung vorzugehen, d. h. es ist ein neues Zertifikat zu beantragen.

4.4 Sperrantrag

Sperren eines Zertifikats kann mittels verschiedener Verfahren zu Übermittlung des Sperrantrages erfolgen. Die Root CA und die Sub CAs nehmen die Sperranträge der berechtigten Zertifikatsnehmer und Zertifizierungsinstanzen entgegen.

5 Ablauforganisation

5.1 Zertifikatsantrag

Arbeitsabläufe zur Beantragung und Ausstellung von Zertifikaten innerhalb des PKI-Dienstes werden im Folgenden dargestellt:

Die vom ITDZ betriebenen Zertifizierungsstellen setzen eine zentrale Registrierungsstelle (RA) für die Identifizierung von Zertifikatnehmern (Personen, Maschinen und Netzwerkkomponenten) und Zertifizierungsinstanzen ein. Die Zertifizierungsanträge von Zertifikatnehmern und Instanzen werden von Mitarbeitern der RA nach vorheriger Prüfung der Identität der Antragsteller weiterbearbeitet.

Die RA übermittelt den geprüften Zertifikatsantrag an die CA zur Erzeugung der Zertifikate. Sofern ein Certificate Request bei der RA eingeht, wird dieser nach der Identitätsprüfung des Antragstellers und Inhaltsprüfung zusammen mit dem Antrag an die CA zur Bearbeitung weitergeleitet.

Die RA kann lokale Registrierungsstellen (LRA) für die Identitätsprüfung von Mitarbeitern bzw. Administratoren von Servern und Netzwerkkomponenten in einzelnen Behörden einrichten. Dabei wird die Aufgabe der Identitätsprüfung von Zertifikatnehmern und Instanzen auf die LRA übertragen. Der geprüfte Antrag wird dann von der RA an die CA zur Bearbeitung übergeben.

5.2 Ausstellung des Zertifikats

Die CA erzeugt Zertifikate im Rahmen ihrer Verpflichtungen nach Vorliegen eines vollständigen und geprüften Antrags und nach erfolgter Identifizierung für Zertifikatnehmer, wenn zusätzlich die Einhaltung des Namenskonzeptes erfüllt ist. Das Namenskonzept sieht vor, dass jeder Zertifikatnehmer und jede Zertifizierungsinstanz einen eindeutigen Namen in Form eines X.500 Distinguished Name (DN) bekommt. Für die Eindeutigkeit der verwendeten Namen trägt die CA die Verantwortung. Es gibt die folgenden drei Möglichkeiten der Beantragung von Zertifikaten an die Zertifizierungsstelle:

- Clients, Server oder Benutzer sind Mitglied im Active Directory und nutzen die MS Autoenrollment Funktion. Der Antragsteller erzeugt sein Schlüsselpaar selbst und generiert einen signierten Zertifikatsantrag (Certificate Signing Request/CSR). Die CA prüft den Zertifikatsantrag anhand der erfolgreichen AD-Authentifizierung des Antragstellers. Danach signiert die CA den öffentlichen Schlüssel und übergibt diesen zurück an den Antragsteller.
- Die zweite Möglichkeit besteht darin, dass nach Vorlage von geprüften Anträgen asymmetrische Schlüsselpaare (geheimer und öffentlicher Schlüssel) für den jeweiligen Antragsteller generiert. Der öffentliche Schlüssel des Antragstellers wird von der

Zertifizierungsstelle signiert. Mit ihrer Unterschrift bestätigt die CA die Gültigkeit des Zertifikats und die Korrektheit der Angaben. Das Zertifikat wird mit dem dazugehörigen geheimen Schlüssel im PKCS#12 Format als PSE mit einem Transportschlüssel gesichert. Der Der Transportschlüssel wird dem Zertifikatsnehmer auf geeignetem Wege zugestellt.

- Die dritte Möglichkeit besteht darin, dass der Antragssteller sein Schlüsselpaar selbst generiert und einen signierten Zertifikatsantrag (Certificate Signing Request/CSR) übergibt. Es wird der Zertifikatsantrag geprüft, mit dem vorgelegten öffentlichen Signatur-Schlüssel. Hiermit wird sichergestellt, dass der vorgelegte öffentliche Signatur-Schlüssel mit den Erstellungsdaten des Zertifikatsantrages korrespondiert. Danach signiert die CA den öffentlichen Schlüssel und übergibt diesen zurück an den ZN. Der Antragsteller kann sich das signierte Zertifikat mit öffentlichem Schlüssel herunterladen. In der Regel werden Zertifikate über einen einem Certificate Signing Request signiert und bereitgestellt.

Mit dem Ausstellen eines Zertifikats durch die CA bestätigt die CA die Zuordnung des Zertifikats zu dem Antragsteller.

5.3 Wirksamkeit des Zertifikats

Das Zertifikat ist sofort nach Erzeugung freigeschaltet und wird nur dann zurückgezogen, wenn ein Zertifikatnehmer die Fehlerhaftigkeit seines Zertifikats (z. B. wegen falscher Angaben im DN) bei Mitarbeitern der RA meldet.

5.4 Regelmäßiges Wiederausstellen

Folgezertifikate müssen wie bei der erstmaligen Registrierung bei der RA beantragt werden. Es gibt dabei keine Rezertifizierung, sondern die Folgezertifikate haben neue Schlüssel. Ausnahmen bestehen bei den Zertifikatnehmern, die selbst einen Certificate Request an der Maschine erzeugen und diesen mit dem Zertifikatsantrag zur RA senden oder bei automatisch ausgerollten Zertifikaten, die Maschinen im AD zugeordnet sind. Ein einmal erzeugter Request kann auch bei Folgezertifikaten verwendet werden.

5.5 Sperrung von Zertifikaten

5.5.1 Sperrgründe

5.5.1.1 Sperrgründe für CA-Zertifikate

CA-Zertifikate können von der Root CA aus folgenden Gründen gesperrt werden:

- Der geheime Signaturerstellungsschlüssel der Sub CA ist nicht mehr verfügbar oder kompromittiert.
- Die Sub CA gibt den Betrieb auf.
- Erhebliche Schwächen eines verwendeten Kryptoalgorithmus samt zugehöriger Schlüssel werden bekannt.
- Erhebliche Schwächen der eingesetzten Hard- und Software werden bekannt.

5.5.1.2 Sperrgründe für End-Zertifikate

Zertifikate können von der CA aus folgenden Gründen gesperrt werden:

- Das Zertifikat für Zertifikatnehmer enthält Angaben, die nicht mehr korrekt sind.
- Erhebliche Schwächen eines verwendeten Kryptoalgorithmus samt zugehöriger Schlüssel werden bekannt.
- Erhebliche Schwächen der eingesetzten Hard- und Software werden bekannt.

5.5.2 Zeitdauer zwischen Sperrantrag und Sperrung

Die PKI-Instanzen sperren bei Vorlage eines gültigen Sperrantrags das Zertifikat unmittelbar, spätestens jedoch am nächsten Arbeitstag.

5.5.3 Ausstellung von Sperrlisten

Die PKI-Instanzen erstellen automatisch eine aktuelle Sperrliste, sobald ein Zertifikat widerrufen wurde und veröffentlichen diese über die Validierungsdienste. Die neue Sperrliste wird den Validierungsdiensten unmittelbar zur Verfügung gestellt.

5.5.4 Bekanntgabe von Sperrungen

Die aktuelle Sperrliste der Root CA wird durch manuelle Publikation und von den untergeordneten Sub CAs automatisch den Validierungsdiensten zur Verfügung gestellt.

5.5.5 Kompromittierung des geheimen Schlüssels

Bei der Feststellung einer Schlüsselkompromittierung ist das zugeordnete Zertifikat unverzüglich zu sperren. Wurde der geheime Schlüssel der Root CA kompromittiert, müssen alle ausgegebenen CA- und End-Zertifikate sowie das eigene Root CA-Zertifikat unverzüglich gesperrt werden. Gleiches gilt bei der Kompromittierung von Sub CA Schlüsseln.

5.5.6 Suspendierung

Die Suspendierung von Zertifikaten ist in der gesamten Land Berlin PKI nicht vorgesehen.

5.6 Beweissicherung und Protokollierung

Alle administrativen Tätigkeiten werden über das Absicherungssystem der Administrationsumgebung protokolliert. Die Protokolle werden für einen Zeitraum von 90 Tagen gespeichert. Der Zugriff erfolgt immer im Mehr-Augen-Prinzip auf Anfrage des Informationssicherheitsbeauftragten des ITDZ Berlin oder des Cyber-Defense-Centers. Die protokollierten Daten wird durch die Administratoren des Absicherungssystems den Anfragenden nach Zustimmung des Personalrates zur Verfügung gestellt.

5.7 Schlüsselwechselmanagement

Beim Wechsel des Schlüssels der Root CA wird ein neues Root CA-Zertifikat ausgestellt. Gleiches gilt bei CA-Zertifikaten, die von der Root CA ausgestellt werden. Es wird mehrere gültige Root CA- und Sub CA-Zertifikate geben (vgl. Abschnitt 3.5).

5.8 Kompromittierung und Wiederherstellung

Die Root CA und die Sub CA verfügen über ein Notfallkonzept, welches die Wiederherstellung des ordnungsgemäßen Betriebes innerhalb einer angemessenen Frist sicherstellt.

Insbesondere wird darin die Kompromittierung des geheimen Schlüssels, das Bekanntwerden von Schwachstellen in den verwendeten kryptografischen Verfahren und die Nichtverfügbarkeit der Sperrlisten als Notfall betrachtet. Dieses Konzept ist Bestandteil des Betriebskonzepts [6] und unterliegt der ständigen Pflege.

5.9 Einstellen des Betriebs

Für den Fall, dass die Root CA oder eine Sub CA beabsichtigt den Betrieb als Zertifizierungsdiensteanbieter einzustellen, ist dies unter Einhaltung der folgenden Bedingungen rechtzeitig anzukündigen:

- Die Root CA kann den Betrieb mit einer Kündigungsfrist von 12 Monaten zum Ende des Quartals einstellen.
- Jede Sub CA kann den Betrieb mit einer Ankündigungsfrist von sechs Monaten ohne Angabe von Gründen einstellen.
- Die Ankündigung muss schriftlich erfolgen und ist zu veröffentlichen.
- Das Einstellen des Betriebs ist zwischen der Root CA und der Sub CA vertraglich geregelt.
- Die Root CA muss den Betrieb dann einstellen, wenn das Zertifikat kompromittiert wurde.

Mit Einstellung des Betriebes einer CA werden alle von ihren ausgestellten und noch gültigen Zertifikaten gesperrt. Werden Zertifikate nach der Ankündigung zur Einstellung des Betriebes ausgestellt, so ist die Gültigkeitsdauer auf den verbleibenden Restzeitraum des Betriebs einer CA beschränkt. Das Betriebskonzept regelt den Umgang mit den Unterlagen und Daten der CA, RA und LRA.

6 Profile für Zertifikate und Sperrlisten

6.1 Zertifikatprofil

Jedem Zertifikat muss durch die ausstellende CA eine eindeutige Seriennummer zugeordnet werden. Die Seriennummer enthält mindestens 64 Bit Zufallsdaten.

6.1.1 Versionsnummer

Zertifikate werden nach X.509v3 ausgestellt. Alle Zertifikate enthalten folgende Inhalte:

- Identifizierung der ausstellenden CA
- Der Name des Zertifikatinhabenden oder ein entsprechendes Pseudonym
- Der öffentliche Schlüssel, der mit dem privaten Schlüssel unter der Kontrolle des Zertifikatinhabenden korrespondiert
- Das Anfangs- und Enddatum der Gültigkeitsperiode des Zertifikats
- Die Seriennummer des Zertifikats
- Die elektronische Signatur der ausstellenden CA
- ggf. Einschränkungen der Einsatzmöglichkeiten des Zertifikats

6.1.2 Zertifikaterweiterungen

Grundsätzlich sind alle Zertifikaterweiterungen nach [X.509], [PKIX], [PKCS] sowie herstellerspezifische Erweiterungen zulässig.

Zertifikate für CA

In Zertifikaten für die CA müssen die Erweiterung keyUsage mit den Werten „keyCertSign“ und „cRLSign“ sowie die Erweiterung basicConstraints mit dem Wert „CA=True“ aufgenommen werden. Des Weiteren beinhalten Zertifikate für CAs eine Erweiterung cRLDistribution- Point mit einem Verweis auf die zugehörige Sperrliste und eine Erweiterung authorityInfoAccess mit einem Verweis auf das signierende CA-Zertifikat.

End-Entity-Zertifikate

Zertifikate für alle anderen Verwendungszwecke werden optional mit der Erweiterung basic-Constraints mit dem Wert „CA=False“ als Nicht-CA-Zertifikat markiert und tragen keine CAspezifische keyUsage-Erweiterung, d. h. die Erweiterung keyUsage darf nicht die Werte „keyCertSign“ oder „cRLSign“ beinhalten.

Die keyUsage-Erweiterung darf nur mit dem Wert „nonRepudiation“ belegt werden, wenn keine Wiederherstellung des privaten Schlüssels möglich ist und der private Schlüssel durch technische und organisatorische Maßnahmen nur dem Zertifikatinhaber/in zugänglich ist. End-Entity-Zertifikate enthalten immer die Erweiterung cRLDistributionPoint mit einem Verweis auf die zugehörige Sperrliste und die Erweiterung authorityInfoAccess mit einem Verweis auf das signierende CA-Zertifikat. Zertifikate für Datenverarbeitungssysteme sowie Zertifikate für natürliche Personen und Gruppen beinhalten zusätzlich immer die Erweiterung authorityInfoAccess.

6.1.3 Objekt Identifikatoren von Algorithmen

Objekt Identifikatoren für Algorithmen werden nach PKIX verwendet.

6.1.4 Namensformen

Siehe Abschnitt 4.1.3

Domainnamen und IP-Adressen, die im Subject-DN enthalten sind, werden immer auch in den alternative Zertifikatnamen („subjectAlternativeName“) unter den Typen „dNSName“ bzw. „iPAddress“ aufgeführt.

6.1.5 Namensbeschränkungen

Es wird keine Erweiterung nameConstraints verwendet.

6.1.6 Objekt Identifikator der Policy in Zertifikaten

Die folgenden OIDs werden in alle End-Entity-Zertifikate aufgenommen:

1.3.6.1.4.1.10769.509.10.2.100.10.2.20: Kennzeichnung der Policy des Basisdienst Land Berlin PKI, Berlin Class2 Typ2 CA 2022

6.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkung

Keine Angaben.

6.1.8 Syntax und Bedeutung von Richtlinienkennungen

Siehe Abschnitt 1.2.

6.1.9 Abarbeitung von kritischen Erweiterungen der CP

Keine Angaben.

6.2 CRL Profil

Für jede CA in des Basisdienst Land Berlin PKI, wird eine CRL bereitgestellt. Diese enthält die gesperrten Zertifikate der jeweiligen CA. Jede CRL enthält folgende Informationen:

- Versionsnummer (siehe Abschnitt 7.2.1)
- Signaturalgorithmus
- Identifizierung der ausstellenden CA
- Zeitpunkt der Ausstellung im Feld thisUpdate
- Spätester Zeitpunkt des nächsten Updates im Feld nextUpdate
- Seriennummern und Sperrungsdaten der gesperrten Zertifikate
- Die elektronische Signatur der ausstellenden CA

6.2.1 Versionsnummer

Sperrlisten werden nach X.509 in der Version 2 erstellt.

6.2.2 Erweiterungen von CRL und CRL Einträgen

Es werden die Erweiterungen cRLNumber und authorityKeyIdentifier (Variante keyid) und crlNextPublish (OID 1.3.6.1.4.1.311.21.4) gesetzt.

6.2.3 Gültigkeitsdauer

Die Gültigkeitsdauer der CRL (nextUpdate) ist 8 Tage nach dem Zeitpunkt der Ausstellung (thisUpdate). Der Wert für Erweiterung crlNextPublish wird auf 4 Tage nach dem Zeitpunkt der Ausstellung gesetzt.

7 Konformitätsprüfung

Die Konformität des Betriebs der PKI zu den Vorgaben dieses CPS und des Sicherheitskonzeptes wird mit internen Audits überprüft. Die Audits werden durch das Informationssicherheitsmanagement gesteuert.

7.1 Frequenz und Umstände der Überprüfung

Als Bestandteils des Informationssicherheitsmanagements wird ein jährliches Audit durchgeführt.

7.2 Identität des Überprüfenden

Audits werden im Regelfall durch Mitarbeitende der ITDZ Berlin in Begleitung eines externen Auditors durchgeführt.

7.3 Verhältnis von Prüfenden zu Überprüftem

Prüfende haben keine Rolle PKI-/CA-Administration, RA/LRA oder Backup-Operator inne (siehe Abschnitt 8.2).

7.4 Überprüfte Bereiche

Es wird der Betrieb des Basisdienst Land Berlin PKI beim ITDZ Berlin überprüft.

7.5 Mängelbeseitigung

Aufgedeckte Mängel werden in einem dem Risiko angemessenen Zeitrahmen behoben.

7.6 Veröffentlichung der Ergebnisse

Ergebnisse werden im Regelfall nicht veröffentlicht.

8 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen für CAs

Alle infrastrukturellen, organisatorischen und personellen Sicherheitsmaßnahmen sind in einem Sicherheitskonzept dargelegt. Die im Folgenden beschriebenen Maßnahmen beziehen sich auf den Betrieb des PKI-Dienst in Bezug auf Zutrittsregelungen, Stromversorgung, Klimatechnik, Brandschutz und Speichermedien.

8.1 Infrastrukturelle Maßnahmen

8.1.1 Lage

Die Betriebskomponenten des PKI-Dienst befinden sich im High Secure Datacenter des ITDZ Berlin. Dort sind die Server des PKI-Dienst und der Validierungsdienste untergebracht. Das High Secure Datacenter erfüllt alle Sicherheitsanforderungen des behördlichen und des Berliner Datenschutzbeauftragten für den hohen und sehr hohen Schutzbedarf.

8.1.2 Zutritt

Das High Secure Datacenter ist zum Schutz gegen unbefugten Zutritt mechanisch gesichert. Eine strenge Zugangssicherung und -kontrolle mit Videoüberwachung ist in jedem Sicherheitsraum gewährleistet. Für betriebsfremde Personen ist der Zutritt zu den Büros der PKI-Mitarbeiter ohne vorherige Anmeldung nicht möglich. Die Büros der Mitarbeiter befinden sich in zutrittsgesicherten Etagen, und ein permanent besetzter Besucherempfang kontrolliert den Zutritt zum Gebäude des ITDZ Berlin.

8.1.3 Stromversorgung und Klimatechnik

Die Räume des High Secure Datacenter sind ausgestattet mit:

- Klimaanlage
- unterbrechungsfreie Stromversorgung (USV) und Notstromversorgung

Durch USV und Klimatisierung der technischen Infrastruktur der PKI werden Betriebsbeeinträchtigungen verhindert.

8.1.4 Brandschutz

Die Räume des High Secure Datacenter des ITDZ Berlin sind mit einer Brandmeldeanlage überwacht und mit Brandabschottungen und sauerstoffreduzierten Räumen ausgestattet.

8.1.5 Speichermedien

Im Betriebskonzept wird der Umgang mit den folgenden schützenwerten Daten zur Sicherung, Wiederherstellung, Archivierung und Vernichtung geregelt:

- Schlüssel der Sub CA
- Backup der Schlüssel
- Protokolldaten

8.2 Organisatorische Maßnahmen

Nachfolgend wird auf die Rollen sowie deren Zuständigkeiten eingegangen. Dazu wird eine RACI-Matrix verwendet. Die RACI-Matrix enthält verschiedene Rollen:

	R	A	C	I
PKI-/CA-Administration	X	X	X	
RA/LRA	X			X
Backup-Operator	X			
Auditor (Unternehmensicherheit)				X

Tabelle 8: PKI Rollen - RACI Matrix

- Responsible (verantwortlich): Eine Person mit diesem Status trägt die Verantwortung dafür, dass eine Aufgabe durchgeführt, erledigt oder erfüllt wird und das erwartete Ergebnis vorliegt. Responsible kann auch bedeuten, dass der betreffende Mitarbeiter oder die Mitarbeiterin die Aufgabe nicht (vollständig) selbst durchführen, sondern die Aufgabe lediglich initiiert/delegiert und für die Umsetzung der Aufgabe sorgt.
    - Das PKI-Team ist verantwortlich für die Bereitstellung und den Betrieb des PKI-Dienst. Dazu zählen die
        - Root CA (Host + Server VM)
        - Sub CAs (Server VMs)
        - CDP/AIA (Server VMs)
        - HSMs (Hardware Appliances)
    - Die RA/LRA ist verantwortlich für die Prüfung der Zertifikatsanträge, über den PKI-Dienst, auf die Richtigkeit und Vollständigkeit der Zertifikatsanträge.
- Accountable (rechenschaftspflichtig): Eine Person muss als accountable sicherstellen, dass das Arbeitsergebnis den Erwartungen und Anforderungen der Stakeholder entspricht. Die Accountable-Rolle prüft und genehmigt Ereignisse, gibt Produkte nach deren Fertigstellung oder auch nur Ressourcen in Form von Kosten (Budget) frei.

    - Das PKI-Team ist der Leitung des ITDZ Berlin den Betrieb des PKI-Service rechenschaftspflichtig.

- Consulted (konsultiert, herangezogen): Die konsultierte Person wird beratend zu einer Aufgabe oder einer Tätigkeit hinzugezogen. Es handelt sich um eine erfahrene Expertin oder einen erfahrenen Experten im jeweiligen Fachbereich, weil sie Wissen haben, das für die Erreichung eines bestimmten Ergebnisses oder das Fertigstellen einer Aufgabe wichtig ist.
    - Das PKI-Team kann zum Betrieb des PKI-Dienstes mit Fachwissen beraten. Bei Bedarf können auch externe Berater dem ITDZ Berlin und dem PKI-Team beratend hinzugezogen werden
- Informed (informiert): Mitarbeitende in dieser Rolle werden über betreffende Aufgaben oder Tätigkeiten informiert. Es wird meistens eine Unterteilung in diese 2 möglichen Informierten vorgenommen:
    - Informationspflicht: Die Person muss (regelmäßig) über Tätigkeiten informiert werden. Es besteht eine Bringschuld.
    - Informationsrecht: Die Person hat das ausdrückliche Recht, Informationen einzuholen. Es besteht eine Holschuld.

8.3 Personelle Maßnahmen

Um eine Rolle beim Betrieb der Sub CA wahrnehmen zu können, erfüllen jeweils in der Rolle tätigen Mitarbeiter die folgenden Voraussetzungen:

- qualifizierte Ausbildung im IT-Bereich,
- qualifizierte Ausbildung im Windows Server Umfeld,
- sachkundige Qualifikation,
- Erfahrung und Zuverlässigkeit im Sachgebiet.

9 Technische Sicherheitsmaßnahmen für Zertifizierungsstellen

Für die technischen Sicherheitsmaßnahmen wird ein Sicherheitskonzept angefertigt und umgesetzt, das den Anforderungen des IT-Grundschutzhandbuchs [7] für den hohen und sehr hohen Schutzbedarf entspricht.

9.1 Schlüsselgenerierung und -installation

9.1.1 Schlüsselgenerierung

Alle Schlüsselpaare für die Berlin Zertifizierungsstelle werden durch das Netzwerk-HSM (Hardware Security Modul) generiert. Die generierten CA Schlüssel werden auch durch das Netzwerk-HSM kryptographisch geschützt. In jegliche Prozesse, die den Zugriff auf den privaten Schlüssel der Zertifizierungsstellen erforderlich machen, ist das HSM zwingend eingebunden.

9.1.2 Übergabe der öffentlichen Schlüssel und Zertifikate

Als Ergebnis des Zertifizierungsantrags (Certificate Signing Request) der SubCA übergibt die Root CA den berechtigten Mitarbeitern der Sub CA das Zertifikat. Zuvor wurde der öffentliche Schlüssel zusammen mit anderen Zertifizierungsdaten (wie z.B. DN, Gültigkeit etc.) von der Root CA signiert.

Die Übergabe der öffentlichen Schlüssel der Zertifikatnehmer erfolgt als Software-Zertifikat in Form einer PKCS#7 Datei. Im Falle der Erstellung von geheimen Schlüsseln, erfolgt die Bereitstellung Schlüssel für die Zertifikatnehmer als Soft-PSE (PKCS#12-Datei). Ein zusätzliches PIN-Schreiben zum Entsperren des geheimen Schlüssels wird dem ZN auf einem getrennten Übertragungsweg übermittelt (vgl. Abschnitt 5.2).

9.1.3 Akzeptanz von Zertifikaten

Die Sub CA im ITDZ Berlin wird die Authentizität des übermittelten Wurzelzertifikats, dessen Integrität anhand des veröffentlichten Fingerabdrucks und die Akzeptanz des zuständigen CA-Zertifikats überprüfen. Nur wenn sich dabei Fehler herausstellen, erfolgt eine Meldung an die Root CA. Für die Zertifikatnehmer der Sub CA im ITDZ Berlin gelten analoge Regelungen (vgl. Abschnitt 5.3).

9.1.4 Kryptoalgorithmen, Schlüssellänge, Parametergenerierung

Die Berlin Class2 Typ2 CA verwendet als kryptographische Algorithmen SHA256 für die Signatur sowie RSA mit einer Länge von 4096 Bit für das Schlüsselmaterial.

Die festgelegte Schlüssellänge für Endzertifikate beträgt bei der Verwendung von RSA 4096 Bit. Mit Ausnahmegenehmigung durch den Informationssicherheitsbeauftragten ist in Sonderfällen eine Schlüssellänge von 2048 Bit für RSA-Schlüssel zulässig. Eine solche Ausnahmegenehmigung ist regelmäßig, mindestens einmal jährlich, auf ihre Notwendigkeit zu überprüfen.

Bei Verwendung von Elliptischen Kurven für das Schlüsselmaterial beträgt die Mindestschlüssellänge 256 Bit.

Die Signatur der Endzertifikate erfolgt mit SHA256.

9.1.5 Schlüsselnutzung

Der geheime Schlüssel der Sub CA wird ausschließlich zum Signieren der öffentlichen Schlüssel von Zertifikatnehmern sowie untergeordneten Zertifizierungsinstanzen und der Sperrliste verwendet.

9.2 Schutz des geheimen Schlüssels

9.2.1 Schlüsselteilung

Eine Schlüsselteilung ist von der Sub CA im PKI-Dienst nicht vorgesehen.

9.2.2 Key Escrow

Eine Schlüsselhinterlegung im klassischen Sinne eines Trust Centers ist bei Sub CA des PKI-Dienst nicht vorgesehen.

9.2.3 Wiederherstellung des privaten Schlüssels

Der geheime Schlüssel Sub CA sowie der von ihr zertifizierten Instanzen, die nicht selbst einen Certificate Signing Request erzeugt haben, ist über ein gesichertes HSM Backupverfahren wiederherstellbar. Das Backupverfahren ist im Betriebskonzept [6] beschrieben.

Die Wiederherstellung der von der Sub CA erstellten geheimen Schlüssel der Zertifikatnehmer ist nur in begründeten Ausnahmefällen und unter Einhaltung der im Betriebskonzept [6] geregelten Prozeduren möglich. Begründete Anforderungen sind z. B.:

- Ein Zertifikatnehmer hat sein Zertifikat verloren und benötigt das Zertifikat, um an zuvor Verschlüsselte Daten (z. B. mit S/MIME verschlüsselte E-Mails) zu gelangen.
- Die Sicherstellung der Informationsverfügbarkeit nach Ausscheiden eines Mitarbeiters einer Behörde/Verwaltungsstelle. In diesem Fall Bedarf die Wiederherstellung der Genehmigung des Vorgesetzten, der Personalvertretung, des Datenschutzes und des Sicherheitsbeauftragten.

9.2.4 Archivierung des privaten Schlüssels

Die geheimen Schlüssel der Sub CA werden ausschließlich in Netzwerk-HSM gespeichert. Ein Export der privaten Schlüssel wird nicht durchgeführt.

9.2.5 Schlüsselinstallation und Aktivierung

Der geheime Schlüssel der Sub CA wurde im ITDZ Berlin von berechtigten Mitarbeitern des PKI-Teams mittels HSM generiert. Die Generierung von öffentlichen Schlüsseln für Zertifikate/ für Zertifikatnehmer und Zertifizierungsinstanzen erfolgt nach vorheriger Überprüfung der Zertifikatsanträge. Die Privaten Schlüssel der Zertifikatsnehmer werden automatisiert bei den Antragstellern (Autoenrollment) oder bei Antragstellung erzeugt. Bei dem Sub CA-Server erzeugt die Sub CA mithilfe des HSMs ihre privaten Schlüssel. Zertifikatnehmer im Active Direcory die am MS-Autoenrollment Verfahren teilnehmen, erzeugen ihre privaten Schlüssel selbst auf den jeweiligen Geräten.

Zertifikatnehmer, denen ein asymmetrisches Schlüsselpaar generiert wurde, benötigen für die Installation ihres Zertifikats eine beim Download festzulegende PIN/Passphrase, die nur ihnen bekannt ist.

9.2.6 Schlüsselvernichtung

Nach Ablauf der Gültigkeit oder nach Sperrung der Sub CA-Zertifikate wird der geheime Schlüssel zuverlässig vernichtet.

9.3 Weitere Aspekte des Schlüsselmanagements

9.3.1 Archivierung öffentlicher Schlüssel

Alle von den Zertifizierungsdiensten ausgestellten Zertifikate werden in der Zertifizierungsstellendatenbank archiviert. Darüber hinaus findet keine Archivierung öffentlicher Schlüssel statt.

Ein öffentlicher Zugriff auf die Archivdaten für Zertifizierungsinstanzen und Zertifikatnehmer besteht nicht. Sämtliche öffentlichen Zugriffe auf aktuelle Zertifikate und Sperrlisten erfolgen nur über die entsprechenden Verzeichnisdienste (vgl. Abschnitt **Fehler! Verweisquelle konnte nicht gefunden werden.**).

9.3.2 Nutzungsdauer für öffentliche und private Schlüssel

Die Nutzungsdauer des Sub CA Schlüsselpaares stimmt grundsätzlich mit der Nutzungsdauer des dazugehörigen Zertifikats überein. Die maximale Gültigkeit eines Sub CA Zertifikats beträgt fünf

Jahre. Ein neues Sub CA Zertifikat wird bei der Root CA in Form eines Certificate Signing Request beantragt.

Auch bei Zertifikaten für Zertifikatnehmer und Zertifizierungsinstanzen einer Sub CA stimmt die Nutzungsdauer des Schlüsselpaares grundsätzlich mit der Nutzungsdauer des dazugehörigen Zertifikats überein. Die maximale Gültigkeit eines Zertifikats für Zertifikatnehmer und Zertifizierungsinstanzen beträgt zwischen einem und zwei Jahren (vgl. Abschnitt 3.5). Über die RA kann die Verlängerung des Zertifikats beantragt werden, damit ein neues Schlüsselpaar von einer Sub CA nach vorheriger Identitätsprüfung generiert bzw. der öffentliche Schlüssel des Antragstellers durch die Signatur der Zertifizierungsstelle bestätigt wird. Für Maschinen im zentralen AD (MS-Autoenrollment) werden automatisch neue Schlüssel innerhalb des Überlappungszeitraumes ausgestellt.

9.3.3 Aktivierungsdaten

Private Signaturschlüssel einer Zertifizierungsstelle werden im HSM nach Authentisierung der Schlüsselverantwortlichen mittels Chipkarten des HSM unter Einhaltung des Vier-Augen-Prinzips aktiviert.

10 Profile für Zertifikate und Sperrlisten

Die Festlegung der Profile des SubCA-Zertifikats und dessen beglaubigte Zertifikate entsprechen ebenso wie die Verwendung von Zertifikatserweiterungen der MailTrusT-Spezifikation der Version 2 (MTTv2) [7]. Ebenfalls ist in der MTTv2-Spezifikation das Profil der Sperrlisten (CRL) einschließlich der Sperrlistenerweiterungen geregelt. Das aktuelle CRL-Format ist CRLv2.

11 Änderung und Anerkennung dieser Policy

11.1 Policy Object Identifier

Die ITDZ Enterprise OID lautet 1.3.6.1.4.1.10769 (Private Enterprise Code)

Berlin Class2 Typ2 CA 2022

Policy: OID: 1.3.6.1.4.1.10769.509.10.2.100.10.2.20

CPS: OID: 1.3.6.1.4.1.10769.509.10.2.100.10.2.21

11.2 Änderungsmanagement

Aktualisierungen der vorliegenden Policy werden nach Änderungen der Dokumente zeitnah vorgenommen. Eine Aktualisierung der Policy wird nur dann den Teilnehmern offiziell bekannt gegeben, falls dies erforderlich ist.

Bei Änderungen wird unterschieden, ob diese die Sicherheit betreffen beziehungsweise Änderungen der Abläufe seitens der Endanwender erfordern und daher einer generellen Bekanntmachung gegenüber den Endanwendern unterliegen.

Die Anpassung und Einhaltung der Policy wird durch einen Auditor überwacht.

11.2.1 Änderungen, die keiner Bekanntmachung unterliegen

Änderungen dürfen dann ohne Bekanntmachung erfolgen, wenn diese nicht relevant für die Sicherheit sind, beziehungsweise keine Änderungen seitens der Abläufe der Endanwender (Registrierung, Prüfung von Zertifikaten, Sperrungen usw.) erfordern. Insbesondere können Korrekturen zur Typographie und Layout ohne weitere Bekanntmachung erfolgen.

11.2.2 Änderungen, die eine Bekanntmachung erfordern

Änderungen, die die Sicherheit oder die Abläufe der Endanwender betreffen, erfordern eine zeitnahe Bekanntmachung.

11.2.3 Verfahren zur Publizierung und Bekanntgabe

Die aktuelle Version sowie ältere Versionen der Policy können auf der Internetseite des ITDZ Berlin abgerufen werden. An gleicher Stelle wird auch rechtzeitig bekannt gegeben, wenn eine neue Version der Policy in Vorbereitung ist.

11.2.4 Anforderung an die Änderung der Version

Die Hauptversion für dieses Dokument wird geändert werden, wenn die Änderung eine Bekanntmachung erfordert. Zertifikate, die nach der alten Version der Policy ausgestellt wurden, werden nicht geändert. Die Zertifikate, welche nach der Änderung der Policy beantragt werden, werden nach den geänderten Festlegungen der Policy ausgestellt.

11.3 Anerkennung

Die Root CA und die Sub CAs verpflichten sich, die vorliegende Policy einzuhalten und die Sicherheitsrichtlinien der Wurzelzertifizierungsinstanz des Basisdienstes Land Berlin PKI anzuerkennen. Auch die Zertifikatnehmer werden auf ihre Rechten und Pflichten als Bestandteil der Basisdienstes Land Berlin PKI bei der Zertifikatsbeantragung hingewiesen und stimmen der Policy zu.

Verweise

Literaturverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik, „Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften," 16 05 2001. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/sigg2001_pdf.pdf?__blob=publicationFile&v=1.

[2] Request for Comments, „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," 05 2008. [Online]. Available: https://www.rfc-editor.org/rfc/rfc5280.

[4] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kompendium," 01 02 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1.

[5] BSI, „Technische Richtlinie TR-02102-3 Kryptographische Verfahren," [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-3.pdf?__blob=publicationFile&v=3.

[6] TeleTrusT, „MailTrusT Version 2, Gesamtkonzeption, Aufbau und Komponenten einer PKI," 16 03 1999. [Online]. Available: https://www.teletrust.de/fileadmin/files/ag8_20mttv2-1.pdf.

[7] IT-Dienstleistungszentrum Berlin, Policy der ITDZ PKI (OID: 1.3.6.1.4.1.10769.50.2), 2022.

[9] Bundesamt für Sicherheit in der Informationstechnik, „BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen," [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html.

[10] ITDZ Berlin, „CP+CPS der Berlin Class2 Typ2 CA 2022," 2022. [Online]. Available: https://www.class2.pki.verwalt-berlin.de/www/Berlin-Class2-Typ2-CA-2022/.

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AD	Active Directory
CA	*Certification Authority*
CRL	*Certificate Revocation List*
CSP	*Cryptographic Service Provider*
DN	*Distinguished Name*
DNS	*Domain Name Service*
HSM	*Hardware Security Module*
LRA	*Local Registration Authority*
OID	*Object Identifier*
SAN	*Subject Alternative Name*
UPN	*User Principal Name*
VLAN	*Virtual Local Area Network*