ITDZ BERLIN

Policy der ITDZ PKI

OID: 1.3.6.1.4.1.10769.50.2

ITDZ BERLIN

Inhalt

Inhalt

Inhalt

Abkürzungsverzeichnis

AD	Active Directory
BMI	Bundesministerium des Inneren
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority (Zertifizierungsstelle)
CN	Common Name (gebräuchlicher Name)
DN	Distinguished Name (eindeutiger Name)
FQDN	Fully Qualified Domain Name, der vollständige DNS-Name eines Computers
ISIS	Industrial Signature Interoperability Specification
ITU-T	International Telecommunications Union-Telecommunication
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung
HSM	Hardware Security Modul
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority (lokale Registrierungsstelle)
MTT	MailTrusT
OID	Object Identifier
PCA	Policy Certificate Authority (Wurzelzertifizierungsstelle)
PIN	Personal Identification Number (persönliche Identifikationsnummer)
PKI	Public Key Infrastructure (öffentliche Schlüssel Infrastruktur)
PKIX	Public Key Infrastructure X.509
PSE	Personal Security Environment (persönliche Sicherheitsumge-bung)
RA	Registration Authority (Registrierungsstelle)
RSA	Asymmetrischer Verschlüsselungsalgorithmus nach Rivest-Shamir- Adleman
SAN	SubjectAlternateName, alternativer Zertifikatsname, enthalten in den erweiterten Eigenschaften eines Zertifikats
S/MIME	Secure Multipurpose Internet Mail Extension
UPN	UserPrincipalName, ein Benutzeranmeldename im Active Directory
ZN	Zertifikatnehmer

1 Einleitung

Dieses Dokument enthält die Zertifizierungsrichtlinien der Policy Certification Authority (PCA) für das IT-Dienstleistungszentrum Berlin (ITDZ) und bezieht sich auf die im ITDZ aufgebaute zertifikatbasierte Schlüsselinfrastruktur (PKI). Das ITDZ baut eine dreistufige PKI (PCA, CA, Zertifikat) auf.

Die in diesem Dokument getroffenen Aussagen sind für die Arbeit der Berlin PCA und der durch sie zertifizierten CAs (Certification Authorities) bindend. Die angeschlossenen CAs werden ebenso zum Bestandteil der ITDZ-PKI wie die durch sie zertifizierten Instanzen und Zertifikatnehmer (RA und ZN). Die Berlin PCA und die angeschlossenen CAs zertifizieren ausschließlich nach den Richtlinien dieser Policy.

Darüber hinaus kann das ITDZ weitere PKI aufbauen, welche nach eigenen Zertifizierungsrichtlinien arbeiten.

2 Überblick

2.1 Aufbau der PKI und ihrer Schnittstellen

Das ITDZ baut eine hierarchisch strukturierte PKI für die zertifikatbasierte Sicherung der IT-Anwendungen

- E-Mail Verschlüsselung
- E-Mail Signaturen (digitale Unterschriften)
- SSL- Zertifikate für Heimarbeitsplätze der Nutzer
- SSL- Zertifikate für Mobile Endgeräte
- SSL- Zertifikate für Web –Server und Gateways
- IPSec Zertifikate für VPN-Gateways, Server und Client
- IPSec Zertifikate für Domänencontroller
- Code-Signaturen
- Software Einschränkungen auf Zertifikatsbasis (Windows 2003 und höher)
- Möglichkeit der Festplattenverschlüsselung für Laptops unter Windows XP und höher
- Key Recovery Möglichkeit für User Zertifikate
- Smart Card – Anmeldung
- EAP (Extensible Authentication Protocol)

auf. Die PKI basiert auf Windows Server 2012 R2 Software, dem Standard X.509v3 und zwei Hardware Security Modulen. Durch die aufgebaute Vertrauensinfrastruktur wird die Gültigkeit des öffentlichen Schlüssels eines Zertifikatnehmers mit den dazugehörenden Identifikationsmerkmalen (wie Schlüsselinhaber, beglaubigende Stelle, Gültigkeitszeitraum etc.) durch die elektronische Signatur der Zertifizierungsinstanz (PCA, CA) beglaubigt. Mit den 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.
Bei der verschlüsselten Kommunikation mit einem zertifizierten Server ist gewährleistet, dass es sich wirklich um den angegebenen Server handelt. Gleiches gilt auch bei der gesicherten Daten- und Informationsübertragung über öffentliche Netze durch IPSec Zertifikate 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 Hardware Security Module (HSM) eingesetzt, um eine Ausfallsicherheit zu gewährleisten. Diese Geräte garantieren die Generierung und Speicherung von hardwarebasierenden Zertifikaten mit einem eigenen mitgelieferten CSP (Cryptographic Service Provider). Der Einsatz der HSM sieht den Schutz der CA Server, also der Zertifizierungsstellen vor. Der Zugriff auf diese Module ist nur direkt am Gerät möglich und Änderungen können nur mit Hilfe der Administrator bzw. Operator Card Sets erfolgen. Die HSM übernehmen auch die Signierung der für die Issuing CAs bereitgestellten Sperrlisten.

Der private Schlüssel der Zertifizierungsstelle wird durch das HSM selbst erzeugt und kann aus dem HSM nicht 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 CAs erfolgt über eine konfigurierte Security World und ist damit 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 der ITDZ-PKI dienen der Absicherung der online Kommunikation durch sichere elektronische Signatur (nach dem Signatur-Gesetz von 2001) und der Verschlüsselung.

2.2 Zertifizierungshierarchie

Die Registrierungsstellen für Endanwender-Zertifikate werden lokal an unterschiedlichen Standorten durch Angestellte der öffentlichen Verwaltung des Landes Berlin betrieben.
Das ITDZ betreibt eine zentrale Registrierungsstelle zur Antragstellung und Registrierung aller von ihr unterstützten Zertifikate. Das folgende Bild veranschaulicht den Aufbau.

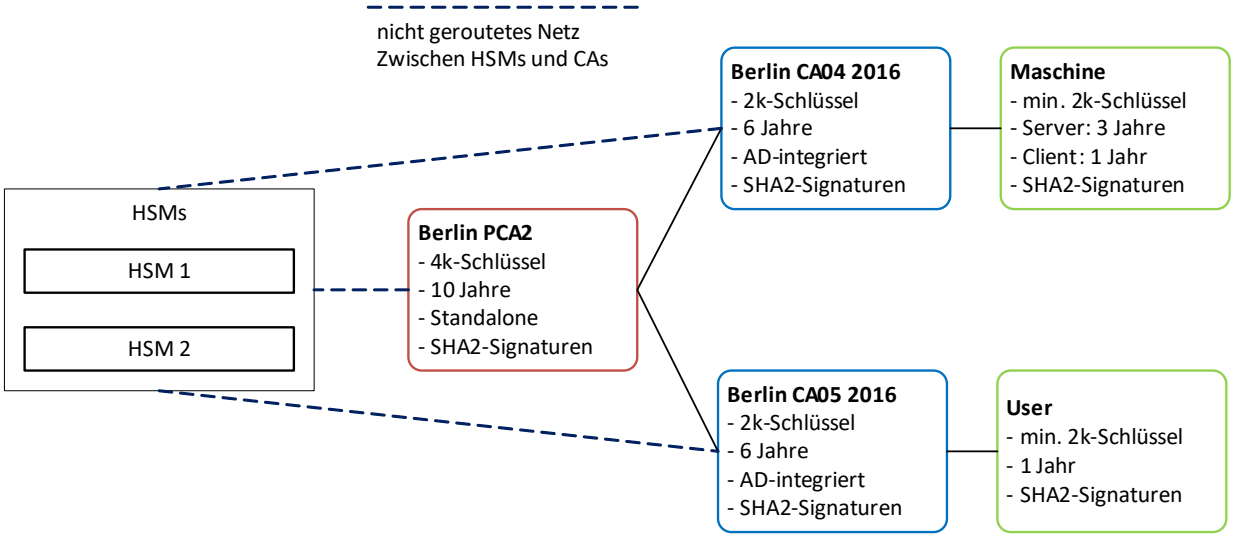

Abbildung 1 Architektur der PKI mit angeschlossenen CAs

Die Wurzelzertifizierungsstelle (Berlin PCA2) des ITDZ erstellt als oberste Zertifizierungsstelle der Hierarchie ein selbstsigniertes Wurzelzertifikat und signiert die Zertifikate der angeschlossenen Zertifizierungsstellen.
Die von der Wurzelzertifizierungsstelle zertifizierten Zertifizierungsstellen (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.
Zertifikatnehmer sind Personen und Maschinen (Server 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 beantragt. PKI-Informationen werden über die Verzeichnisdienste der ITDZ-PKI abgerufen.

Unterhalb der Berlin PCA2 besteht die Unterstruktur im Land Berlin aus drei verschiedenen Ebenen:

1. Zertifizierungsinstanzen CAs
2. Registrierungsinstanzen (RA und LRA)
3. Zertifikatnehmer (ZN) für folgende IT-Anwendungen:

- *AD- Nutzer und Komponenten für Verschlüsselung; Signatur, Authentication und IPSec-Verbindungen*
- *externe Nutzer und Komponenten für Verschlüsselung, Signatur, Authentication und IPSec-Verbindungen*
- *Code Signatur*
- *Client Authentication Nortel/Netscreen VPN*
- *Server Authentication Nortel/Netscreen VPN*

4. 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 Sicherung der IT- Anwendungen:

- **User**-Zertifikate werden von der **Berlin CA05 2016** ausgestellt und signiert.
- **Maschinen**-Zertifikate werden von der **Berlin CA04 2016** ausgestellt und signiert.

Mit der ITDZ PKI ist es auch möglich, dass Behörden eine eigene, durch die landeseigene Root-CA signierte Zertifizierungsstelle betreiben, um z.B. eigene, ihren Wünschen angepasste Zertifikate ausgeben zu können.

2.4 Verzeichnisdienst

Der Typ des Zertifikats entscheidet beim Zertifikatsantrag darüber, ob und wo (intern und/oder extern) das Zertifikat veröffentlicht wird. Die von den Berlin PCA und den CAs erzeugten Zertifikate sowie die Sperrlisten (CRL) zurückgezogener Zertifikate werden, falls im Antrag nicht ausgeschlossen, in internen sowie externen ITDZ-Verzeichnisdiensten veröffentlicht. Die Daten werden sowohl auf Web-Servern als auch im zentralen AD des Landes Berlin bereitgestellt.

Folgende Web-Veröffentlichungsorte sind vorgesehen:

ITDZ-Berlin CP	-	http://pki.verwalt-berlin.de/Berlin/CPS/Policy.pdf
ITDZ-Berlin CPS	-	http://pki.verwalt-berlin.de/pki/cps.htm
ITDZ-Berlin CRLs	-	Berlin PCA2 http://pki.verwalt-berlin.de/PKI/BerlinPKI/CDP/Berlin%20PCA2(2).crl

	- Berlin CA04 2016 http://pki.verwalt-berlin.de/PKI/BerlinPKI/CDP/Berlin%20CA04%202016.crl - Berlin CA05 2016 http://pki.verwalt-berlin.de/PKI/BerlinPKI/CDP/Berlin%20CA05%202016.crl
ITDZ-Berlin CA-Zertifikate	- Berlin PCA2 http://pki.verwalt-berlin.de/PKI/BerlinPKI/AIA/ITPCA2.it.verwalt-berlin.de_Berlin%20PCA2(2).crt - Berlin CA04 2016 http://pki.verwalt-berlin.de/PKI/BerlinPKI/AIA/ITCA004.it.verwalt-berlin.de_Berlin%20CA04%202016(1).crt - Berlin CA05 2016 http://pki.verwalt-berlin.de/PKI/BerlinPKI/AIA/ITCA005.it.verwalt-berlin.de_Berlin%20CA05%202016(1).crt

Als LDAP-Veröffentlichungsort für Sperrlisten und Zertifikate ist der jeweilige Standardpfad im zentralen AD vorgesehen.

2.5 Anwendungsbereich

Auf Antrag erzeugt die Berlin PCA durch ein HSM X.509v3-Zertifikate für Zertifizierungsstellen (CAs), die wiederum auf Antrag verschiedene Zertifikate (ZN) erzeugen.
Darüber hinaus können die jeweiligen CAs für weitere Registrierungs- und Zertifizierungsinstanzen (RAs) Zertifikate ausstellen.
Der Zuständigkeitsbereich der Berlin PCA und der angeschlossenen CAs umfasst alle Einrichtungen der Berliner Verwaltung. Weitere Organisationen und Teilnehmer können auf Anfrage zertifiziert werden.

Diese Policy unterstützt das Zertifikat-Format X.509v3, das in aktuellen Standard-Browsern für unterschiedliche Anwendungen eingesetzt wird. X.509v3 ist ein Standardformat der ITU-T für Zertifikate (International Telecommunications Union-Telecommunication). 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.509v3 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 zu den Wurzelzertifizierungsstellen und zu den angeschlossenen CAs.
Die Wurzelzertifizierungsstelle (Berlin PCA2) und die angeschlossenen CAs werden vom ITDZ für das Land Berlin betrieben.

2.6.2 Ansprechstelle der Zertifizierungsstelle

Die Berlin PCA2 und Berlin CAs werden von Mitarbeitern aus dem entsprechenden Fachgebiet des ITDZ betrieben. Diese Informationen werden im Betriebskonzept [1] erarbeitet und im Betriebshandbuch fortgeschrieben.
Erreichbar sind die Mitarbeiter der Berlin PCA2 und der Berlin CAs 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 Wurzelzertifizierungsstelle Berlin PCA

Die Wurzelzertifizierungsstelle (Berlin PCA) übernimmt folgende Verpflichtungen:

- Sie erzeugt über das HSM ein kryptografisch geeignetes Schlüsselpaar in einer gesicherten Umgebung.
- Sie erzeugt ihr selbstsigniertes Zertifikat.
- Sie erstellt die Sicherheitsrichtlinien (Policy) der PCA und hält sich an diese.
- Von ihr werden folgende Informationen veröffentlicht:
    - ihr integres und authentisches Zertifikat mit dazugehörigem Fingerabdruck,
    - die von ihr ausgestellten (CA) Zertifikate,
    - die Sperrliste der Zertifizierungsstellen

3.2 Verpflichtungen der untergeordneten Zertifizierungsstellen

- Jeder Berlin CA wird ein eindeutiger Name zugeteilt, der innerhalb der gesamten PKI gilt. Damit wird sichergestellt, dass die vereinbarten Namensbestandteile in ihrem Zuständigkeitsbereich verwendet werden.
- Mit Installation ist die CA an die Einhaltung und Erfüllung der in den Sicherheitsrichtlinien der Berlin PCA gestellten Anforderungen gebunden (auf HSM basierender Aufbau).
- Jede Berlin CA ist an die Einhaltung des durch die Wurzelzertifizierungsstelle (Berlin PCA) festgelegten Namensraumes gebunden (auf HSM basierender Aufbau).
- Die Einhaltung der Sicherheitsrichtlinien ist durch die Nutzung des HSM vorgegeben.
- Über die Berlin CAs ist jederzeit der Nachweis zur Zertifikatsbeantragung, -ausstellung und -sperrung möglich.
- Die veröffentlichten Zertifikate werden durch das HSM gesichert.
- Das HSM stellt sicher, dass das Berlin CA-Schlüsselpaar 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 CA stellt einen Sperrdienst zur Verfügung.

3.3 Verpflichtungen von weiteren untergeordneten Zertifizierungsstellen

- Jede behördeneigene CA vereinbart mit der Berlin PCA ihren eindeutigen Namen, der innerhalb der gesamten PKI gilt und stellt damit sicher, dass die vereinbarten Namensbestandteile in ihrem Zuständigkeitsbereich verwendet werden.
- Mit Vertragsabschluss verpflichtet sich die CA zur Einhaltung und Erfüllung der in den Sicherheitsrichtlinien der Berlin PCA gestellten Anforderungen.

- Jede Behörden CA verpflichtet sich zur Einhaltung des durch die Wurzelzertifizierungsstelle (Berlin PCA) festgelegten Namensraumes.
- Sobald die CA erkennt, dass sie die in den Sicherheitsrichtlinien der Berlin PCA gestellten Anforderungen nicht mehr erfüllt, ist sie verpflichtet, dies der Berlin PCA unverzüglich schriftlich mitzuteilen.
- Erkennt die Berlin PCA, dass die in ihren Sicherheitsrichtlinien gestellten Anforderungen von der CA nicht mehr erfüllt werden, wird sie die CA hierüber schriftlich informieren und zur Stellungnahme auffordern. Die Stellungnahme der CA muss innerhalb von zwei Wochen nach Zugang der Aufforderung schriftlich erfolgen.
- Jede CA ist auf Verlangen der Berlin PCA verpflichtet, Aufzeichnungen und Unterlagen zur Prüfung vorzulegen. Liegen die geforderten Unterlagen nicht innerhalb von zwei Wochen vor, ist die PCA berechtigt, das CA-Zertifikat mit sofortiger Wirkung zu sperren.
- Jede CA erklärt ihr Einverständnis mit der Veröffentlichung ihres Zertifikates durch die Berlin PCA.
- Jede CA stellt sicher, dass das CA-Schlüsselpaar in einer gesicherten Umgebung kryptografisch geeignet erzeugt wird. Darüber hinaus stellt jede CA sicher, dass der geheime Schlüssel nur zur Bestätigung von Zertifikaten verwendet wird.
- Jede CA stellt einen Sperrdienst zur Verfügung.

3.4 Verpflichtungen der Registrierungsstelle (RA)

- Zu den Aufgaben und Pflichten der Mitarbeiter der RA gehört, dass Zertifikatnehmer durch persönliches Erscheinen in der RA identifiziert und anhand eines gültigen amtlichen Ausweises oder bei Verwaltungsbeschäftigten durch einen gültigen Dienstausweis authentisiert werden. Optional kann für die festangestellten Mitarbeiter der Berliner Verwaltung 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 Gruppenzertifikaten wird eine natürliche Person als Schlüsselverantwortlicher durch die RA identifiziert und authentisiert. Der Schlüsselverantwortliche muss seine Berechtigung zur Beantragung der Gruppenzertifikate gegenüber der RA belegen und seine Bereitschaft erklären, sich an die Verpflichtung der lokalen Registrierungsstelle zu halten.
- Bei Maschinenzertifikaten (für Server und Netzwerkkomponenten) wird die Identität des entsprechenden Administrators der Maschine 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.

3.5 Verpflichtungen von lokalen Registrierungsstellen

Die RA des ITDZ kann lokale Registrierungsoperatoren (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 der Berliner Verwaltung 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 PCA und der zuständigen CA.
- Die LRA Mitarbeiter haben dieselben Aufgaben und Pflichten wie die Mitarbeiter der RA.

3.6 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 ADs zieht die Deaktivierung des Active Directory Kontos automatisch die Sperrung der entsprechenden Zertifikate nach sich.

3.7 Vertraulichkeit

Alle Konzepte und Unterlagen der Berlin PCA sowie der CAs, RAs und LRAs unterliegen der Vertraulichkeit. Die gültige Policy kann nach der Freigabe der Berlin PCA veröffentlicht werden.

3.8 Gültigkeitsdauer

Das Zertifikat der Berlin PCA hat eine Gültigkeitsdauer von 10 Jahren. Eine regelmäßige Erneuerung des Zertifikats der Berlin PCA ist vorgesehen, dazu wird spätestens nach Ablauf von

sechs Jahren ein weiteres gültiges Berlin PCA Zertifikat erstellt. Dementsprechend gibt es mehrere gültige Berlin PCA Zertifikate, die sich im Gültigkeitsdatum unterscheiden.

Die Gültigkeitsdauer von Zertifikaten für CAs beträgt maximal sechs Jahre. Ein regelmäßiger Schlüsselwechsel des Zertifikats der CAs ist spätestens nach drei Jahren vorgesehen. Dementsprechend gibt es mehrere gültige CA Zertifikate, die sich im Gültigkeitsdatum unterscheiden.

Die Gültigkeitsdauer von Zertifikaten für RA und LRAs beträgt maximal drei Jahre. ITDZ-Zertifikatnehmer unterscheiden sich bei der Gültigkeitsdauer dahingehend, dass Userzertitfikate für maximal ein Jahr und Maschinenzertifikate für maximal drei Jahre ausgestellt werden.

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 identifiziert und anhand eines gültigen amtlichen Ausweises oder bei Verwaltungsbeschäftigten durch einen gültigen Dienstausweis authentisiert. Die festangestellten Mitarbeiter der Berliner Verwaltung können über die gültigen Mitarbeiterverzeichnisse der Verwaltung oder durch Anfrage bei den Personalstellen überprüft werden.
Sofern ein LRA-Operator eingesetzt wurde, erfolgt die Identifizierung und Authentisierung der Zertifikatnehmer auf die gleiche Weise über ihn.

4.1.2 Identifizierung und Authentisierung einer juristischen Person

Juristische Personen, die ein Zertifikat beantragen, werden durch persönliches Erscheinen mindestens einer sie vertretenden Person identifiziert. Diese Person muss sich, wie unter 4.1.1 dargestellt, authentisieren. Zusätzlich ist durch sie nachzuweisen:

- ihre Vertretungsvollmacht zur Beantragung eines Zertifikats für die juristische Person,
- den Nachweis der Existenz der juristischen Person durch Handelsregisterauszug oder vergleichbare Dokumente und
- die Erklärung, dass gegenwärtig kein Insolvenzverfahren gegen die juristische Person eröffnet worden ist oder dessen Eröffnung beantragt worden ist.

4.1.3 Identifizierung und Authentisierung bei Gruppenzertifikaten

Für jedes Gruppenzertifikat ist eine natürliche Person als Schlüsselverantwortlicher zu benennen. Diese Person muss gemäß Abschnitt 4.1 ein entsprechendes Zertifikat beantragen und die in Abschnitt 4.1.1 geforderten Identitäts- und Authentisierungsnachweise erbringen.
Der Gruppenverantwortliche teilt der RA die Anzahl der Gruppenmitglieder mit und verwaltet die Liste der Gruppenmitglieder, die der RA auf Verlangen gezeigt wird.

4.1.4 Identifizierung und Authentisierung bei Maschinenzertifikaten

Maschinenzertifikate 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.

4.1.5 Namensregeln

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

4.1.6 Zertifizierungsinstanzen

- Der Namensraum der Berlin PCA2 lautet:
  CN=Berlin PCA2, O=Landesverwaltung Berlin, C=DE
- Der Namensraum der Berlin CA04 2016 die maschinenbezogene Zertifikate generiert, lautet:
  CN=Berlin CA04 201, OU=IT, O=Landesverwaltung Berlin, C=DE
- Der Namensraum der Berlin CA05 2016, die userbezogene Zertifikate generiert, lautet:
  CN=Berlin CA05 2016 , OU=IT, O=Landesverwaltung Berlin, C=DE

Die Alt-Systeme Berlin PCA, Berlin CA01 2011 und Berlin CA02 2011 stellen keine Zertifikate mehr aus, werden aber noch betrieben, um Sperrinformationen für noch gültige Alt-Zertifikate bereitzustellen.

- Der Namensraum der Berlin PCA lautet:
  CN=Berlin PCA, O=Landesverwaltung Berlin, C=DE
- Der Namensraum der Berlin CA01 2011 für maschinenbezogene Zertifikate, lautet:
  CN=Berlin CA01 2011, OU=IT, O=Landesverwaltung Berlin, C=DE

- Der Namensraum der Berlin CA02 2011, für userbezogene Zertifikate, lautet:
  CN=Berlin CA02 2011 , OU=IT, O=Landesverwaltung Berlin, C=DE
- Der Namensraum der Berlin CA03, lautet:
  CN=Berlin CA03 , OU=IT, O=Landesverwaltung Berlin, C=DE

- Der Namensraum einer Behörden CA sieht folgendermaßen aus:
  CN=<Behörde>_CAXX , OU=<Behördenkürzel>, O=Landesverwaltung Berlin, C=DE
  XX steht dabei als fortlaufende Nummerierung über alle CAs.

4.1.7 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 CA02 2011 ist für die Einheitlichkeit und Eindeutigkeit der vergebenen Namen (DNs) für User-zertifikate verantwortlich.

Die DNs aller Zertifikatnehmer, deren Zertifikate von der Berlin CA05 2016 generiert wurden, enthalten die folgenden festen Attribute:

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

und die folgenden spezifischen Attribute:

Attribut	*Kürzel*	*Wert*
Organizational Unit	OU	<Verfahren> oder <Bereich>
Common Name	CN	<Nachname Vorname> oder <Login-Name>
E-Mail	E	<E-Mail-Adresse>

Das OU-Attribut kann mehrfach vorkommen.

Über den SubjectAlternateName (SAN) können auch weitere Namen wie z.B. die E-Mail-Adresse oder der UserPrincipalName (UPN) angegeben werden.

Ein Namenszertifikat hat beispielsweise folgenden DN:
CN=Mustermann Paul, OU=ITDZ Berlin, O=Landesverwaltung Berlin, C=DE

4.1.8 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 CA01 2011 ist für die Einheitlichkeit und Eindeutigkeit der vergebenen Namen (DNs) verantwortlich.

Die DNs aller Maschinen, deren Zertifikate von der Berlin CA04 2016 generiert wurden, enthalten ebenfalls die folgenden festen Attribute:

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

und die folgenden spezifischen Attribute:

Attribut	*Kürzel*	*Wert*
Organizational Unit	OU	<Verfahren> oder <Bereich>
Common Name	CN	<Maschinenname>
E-Mail	E	<E-Mail-Adresse>

Das OU-Attribut kann mehrfach vorkommen.

Über den SubjectAlternateName (SAN) können auch weitere Namen wie z.B. die E-Mail-Adresse, weitere DNS-Namen oder IP-Adressen angegeben werden.

Ein Maschinen-Zertifikat hat beispielsweise folgenden DN:
CN=<Webserver FQDN>, OU=ITDZ Berlin, O=Landesverwaltung Berlin, C=DE

4.1.9 Pseudonymzertifikate

Auf Wunsch des Zertifikatnehmers werden Pseudonymzertifikate von der Berlin CA02 2011 ausgestellt, bei denen anstelle des realen Namens ein Pseudonym verwendet wird. Voraussetzung ist, dass das Pseudonymzertifikat durch den Zusatz ":PN" am Ende des CN gekennzeichnet wird.
Pseudonymzertifikate werden grundsätzlich nur für natürliche Personen und nicht für juristische Personen oder für Gruppen vergeben.
Ein Pseudonymzertifikat hat beispielsweise folgenden DN:
CN=Nebel (PN), OU=<Stellenzeichen>, OU=ITDZ Berlin, O=Landesverwaltung Berlin, C=DE

Die Abkürzung PN im CN steht für Pseudonym.

4.1.10 Gruppenzertifikate

Auf Wunsch eines Zertifikatnehmers können Gruppenzertifikate für Personen einer Behörde ausgestellt werden.
Ein Gruppenzertifikat hat beispielsweise folgenden DN:
CN = Gruppe, OU=<Behörde>, O=Landesverwaltung Berlin, C=DE

4.2 Regelmäßiges Wiederausstellen

Folgezertifikate müssen entweder wie bei der erstmaligen Registrierung auf der RA oder als elektronisch signierter Verlängerungsantrag per E-Mail 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 Sperrung

Nach einer Sperrung des Zertifikats ist wie bei einer erstmaligen Registrierung vor-zugehen, 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 Berlin PCA und die CAs nehmen die Sperranträge der berechtigten Zertifikatnehmer und Zertifizierungsinstanzen per

- signierter E-Mail,
- unterschriebener Fax-Mitteilung oder
- Briefpost

entgegen.

5 Geheimhaltungsgrad bei Verschlüsselung

Es gelten die Regelungen zum Geheimhaltungsgrad bei Verschlüsselung der jeweiligen Dienststellen.

6 Ablauforganisation

6.1 Zertifikatsantrag

Arbeitsabläufe zur Beantragung und Ausstellung von Zertifikaten innerhalb der ITDZ-PKI 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 beantragt.
Die RA übermittelt den geprüften Zertifikatsantrag an die jeweilige CA zur Erzeugung der Zertifikate. Sofern ein Certificate Request bei der RA eingeht, wird dieser nach der Identitätsprüfung des Antragstellers zusammen mit dem Antrag an die entsprechende CA zur Bearbeitung signiert 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.

6.2 Ausstellung des Zertifikats

Die jeweiligen CAs erzeugen dann 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 tragen die CAs die Verantwortung.
Es gibt die folgenden zwei Möglichkeiten der Beantragung von Zertifikaten bei Zertifizierungsstellen:

- Die erste Möglichkeit besteht darin, dass die Zertifizierungsstellen 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 Zertifikatnehmer erhält die Dateien und das dazugehörige PIN-Schreiben auf getrennten Übertragungswegen.

- Die zweite Möglichkeit besteht darin, dass der Antragssteller sein Schlüsselpaar selbst generiert und der Zertifizierungsstelle einen signierten Zertifikatsantrag (Certificate-Request) übergibt. Die Zertifizierungsstelle prüft den Zertifikatsantrag 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 per E-Mail oder Post an den Antragsteller. In der Regel werden IPSec-Zertifikate für Firewalls und SSL-Zertifikate für Server aus einem Certificate Request erstellt.

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

6.3 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.

6.4 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. Hier erfolgt die Erneuerung der Zertifikate automatisch, wenn die Maschinen die gleichen Namen und Funktionen behalten. (z.B. Domänen-Controller)
Der erstellt Request kann auch bei Folgezertifikaten verwendet werden.

6.5 Sperrung von Zertifikaten

6.5.1 Sperrgründe

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

- Nach dem Wirksamwerden der Kündigung des Vertrages zwischen der Berlin PCA und der Behörden CA wird das CA-Zertifikat gesperrt.
- Der geheime Signaturerstellungsschlüssel der CA ist nicht mehr verfügbar oder kompromittiert.
- Die CA kann die Sperrung ihres Zertifikats jederzeit ohne Angabe von Gründen beantragen und veranlassen.
- Die CA gibt den Betrieb auf.

- 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.

6.5.2 Zeitdauer zwischen Sperrantrag und Sperrung

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

6.5.3 Ausstellung von Sperrlisten

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

6.5.4 Bekanntgabe von Sperrungen

Die aktuelle Sperrliste der Berlin PCA wird durch manuelle Publikation und von den untergeordneten CAs automatisch den Verzeichnisdiensten zur Verfügung gestellt.

6.5.5 Kompromittierung des geheimen Schlüssels

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

6.5.6 Suspendierung

Die Suspendierung von Zertifikaten ist in der gesamten ITDZ-PKI nicht vorgesehen.

6.6 Beweissicherung und Protokollierung

Im Betriebskonzept [1] wird festgelegt, welche Daten und Ergebnisse der Zertifikatshierarchie in welchen Abständen von wem aufgezeichnet sowie über welchen Zeitraum Datensicherungen und Protokolldaten archiviert werden. Der Zugriff auf solche Archive wird in einem Rollenkonzept, welches Bestandteil des Betriebskonzeptes ist, geregelt und enthält Angaben darüber, welche Rechte, Pflichten, Aufgaben und Anforderungen jede im Rollenkonzept festgelegte Funktion hat.

6.7 Schlüsselwechselmanagement

Beim Wechsel des Schlüssels der Berlin PCA wird ein neues PCA-Zertifikat ausgestellt. Gleiches gilt bei CA-Zertifikaten, die von der Berlin PCA ausgestellt werden. Es wird mehrere gültige PCA- und CA-Zertifikate geben (vgl. Abschnitt 3.8).

6.8 Kompromittierung und Wiederherstellung

Die Berlin PCA und die Berlin CAs 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 und unterliegt der ständigen Pflege.

6.9 Einstellen des Betriebs

Für den Fall, dass die Berlin PCA oder eine CA beabsichtigt den Betrieb als Zertifizierungsdiensteanbieter einzustellen, ist dies unter Einhaltung der folgenden Bedingungen rechtzeitig anzukündigen.

- Die Berlin PCA kann den Betrieb mit einer Kündigungsfrist von 12 Monaten zum Ende des Quartals einstellen.
- Jede 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 Berlin PCA und der CA vertraglich geregelt.
- Die Berlin PCA muss den Betrieb dann einstellen, wenn das Zertifikat kompromittiert wurde.

Mit Einstellung des Betriebes einer CA werden alle von ihr ausgestellten und noch gültigen Zertifikate 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 [1] regelt den Umgang mit den Unterlagen und Daten der CAs, RA und LRAs.

7 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen für Zertifizierungsstellen

Alle infrastrukturellen, organisatorischen und personellen Sicherheitsmaßnahmen sind in einem Sicherheitskonzept [2] dargelegt. Die im Folgenden beschriebenen Maßnahmen beziehen sich auf den Betrieb der Berlin PCA und den angeschlossenen CAs in Bezug auf Zutrittsregelungen, Stromversorgung, Klimatechnik, Brandschutz und Speichermedien.

7.1 Infrastrukturelle Maßnahmen

7.1.1 Lage

Die Betriebskomponenten der Berlin PCA und der angeschlossenen CAs befinden sich im High Secure Datacenter des ITDZ. Dort sind die Server der PCA, CAs und der Verzeichnisdienste untergebracht. Das High Secure Datacenter erfüllt alle Sicherheitsanforderungen des behördlichen und des Berliner Datenschutzbeauftragten für den hohen und sehr hohen Schutzbedarf.

7.1.2 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 PCA- und CA 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.

7.1.3 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 Berlin PCA und CAs werden Betriebsbeeinträchtigungen verhindert.

7.1.4 Brandschutz

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

7.1.5 Speichermedien

Im Betriebskonzept [1] wird der Umgang mit den folgenden schützenwerten Daten zur Sicherung, Wiederherstellung, Archivierung und Vernichtung geregelt:

- Schlüssel der PCA
- Schlüssel der CAs
- Backup der Schlüssel
- Protokolldaten

7.2 Organisatorische Maßnahmen

Im Betriebskonzept [1] der Berlin PCA und der angeschlossenen CAs ist ein Rollenkonzept festgelegt, welches die organisatorischen Maßnahmen regelt.

7.3 Personelle Maßnahmen

Im Betriebskonzept [1] gibt es für jede Rolle der Berlin PCA und der angeschlossenen CAs ein Anforderungsprofil.
Folgende Voraussetzungen erfüllen die Mitarbeiter, die hierbei eine Rolle übernehmen:

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

8 Technische Sicherheitsmaßnahmen für Zertifizierungsstellen

Für die technischen Sicherheitsmaßnahmen wird ein Sicherheitskonzept [2] angefertigt und umgesetzt, das den Anforderungen des IT-Grundschutzhandbuchs [3] für den hohen und sehr hohen Schutzbedarf entspricht.

8.1 Schlüsselgenerierung und –installation

8.1.1 Schlüsselgenerierung

Alle Schlüsselpaare für die Berlin Zertifizierungsstellen 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.

8.1.2 Übergabe der öffentlichen Schlüssel und Zertifikate

Als Ergebnis des Zertifizierungsantrags (Certificate Request) übergibt die Berlin PCA den berechtigten Mitarbeitern der zuständigen CA das Zertifikat. Zuvor wurde der öffentliche Schlüssel zusammen mit anderen Zertifizierungsdaten (wie z.B. DN, Gültigkeit etc.) von der Berlin PCA signiert.
Die Übergabe der öffentlichen und geheimen Schlüssel der Zertifikatnehmer erfolgt als Software-Zertifikat in Form einer PKCS#12 Datei mit einem zusätzlichen PIN-Schreiben zum Entsperren des geheimen Schlüssels. Die Datei und das PIN-Schreiben werden auf getrennten Übertragungswegen übermittelt (vgl. Abschnitt 6.2). Analoge Abläufe der Übergabe bestehen bei Zertifizierungsinstanzen, deren Schlüsselpaare durch eine CA im ITDZ generiert wurden.

8.1.3 Akzeptanz von Zertifikaten

Die zuständige CA im ITDZ 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 Berlin PCA. Für die Zertifikatnehmer einer CA im ITDZ gelten analoge Regelungen (vgl. Abschnitt 6.3).

8.1.4 Kryptoalgorithmen, Schlüssellänge, Parametergenerierung

Die Berlin PCA verwendet als kryptografische Algorithmen SHA2 und eine Schlüssellänge von 4096 Bit für das PCA-Zertifikat. Die zuständigen CAs im ITDZ verwenden als kryptografische

Algorithmen SHA2 und eine Schlüssellänge von 2048 Bit für das jeweilige CA Zertifikat. Die festgelegte Schlüssellänge für Zertifikate von Zertifikatnehmern und Registrierungsstellen beträgt ebenfalls mindestens 2048 Bit.

8.1.5 Schlüsselnutzung

Der geheime Schlüssel der Berlin PCA wird ausschließlich zum Signieren der öffentlichen Schlüssel von Zertifizierungsstellen und der Sperrliste verwendet.
Der geheime Schlüssel jeder CA wird ausschließlich zum Signieren der öffentlichen Schlüssel von Zertifikatnehmern sowie untergeordneten Zertifizierungsinstanzen und der Sperrliste verwendet.

8.2 Schutz des geheimen Schlüssels

8.2.1 Schlüsselteilung

Eine Schlüsselteilung ist von den Berlin PCA und den angeschlossenen CAs im ITDZ nicht vorgesehen.

8.2.2 Key Escrow

Eine Schlüsselhinterlegung im klassischen Sinne eines TrustCenters ist bei der Berlin PCA und den angeschlossenen CAs im ITDZ nicht vorgesehen.

8.2.3 Wiederherstellung des privaten Schlüssels

Der geheime Schlüssel der Berlin PCA und der angeschlossenen CAs sowie der von ihr zertifizierten Instanzen, die nicht selbst einen Certificate Request erzeugt haben, ist über ein gesichertes HSM Backupverfahren wiederherstellbar. Das Backupverfahren ist im Betriebskonzept [1] beschrieben.
Die Wiederherstellung der von den CAs erstellten geheimen Schlüssel der Zertifikatnehmer ist nur in begründeten Ausnahmefällen und unter Einhaltung der im Betriebskonzept [1] geregelten Prozeduren möglich. Begründete Anforderungen sind z.B.:

- Ein Zertifikatnehmer hat sein Zertifikat verloren und benötigt es, 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. In diesem Fall Bedarf die Wiederherstellung der Genehmigung des Vorgesetzten, der Personalvertretung, des Datenschutzes und des Sicherheitsbeauftragten.

8.2.4 Archivierung des privaten Schlüssels

Die geheimen Schlüssel der Berlin PCA und der angeschlossenen CAs werden ausschließlich in der Netzwerk HSM gespeichert. Sie können aus dieser nur im 4-Augen-Prinzip exportiert werden; ein Export der privaten Schlüssel wird jedoch nicht durchgeführt.
Eine verschlüsselte Archivierung von privaten Schlüsseln für Zertifikate mit dem Zweck „Datenverschlüsselung“ der Zertifikatnehmer wird vorgenommen, wenn das Schlüsselmaterial nicht durch den Zertifikatnehmer selbst erzeugt wurde. Sofern Zertifikatnehmer das gesamt Schüsselmaterial durch die CA erhalten, können sie die Dateien für den privaten Informationsaustausch (*.pfx) selbst in geeigneter Weise archivieren.

8.2.5 Schlüsselinstallation und Aktivierung

Der geheime Schlüssel der Berlin PCA und der angeschlossenen CAs wurde im ITDZ von berechtigten Mitarbeitern der Berlin PCA bzw. CAs generiert. Die Generierung von Zertifikaten für Zertifikatnehmer und Zertifizierungsinstanzen erfolgt nach vorheriger Überprüfung der Zertifikatsanträge automatisiert auf den CA-Servern.
Zertifikatnehmer, denen ein asymmetrisches Schlüsselpaar von einer CA generiert wurde, benötigen für die Installation ihres Zertifikats die dazugehörige PIN, die nur ihnen bekannt ist.

8.2.6 Schlüsselvernichtung

Nach Ablauf der Gültigkeit oder nach Sperrung der PCA- oder eines CA-Zertifikats wird der geheime Schlüssel zuverlässig vernichtet.

8.3 Weitere Aspekte des Schlüsselmanagements

8.3.1 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 2.4).

8.3.2 Nutzungsdauer für öffentliche und private Schlüssel

Die Nutzungsdauer des PCA- oder eines CA Schlüsselpaares stimmt grundsätzlich mit der Nutzungsdauer des dazugehörigen Zertifikats überein. Die maximale Gültigkeit eines CA Zertifikats beträgt sechs Jahre. Ein neues CA Zertifikat wird bei der Berlin PCA in Form eines Certificate Request beantragt.

Auch bei Zertifikaten für Zertifikatnehmer und Zertifizierungsinstanzen einer 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 drei Jahren (vgl. Abschnitt 3.8). Über die RA kann die Verlängerung des Zertifikats beantragt werden, damit ein neues Schlüsselpaar von einer CA nach vorheriger Identitätsprüfung generiert bzw. der öffentliche Schlüssel des Antragstellers durch die Signatur der Zertifizierungsstelle bestätigt wird. Für Maschinen im zentralen AD werden automatisch neue Schlüssel innerhalb des Überlappungszeitraumes ausgestellt.

8.3.3 Aktivierungsdaten

Die PIN zur Aktivierung der privaten Schlüssel der Endanwender wird von der Registrierungsstelle vom System automatisiert vergeben und in einen PIN/PUK-Brief gedruckt. Den PIN/PUK-Brief bekommt der Zertifikatsinhaber auf unterschiedlichen Wegen bereit gestellt oder in der Registrierungsstelle persönlich übergeben. Private Signaturschlüssel einer Zertifizierungsstelle werden im HSM nach Authentisierung der Schlüsselverantwortlichen mittels Chipkarten des HSM unter Einhaltung des Vier-Augen-Prinzips aktiviert.

9 Profile für Zertifikate und Sperrlisten

Die Festlegung der Profile der Berlin PCA- oder eines CA-Zertifikats und dessen beglaubigte Zertifikate entsprechen ebenso wie die Verwendung von Zertifikatserweiterungen der MailTrusT-Spezifikation der Version 2 (MTTv2) [4]. Ebenfalls ist in der MTTv2-Spezifikation das Profil der Sperrlisten (CRL) einschließlich der Sperrlistenerweiterungen geregelt. Das aktuelle CRL-Format ist CRLv2.

10 Änderung und Anerkennung dieser Policy

10.1 Policy Object Identifier

Die ITDZ Enterprise OID lautet: 1.3.6.1.4.1.10769
Private Enterprise Code

Der Policy Object Identifier für die ITDZ PKI lautet: 1.3.6.1.4.1.10769.50.2.

10.2 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.

10.2.1 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 etc.) erfordern. Insbesondere können Korrekturen zur Typographie und Layout ohne weitere Bekanntmachung erfolgen.

10.2.2 Änderungen, die eine Bekanntmachung erfordern

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

10.2.3 Verfahren zur Publizierung und Bekanntgabe

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

10.2.4 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.

10.3 Anerkennung

Die Berlin PCA und die angeschlossenen CAs verpflichten sich, die vorliegende Policy einzuhalten und die Sicherheitsrichtlinien der Wurzelzertifizierungsinstanzen des ITDZ anzuerkennen. Auch die Zertifikatnehmer werden auf ihrer Rechte und Pflichten als Bestandteil das ITDZ-PKI bei der Zertifikatsbeantragung hingewiesen und stimmen der Policy zu.

11 Literaturverzeichnis

[1] ITDZ, Betriebskonzept PKI, Version 1.0

[2] ITDZ, Sicherheitskonzept PKI, Version 1.0

[3] BSI, IT-Grundschutzhandbuch (in der aktuellen Version), Bundesanzeigerverlag

[4] Teletrust Verein, MailTrusT Version 2, Gesamtkonzeption, Aufbau und Komponenten einer PKI, Stand: 16. März 1999

[5] ITDZ, Einführungskonzept PKI, (ITDZ-PKI-Konzept-V3.pdf)

[6] ITDZ, Zertifikatsvorlagen, (itdz-profil-v1.xls)