Zertifikatsrichtlinie des nicht-hoheitlichen Document Verifiers der D-Trust GmbH (BerCA)

Version 1.2

Erscheinungsdatum	21.10.2010
Datum des Inkrafttretens	01.11.2010

Vermerk zum Copyright

D-Trust GmbH
Kommandantenstraße 15
10969 Berlin, Germany
E-Mail: info@d-trust.net

Dokumentenhistorie

Version	Datum	Beschreibung
1.0	08.09.2010	Initialversion
1.1	15.10.2010	Änderungen nach Kommentierung durch Herrn Beyer (BSI)
1.2	21.10.2010	Korrektur nach zweitem Review

Inhaltsverzeichnis

1. Einleitung

1.1 Überblick

Dieses Dokument beschreibt die Zertifikatsrichtlinie (engl. *Certificate Policy*, kurz CP) der nicht-hoheitlichen BerCA PKI der D-TRUST GmbH, einem Unternehmen der Bundesdruckerei Gruppe, im Rahmen des angezeigten Betriebes entsprechend der [TR-03128].

Die nicht-hoheitliche BerCA PKI ist Teilmenge der in [CP-eID] spezifizierten CVCA-eID PKI. Sie unterwerfen sich den Anforderungen für den nicht-hoheitlichen Betrieb der CVCA-eID PKI.

1.1.1 Zertifizierungsinstanz und Betreibermodel

Zertifizierungsinstanz und technischer Betreiber der in diesem Dokument beschriebenen Zertifizierungsdienste der BerCA PKI ist die

D-Trust GmbH
Kommandantenstraße 15
10969 Berlin

1.1.2 Zielsetzung der Sicherheitsleitlinie

Diese CP stellt Vorgaben und Anforderungen an die BerCA PKI. Sie regelt somit den Betrieb der BerCA, den Zertifizierungsprozess während der gesamten Lebensdauer der von ihr ausgestellten Zertifikate sowie das Zusammenwirken, Rechte und Pflichten der PKI-Teilnehmer[1].

Die gesamte CP ist rechtsverbindlich, soweit dies im Rahmen der deutschen Gesetzgebung zulässig ist. Sie enthält Aussagen über Pflichten, Gewährleistung und Haftung für die PKI-Teilnehmer. Soweit nicht ausdrücklich genannt, erfolgen auf Basis dieser CP keine Zusicherungen oder Garantien im Rechtssinne.

Die Kenntnis der in dieser CP beschriebenen Zertifizierungsverfahren und -regeln sowie der rechtlichen Rahmenbedingungen erlaubt es Zertifikatsnutzern, Vertrauen in die Komponenten und PKI-Teilnehmer aufzubauen und Entscheidungen zu treffen, inwieweit das durch die BerCA PKI gewährte Vertrauens- und Sicherheitsniveau für Anwendungen geeignet ist.

1.1.3 Struktur des Dokumentes

Die Struktur dieses Dokumentes ist eng an den Internet-Standard RFC 3647 *„Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework“* angelehnt, um eine einfache Lesbarkeit und Vergleichbarkeit mit anderen CPs zu erreichen.

[1] Im Interesse einer leichteren Lesbarkeit wird in diesem Dokument auf die weibliche Form der PKI-Teilnehmer und sonstigen genannten Personengruppen verzichtet. Es wird gebeten, die weibliche Form jeweils als eingeschlossen anzusehen.

1.2 Name und Kennzeichnung des Dokuments

Dokumentname: Zertifikatsrichtlinie des nicht-hoheitlichen Document Verifiers der D-Trust GmbH (BerCA)

Kennzeichnung (OID): 1.2.276.0.80.7.500.30

Dieser CP-OID liegt im registrierten OID-Zweig der Bundesdruckerei GmbH.

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstelle (BerCA)

Die Country Verifying Certification Authority – electronic Identity (CVCA-eID) ist der nationale Vertrauensanker (Root) der CVCA-eID PKI. Sie stellt DV-Berechtigungszertifikate für die Document Verifying Certification Authority (DVCA) aus, die im nicht-hoheitlichen Bereich nach [CP-eID] als Berechtigungs-CAs (BerCA) bezeichnet wird. Die BerCA ist eine organisatorische Einheit, welche von der CVCA-eID zur Ausgabe von Terminalberechtigungszertifikaten[2] an Diensteanbieter (gemäß §2 Abs. 3 [PAuswG]) autorisiert ist. Zwischen Diensteanbieter und BerCA wird ein bilateraler Vertrag geschlossen. Sowohl die Zugriffsrechte als auch die Gültigkeitsdauer der ausgestellten Terminalberechtigungszertifikate werden von der BerCA entsprechend der Vorgabe der Vergabestelle für Berechtigungszertifikate (VfB) und den Anforderungen der [CP-eID] definiert.

1.3.2 Registrierungsstelle und Teilnehmerservice

Gemäß [TR-03128]: „Für nicht-hoheitliche Aufgabenstellungen des elektronischen Identitätsnachweises wird der Registrierungsdienst in der „Vergabestelle für Berechtigungszertifikate (VfB)“ angesiedelt. Diese ist einer Institution der Bundesverwaltung zugeordnet und wird vom Bundesverwaltungsamt wahrgenommen. Die Aufgabenstellung entspricht der eines hoheitlichen Betreibers.“

Gemäß [CP-eID] müssen die Teilnehmer eindeutig und sicher identifiziert werden. Der Teilnehmerservice der BerCA gewährleistet die sichere Teilnehmeridentifikation im Rahmen des technisch etablierten Prozesses, beschrieben in Abschnitt 3.2.2.

1.3.3 Zertifikatsnehmer (ZNE)

Zulässige Zertifikatsnehmer sind Diensteanbieter nach §2 Abs. 3 [PAuswG]. Diensteanbieter benötigen zur Erbringung ihrer Dienste Zugriff auf die eID-Funktion des neuen elektronischen Personalausweises. Zu diesem Zweck beantragen sie ein Terminalberechtigungszertifikat, welches ihnen den Zugriff ermöglicht. Terminalberechtigungszertifikate werden im Folgenden gemäß ihrer Funktion als Terminalberechtigungszertifikate bezeichnet. Ein Diensteanbieter kann einen eID-

[2] In diesem Dokument wird die BerCA PKI um die Berechtigungszertifikate (DV-Berechtigungszertifikate und Terminalberechtigungszertifikate) beschrieben. Wird von Zertifikaten oder Zertifikats-Requests gesprochen sind grundsätzlich Berechtigungszertifikate gemeint. Zur Absicherung der Kommunikationsbeziehungen werden Kommunikationszertifikate benötigt. Wenn diese gemeint sind, wird dies explizit gekennzeichnet

Service-Provider beauftragen, den Zugriff auf die Authentisierungsfunktion technisch umzusetzen.

Die BerCA ist ihrerseits Zertifikatsnehmer der CVCA-eID.

1.3.4 Zertifikatsnutzer (ZNU)

Es gilt 1.3.4 der [CP-eID].

1.3.5 Andere PKI-Teilnehmer

Es gilt 1.3.5 der [CP-eID].

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

Es gilt 1.4.1 – nicht-hoheitlicher Bereich – der [CP-eID].

1.4.2 Verbotene Verwendungen von Zertifikaten

Es gilt 1.4.2 der [CP-eID].

1.5 Pflege der CP

1.5.1 Zuständigkeit für das Dokument

Diese CP wird für und im Auftrag der Bundesdruckerei GmbH durch die D-Trust GmbH gepflegt.

1.5.2 Ansprechpartner/Kontaktperson/Sekretariat

Eine Kontaktaufnahme kann über folgende Adressen erfolgen:

D-Trust GmbH
Kommandantenstr. 15
10969 Berlin, Germany

1.5.3 Eingliederung dieser CP

Diese CP unterwirft sich der [CP-eID] und bestätigt die Erfüllung der erforderlichen Anforderungen. Das Bundesamt für Sicherheit in der Informationstechnik prüft und bestätigt dieses Dokument vor Inkrafttreten.

1.6 Begriffe und Abkürzungen

1.6.1 Deutsche Begriffe und Namen

CVCA-eID PKI	PKI nach [CP-eID].
BerCA PKI	Im Auftrag der Bundesdruckerei GmbH von der D-Trust technisch und organisatorisch betriebene PKI unterhalb der CVCA-eID PKI.
DV-Berechtigungszertifikat	Zertifikat der BerCA gemäß Abschnitt 1.3.1
Kommunikationszertifikate	X.509-Zertifikate zur Absicherung der Kommunikationsbeziehungen
Registrierungsstelle	Einrichtung der BerCA PKI gemäß Abschnitt 1.3.2.
Statusabfragedienst	PKI-Dienstleistung zur Online-Abfrage über den Status eines Zertifikats.
Terminalberechtigungs-zertifikat	Berechtigungszertifikate innerhalb der BerCA PKI gemäß §2 Abs.4 [PAuswG]
Trustcenter	Der Sicherheitsbereich in den Räumen der D-Trust GmbH.
Verzeichnisdienst	PKI-Dienstleistung zum Online-Abrufen von Zertifikaten [TR-03128]; internes DV PKD.
Zertifikatsnehmer	erhalten Zertifikate, siehe Abschnitt 1.3.3.
Zertifikatsnutzer	Relying Party, natürliche oder juristische Personen, die Zertifikate nutzen, siehe Abschnitt 1.3.4.
Zertifikatsrichtlinie	Certificate Policy - (CP), siehe Abschnitt 1.1.

1.6.2 Englische Begriffe

Certificate Holder Reference	Identifikationsmerkmal des Zertifikatsinhabers
Certificate Policy (CP)	Zertifikatsrichtlinie
Certification Authority (CA)	Instanz der PKI, die Zertifikate an weitere PKI Teilnehmer ausstellt.
Country Code	Länderkennzeichen
Holder Mnemonic	Inhaberkürzel
Relying Party	Zertifikatsnutzer
Registration Authority (RA)	Registrierungsstelle

1.6.3 Abkürzungen

BerCA	Berechtigungs-CA
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVA	Bundesverwaltungsamt
CA	Certification Authority
CHR	Certificate Holder Reference
CP	Certificate Policy
DV	Document Verifier
HSM	Hardware Security Module
KEK	Key Encryption Key
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKD	Public Key Directory
PKI	Public Key Infrastructure
RA	Registration Authority
URL	Uniform Resource Locator
VfB	Vergabestelle für Berechtigungszertifikate

1.6.4 Referenzen

[CP-eID]	Bundesamt für Sicherheit in der Informationstechnik, Elektronischer Identitätsnachweis mit dem elektronischen Personalausweis, in der aktuellen Version
[PAuswG]	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG)
[RFC 3647]	Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, November 2003
[SiKo-BerCA]	D-Trust GmbH, Sicherheitskonzept des signaturgesetzkonformen Zertifizierungsdiensteanbieters D-Trust GmbH – Teilmodul Betrieb der Berechtigungs-CA, in der aktuellen Version

[SiKo-DTR]	D-Trust GmbH, Sicherheitskonzept des signaturgesetzkonformen Zertifizierungsdiensteanbieters D-Trust GmbH, in der aktuellen Version
[TR-02102]	Bundesamt für Sicherheit in der Informationstechnik, BSI TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, in der aktuellen Version
[TR-03110]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), in der aktuellen Version
[TR-03116-2]	Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03116-2, eCard-Projekte der Bundesregierung Teil 2 – Hoheitliche Ausweisdokumente, in der aktuellen Version
[TR-03128]	Bundesamt für Sicherheit in der Informationstechnik, EAC-PKI'n für den elektronischen Personalausweis, Rahmenkonzept für den Aufbau und den Betrieb von Document Verifiern, in der aktuellen Version
[TR-03129]	Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03129, PKIs for Machine Readable Travel Documents Protocols for the Management of Certificates and CRLs, in der aktuellen Version

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Die BerCA betreibt einen Verzeichnisdienst mit allen aktuellen Einträgen zu den von ihr ausgestellten Terminalberechtigungszertifikaten gemäß [TR-03128]. Die Daten werden entsprechend der Aufbewahrungszeiten nach Abschnitt 6.3.1 gespeichert.

Die BerCA stellt keinen Online-Statusdienst der Zertifikate (OCSP) zur Verfügung.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Der Verzeichnisdienst ist nicht öffentlich zugänglich.

Diese CP kann im PDF-Format von den Webseiten der Zertifizierungsstelle heruntergeladen werden.

2.3 Häufigkeit von Veröffentlichungen

Es findet keine Veröffentlichung von Zertifikatsinformationen statt. Die BerCA stellt zu Revisionszwecken sicher, dass es jederzeit möglich ist, den aktuellen Bestand der ausgestellten Terminalberechtigungszertifikate festzustellen. Im Sinne der [CP-eID] werden zu jeder Zeit alle weiteren für die eID-Authentisierung erforderlichen Zertifikate für die Teilnehmer bereitgestellt. Dies erfolgt über die Kommunikationsschnittstelle gemäß [TR-03129].

Geänderte Versionen der DV CP werden ebenfalls veröffentlicht (Abschnitt 2.3).

2.4 Zugriffskontrollen auf Verzeichnisse

Die BerCA betreibt den Verzeichnisdienst in einem zugriffsgeschützten Bereich. Technische (Abschnitt 6) und organisatorische (Abschnitt 5) Maßnahmen stellen sicher, dass die Vertraulichkeit und Integrität der Informationen gewahrt bleibt.

3. Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

Die DV-Berechtigungszertifikate der BerCA entsprechen dem in Abschnitt 3.1.1 – nicht-hoheitlicher Bereich – der [CP-eID] geforderten Format. Das verwendete Betreiberkürzel lautet:

- DVeIDDTR<>

Die Certificate Holder Reference der Terminalberechtigungszertifikate wird von der BerCA entsprechend [TR-03110] vergeben und zugewiesen.

3.1.2 Notwendigkeit für aussagefähige Namen

Terminals werden durch Country Code, Holder Mnemonic und Sequence Number [TR-03110] Anhang A.6.1 eindeutig referenziert.

3.1.3 Anonymität oder Pseudonyme von Zertifikatsnehmern

Anonymität oder Pseudonymität des Zertifikatnehmers ist nicht erlaubt.

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Es werden die Namensformate entsprechend Abschnitt 3.1.1 verwendet. Der Bezeichner im Feld Certificate Holder Reference ist eindeutig.

3.1.5 Eindeutigkeit von Namen

Terminalberechtigungszertifikate sind eindeutig einem Zertifikatsnehmer zugeordnet. Sie werden durch die Certificate Holder Reference, bestehend aus Country Code, Holder Mnemonic und Sequence Number [TR-03110] eindeutig referenziert. Die BerCA vergibt pro Bescheid auf ein Terminalberechtigungszertifikat eine eindeutige Holder Mnemonic. Die sequenziell ausgestellten Terminalberechtigungszertifikate erhalten jeweils eine eindeutige Seriennummer.

3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen

Entfällt.

3.2 Initiale Überprüfung der Identität

3.2.1 Nachweis für den Besitz des privaten Schlüssels

Der öffentliche Schlüssel der Terminalberechtigungszertifikate wird der BerCA bei der Beantragung innerhalb eines Zertifikats-Request nach [TR-03110] Anhang C.2 übermittelt. Im Rahmen der Antragsprüfung wird durch Verifikation der inneren Signatur nachvollzogen, ob der Zertifikatsnehmer im Besitz des privaten Schlüssels ist.

3.2.2 Authentifizierung von Organisationen

Im Vorfeld der Beantragung von Terminalberechtigungszertifikaten durchlaufen Diensteanbieter resp. deren beauftragte eID-Service-Provider mit der Zertifizierungsstelle einen vorbereitenden Prozess, der die initiale Teilnehmeridentifizierung umfasst.

Die Vertreter[3] der Diensteanbieter resp. deren beauftragte eID-Service-Provider beantragen zunächst qualifizierte Zertifikate, in denen die betroffene Organisation aufgenommen wird. Die Identität der antragstellenden Person sowie der Organisation wird geprüft. Die Zertifizierungsstelle stellt die Zertifikate gemäß Signaturgesetz aus. Mittel Hilfe der QES werden die benötigten Kommunikationszertifikate (EAC Anwender PKI) beantragt. Die Zertifizierungsstelle stellt die Kommunikations-zertifikate aus und ordnet sie als BerCA dem Diensteanbieter resp. dessen beauftragten eID-Service-Provider zu.

Die initiale Registrierung und die Wiederholungsanträge des Diensteanbieters resp. dessen beauftragter eID-Service-Provider findet abgesichert über die zugeordneten Kommunikationszertifikate statt. Dies stellt die BerCA über automatisiert Prozesse sicher. Andere Nachrichten des Diensteanbieters resp. dessen beauftragten eID-Service-Providers werden mit Hilfe der QES abgesichert.

Der Zertifikatsnehmer stellt sicher, dass die benötigten Kommunikationszertifikate über den gesamten Zeitraum der Geschäftsbeziehung gültig sind bzw. rechtzeitig vor Ablauf der Gültigkeit erneuert werden.

3.2.3 Authentifizierung von natürlichen Personen

Zertifikats-Requests von Einzelpersonen werden nicht angenommen, da ausschließlich Organisationen die Berechtigung zur Teilnahme an der BerCA PKI haben.

3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Es gilt 3.2.4 – nicht-hoheitlicher Bereich – der [CP-eID].

3.2.5 Prüfung der Berechtigung zur Antragstellung

Es gilt 3.2.5 – nicht-hoheitlicher Bereich – der [CP-eID].

3.2.6 Kriterien für die Interoperabilität

Entfällt.

[3] Vertreter sind Organisationsvertreter und Schlüsselbeauftragter.

3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying)

3.3.1 Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Schlüsselerneuerung

Die Identifizierung und Authentifizierung eines routinemäßigen Antrags zur Schlüsselerneuerung erfolgt automatisiert über die in [TR-03129] definierten Kommunikationsprotokolle und beinhaltet die folgenden Verifikationen:

- die erfolgreiche Authentisierung der gesicherten Verbindung findet mittels der hinterlegten Kommunikationszertifikate statt,
- das zur Signatur des Zertifikats-Requests verwendete Schlüsselpaar ist gültig und die Prüfung der inneren und äußeren Signatur des Zertifikats-Request verläuft erfolgreich,
- der Wert des Felds Certificate Holder Reference entspricht dem von der BerCA zugewiesenen Inhalt nach Abschnitt 3.1.1.

3.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen

Bei einem nicht routinemäßigen Wiederholungsantrag erfolgt eine erneute Überprüfung des Antragsstellers gemäß Abschnitt 3.2. Die Gründe für den nicht routinemäßigen Wiederholungsantrag sind vom Zertifikatsnehmer darzulegen und werden dokumentiert. Sollten die registrierten Kommunikationszertifikate abgelaufen sein, müssen wie bei einem initialen Vorgang neue Kommunikationszertifikate registriert werden.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Es gilt 3.4 der [CP-eID].

4. Betriebsanforderungen

4.1 Zertifikatsantrag und Registrierung

4.1.1 Berechtigung zur Antragstellung

Die Berechtigung zur Antragstellung wird von der VfB festgestellt. Die VfB übermittelt der BerCA einen entsprechenden Bescheid.

Die BerCA führt mit dem Diensteanbieter resp. dessen eID-Service-Provider eine Testzertifizierung (Test-Terminalberechtigungszertifikate) auf Basis von Testschlüsseln gemäß Anhang C.2 in [TR-03110] unter Einhaltung der Anforderungen aus [TR-03128] und [CP-eID] durch.

Voraussetzung für den Beginn des Testverfahrens ist das Durchlaufen des Identifizierungsprozesses nach Abschnitt 3.2.2 durch den Diensteanbieter resp. dessen eID-Service-Provider einschließlich Erhalt der QES und Kommunikationszertifikate.

Der Diensteanbieter resp. dessen eID-Service-Provider übermittelt der BerCA eine Akzeptanzbestätigung nach [TR-03128] Nr. 195 nach dem erfolgreichen Abschluss der Testzertifizierung.

Erst nach erfolgreichem Abschluss der Testzertifizierung und nach Eingang der Mitteilung durch die VfB, beginnt die BerCA mit der Bearbeitung des Antragsprozesses für die Terminalberechtigungszertifikate.

4.1.2 Registrierungsprozess und Zuständigkeiten

Die Einhaltung des Registrierungsprozesses entsprechend der Abschnitte 3.2, 3.3 und 4.1.1, die Übermittlung der Terminalberechtigungszertifikate an die Teilnehmer sowie deren Archivierung gemäß Abschnitt 6.3.1 gewährleistet die BerCA.

Der Diensteanbieter verantwortet

- die Generierung von Terminal-Schlüsselpaaren mit Hilfe des sicheren Kryptographiemoduls,
- die Durchführung der in Kapitel 3 aufgeführten Identifizierungs- und Authentifizierungsprozeduren,
- Prüfen von erhaltenen Terminalberechtigungszertifikaten auf Korrektheit.

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Die Identifizierung und Authentifizierung erfolgt gemäß Abschnitt 3.2.2. Die Kommunikation mit den Diensteanbietern resp. deren eID-Service-Providern findet über die zugeordneten Kommunikationszertifikate statt, durch die die Authentisierung gewährleistet ist.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Es gilt 4.2.2 der [CP-eID].

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Es gilt 4.2.3 – nicht-hoheitlicher Bereich – der [CP-eID].

4.3 Ausstellung von Zertifikaten

Nach erfolgreichem Abschluss der Testzertifizierung beginnt die BerCA mit der Bearbeitung des Zertifikats-Requests. Die Bearbeitung des initialen Zertifikats-Requests erfolgt, wenn der Zertifikats-Request über die Schnittstelle der BerCA gemäß [TR-03129] zugestellt wurde und das zuvor registrierte Kommunikationszertifikat den Diensteanbieter resp. dessen eID-Service-Provider innerhalb der gesicherten Verbindung mit der BerCA authentisiert.

Der Inhalt des Zertifikats-Requests wird auf Basis des von der VfB mitgeteilten Bescheides auf Korrektheit geprüft.

Zusätzlich werden die folgenden Verifikationen durchgeführt:

- Prüfung der inneren Signatur des Zertifikats-Requests,
- Prüfung der äußeren Signatur, wenn der Zertifikats-Request mit einer äußeren Signatur versehen ist (optional bei initalen Request nach [TR-03110] Anhang C.2.6),
- der Wert des Felds Certificate Holder Reference entspricht dem vorgegebenen Namensschema.

4.3.1 Benachrichtigung des Zertifikatsnehmers über die Ausstellung des Zertifikats

Das ausgestellte Terminalberechtigunszertifikat wird dem Antragssteller über die in [TR-03129] definierten Kommunikationsprotokolle als Antwort auf die Anfrage zur Verfügung gestellt. Die Verbindung ist dabei über die bei der initialen Registrierung hinterlegten Kommunikationszertifikate authentisiert und verschlüsselt.

4.4 Annahme von Zertifikaten

4.4.1 Verhalten bei der Zertifikatsübergabe

Die erfolgreiche Implementierung des ausgestellten, initialen Terminalberechtigungs-zertifikats für den Wirkbetrieb bestätigt der Diensteanbieter resp. dessen eID-Service-Provider der BerCA schriftlich (Aktzeptanzbestätigung).

Nach Eingang dieser Akzeptanzbestätigung informiert die BerCA die VfB über den Beginn des Wirkbetriebes des Dienstleisters resp. dessen eID-Service-Providers.

4.4.2 Veröffentlichung des Zertifikats

Siehe Abschnitt 2.1.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Es gilt 4.5.1 – nicht-hoheitlicher Bereich – der [CP-eID].

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Es gilt 4.5.2 der [CP-eID].

4.6 Zertifikatserneuerung (certificate renewal)

Eine Zertifikatserneuerung wird nicht angeboten.

4.7 Zertifizierung nach Schlüsselerneuerung

4.7.1 Bedingungen zur Schlüsselerneuerung

Es muss sich um einen routinemäßigen Wiederholungsantrag gemäß Abschnitt 3.3 handeln.

4.7.2 Berechtigung zur Schlüsselerneuerung

Die Berechtigung zur Schlüsselerneuerung ist definiert in Abschnitt 3.3.

4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Für die Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen gilt Abschnitt 3.3.

4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Die Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats erfolgt analog Abschnitt 4.3.1.

4.7.5 Verhalten für die Ausgabe von Zertifikaten nach Schlüsselerneuerungen

Das Verhalten für die Ausgabe von Terminalberechtigungszertifikaten für Schlüsselerneuerungen entspricht dem Verhalten beschrieben in Abschnitt 4.4.

4.7.6 Veröffentlichung von Zertifikaten nach Schlüsselerneuerungen

Die Veröffentlichung von Terminalberechtigungszertifikaten für Schlüssel-erneuerungen entspricht den Regelungen beschrieben in Abschnitt 4.4.1.

4.7.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Die Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats entspricht den Regelungen, beschrieben in Abschnitt 4.4.1.

4.8 Zertifikatsänderung

Zertifikatsänderungen werden nicht angeboten.

4.9 Sperrung und Suspendierung von Zertifikaten

Das Sperren von Terminalberechtigungszertifikaten über eine Sperrliste ist in der CVCA-eID PKI nicht vorgesehen.

Eine Sperrung erfolgt durch die Rücknahme einer erteilten Berechtigung durch die VfB. Eine Rücknahme führt aufgrund der kurzen Zertifikatslaufzeiten zu einer Ablehnung weiterer Zertifikatsanträge bzw. Wiederholungsanträge (siehe Prozeduren in den Abschnitten 3.3 und 3.4).

Die BerCA führt Wiederholungsanträge nur dann durch, wenn keine Sperrung vorliegt. Anhand eines für den Zertifikatsinhaber geführten Merkmals wird entschieden, ob eine Zertifikatsausstellung (Initial- oder Folgezertifikat) erfolgen darf oder nicht.

4.10 Statusabfragedienst für Zertifikate

In der CVCA-eID PKI ist kein Service zur Statusabfrage von Terminalberechtigungszertifikaten vorgesehen.

Die BerCA betreibt einen nicht-öffentlichen Verzeichnisdienst nach Abschnitt 2.1, in dem der aktuelle Bestand der ausgestellten Terminalberechtigungszertifikaten zur Verfügung gestellt wird.

4.11 Beendigung der Teilnahme

Es gilt 4.11 der [CP-eID].

4.12 Schlüsselhinterlegung und –wiederherstellung

Eine Hinterlegung und Wiederherstellung von Schlüsseln wird nicht angeboten.

5. Nicht-technische Sicherheitsmaßnahmen

5.1 Bauliche Sicherheitsmaßnahmen

Die D-Trust GmbH ist ein akkreditierter Zertifizierungsdiensteanbieter nach deutschem Signaturgesetz. Für die baulichen Sicherheitsmaßnahmen liegt eine detaillierte Dokumentation vor (Sicherheitskonzept des signaturgesetzkonformen Zertifizierungsdiensteanbieters [SiKo-DTR]), die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann. Das Sicherheitskonzept wurde durch die von der Bundesnetzagentur anerkannte Prüf- und Bestätigungsstelle TÜV Informationstechnik GmbH geprüft. Die Prüfung und Bestätigung wird nach sicherheitserheblichen Veränderungen sowie in regelmäßigen Zeitabständen wiederholt.

Teil des Sicherheitskonzepts ist eine detaillierte Dokumentation der baulichen Sicherheits- und Überwachungsmaßnahmen, die im Einzelfall und bei begründetem Interesse in den relevanten Teilen eingesehen werden kann.

Die genannten Zertifikate bestätigen der D-Trust GmbH einen hohen Sicherheitsstandard der nicht-technischen Sicherheitsmaßnahmen.

Die BerCA wird unter den gleichen baulichen Bedingungen betrieben wie die CAs der D-Trust GmbH zur Ausstellung qualifizierter Zertifikate mit Anbieterakkreditierung nach deutschem Signaturgesetz.

Für die BerCA wird ein Backup-Konzept umgesetzt, um im Notfall eine zeitnahe Wiederherstellung des Betriebes der BerCA sicherzustellen.

5.2 Verfahrensvorschriften

Teil des Sicherheitskonzeptes ist ein Rollenkonzept [SiKo-DTR], in dem Mitarbeiter einer oder mehreren Rollen zugeordnet werden und entsprechende Berechtigungen erhalten. Die Berechtigungen der einzelnen Rollen beschränken sich auf diejenigen, die sie zur Erfüllung ihrer Aufgaben benötigen. Das Rollenkonzept findet auch beim Betrieb der BerCA Anwendung.

Die Identität, Zuverlässigkeit und Fachkunde des Personals wird vor Aufnahme der Tätigkeit überprüft. Regelmäßige und anlassbezogene Schulungen gewährleisten die Kompetenz in den Tätigkeitsbereichen sowie die allgemeine Informationssicherheit. Schulungen und Leistungsnachweise werden dokumentiert.

Besonders sicherheitskritische Vorgänge müssen mindestens im Vier-Augen-Prinzip durchgeführt werden. Dies wird durch technische und organisatorische Maßnahmen wie beispielsweise Zutrittsberechtigungen und Abfrage von Wissen durchgesetzt.

5.3 Eingesetztes Personal

Die Zertfifizierungsstelle gewährleistet, dass die im Bereich des Zertifizierungs-dienstes tätigen Personen über die für diese Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen.

5.4 Überwachungsmaßnahmen

Die BerCA protokolliert sicherheitssensitive Vorgänge. Somit wird sichergestellt, dass eine unberechtigte oder fehlerhafte Nutzung des Systems im Nachhinein erkannt und analysiert werden kann.

5.5 Archivierung von Aufzeichnungen

Die ausgestellten Terminalberechtigungszertifikate werden für die Archivierungsdauer laut Abschnitt 6.3.1 zur Verfügung gehalten und dann gelöscht.

5.6 Schlüsselwechsel bei der Zertifizierungsstelle

Vor Ablauf des Gültigkeitszeitraumes des aktuellen DV-Berechtigungszertifikates wird ein routinemäßiger Wiederholungsantrag gestellt nach den Vorgaben der [CP-eID]. Der Prozess erfolgt gemäß Abschnitt 3.3 vollständig automatisiert.

Nach Annahme des neuen DV-Berechtigungszertifikates durch die BerCA gegenüber der CVCA-eID wird dieses im System installiert.

5.7 Wiederaufnahme der Tätigkeit nach Kompromittierung oder Notfall

Das Sicherheitskonzept [SiKo-BerCA] berücksichtigt das Vorgehen im Fall einer Kompromittierung des privaten BerCA Schlüssels.

Bei Verdacht auf Kompromittierung oder Missbrauch des privaten Schlüssels der BerCA informiert die BerCA die CVCA-eID sowie die VfB. Dabei informiert der IT-Sicherheitsbeauftragte die CVCA-eID.

Bei Meldung auf Verdacht auf Kompromittierung oder Missbrauch eines privaten Schlüssels eines Diensteanbieters übermittelt die BerCA die vollständigen Unterlagen an die CVCA-eID:

- Bericht über den Vorfall,
- Protokolldaten,
- in Relation stehende Betriebsdokumente.

Die VfB wird ebenfalls informiert.

Fehlgeschlagene oder versäumte, routinemäßige Wiederholungsanträge meldet die BerCA an die VfB.

6. Technische Sicherheitsmaßnahmen

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

Es gilt 6.1.1 der [CP-eID].

Im Vier-Augen-Prinzip erzeugt die Zertifizierungsstelle nach den Richtlinien [TR-03110] und [TR-03116-2] kryptographisch sichere Schlüsselpaare für die BerCA. Die Schlüsselgenerierung findet in einem Sicherheitsmodul (siehe Abschnitt 6.2) statt. Der Zugriff auf den privaten Schlüssel ist durch eine PIN geschützt, die zugriffsgeschützt aufbewahrt wird.

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Die Lieferung privater Schlüssel an den Zertifikatsnehmer erfolgt nicht.

6.1.3 Lieferung öffentlicher Schlüssel an die Zertifizierungsstelle

Siehe Abschnitt 4.1.

6.1.4 Lieferung öffentlicher CA-Schlüssel an Zertifikatsnutzer

Siehe Abschnitt 4.1.

6.1.5 Schlüssellängen

Zur Schlüsselgenerierung werden ausschließlich Schlüssellängen und kryptographische Algorithmen verwendet, die der Richtlinie [TR-03116-2] und [TR-02102] entsprechen.

Die zu verwendenden Schlüsselparameter (Domainparameter) werden durch die CVCA-eID festgelegt und gelten für alle untergeordneten Instanzen (BerCA und Terminalberechtigungszertifikate).

6.1.6 Festlegung der Schlüsselparameter und Qualitätskontrolle

Die Einhaltung der Profilanforderungen nach [TR-03110] an Schlüsselparameter und Request für die BerCA wird nach der Request-Generierung geprüft.

6.1.7 Schlüsselverwendungen

Es gilt 6.1.7 der [CP-eID].

6.2 Sicherung des privaten Schlüssels und Anforderungen an krytographische Module

Es gilt 6.2 der [CP-eID].

6.2.1 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m)

Der Zugriff auf die Signierschlüssel wird bei der Inbetriebnahme des HSMs freigegeben. Die Inbetriebnahme erfolgt im Vier-Augen-Prinzip. Das Ausstellen von Terminalberechtigungszertifikaten ist nur durch den automatischen Prozess möglich.

6.2.2 Hinterlegung privater Schlüssel (key escrow)

Private BerCA- und Terminalschlüssel werden nicht hinterlegt.

6.2.3 Backup privater Schlüssel

Der private Schlüssel der BerCA wird in einem kryptographisch gesicheren Verfahren in das HSM-Cluster migriert. Der private Schlüssel ist zu keinem Zeitpunkt im Klartextzustand.

6.2.4 Archivierung privater Schlüssel

Es findet keine Archivierung privater BerCA- und Terminalschlüssel statt.

6.2.5 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Zur Sicherstellung der Verfügbarkeits- und Lastanforderung werden jeweils zwei kryptographische Module im ausfallsicheren Cluster betrieben. Beide kryptographischen Module verfügen über einen gemeinsamen Key Encryption Key (KEK, AES 128 Bit) der zur Synchronisation des privaten Signierschlüssels der BerCA verwendet wird.

Die Erzeugung des Signaturschlüsselpaares der BerCA erfolgt in einem der beiden kryptographischen Module, der private Schlüssel wird dann mit Hilfe des KEK verschlüsselt und als Kryptogramm zum anderen kryptographischen Modul übertragen. Dort erfolgt die Entschlüsselung und Speicherung der Schlüsselkopie.

6.2.6 Speicherung privater Schlüssel in kryptographischen Modulen

Das Sicherheitsmodul nach Abschnitt 6.2 unterstützt alle Anforderungen der [CP-eID] bezüglich der Speicherung privater Schlüssel.

6.2.7 Aktivierung privater Schlüssel

Die Aktivierung der privaten Schlüssel der BerCA erfordert die Authentisierung mittels PIN gemäß Anforderung der [CP-eID].

6.2.8 Deaktivieren privater Schlüssel

Die Deaktivierung des privaten Schlüssels des DV-Berechtigungszertifikats erfolgt durch Ausschaltens des Kryptographiemodus im Rahmen des Gültigkeitszeitraums des Schlüssels. Der private Schlüssel steht infolge dessesn nicht für Signaturleistungen zur Verfügung und muss bei neuerlicher Nutzung entsprechend Abschnitt 6.2.7 wieder aktiviert werden. Sofern der Gültigkeitszeitraum für den privaten Schlüssel abgelaufen ist, greift Abschnitt 6.2.9.

6.2.9 Zerstörung privater Schlüssel

Nach Ablauf der Gültigkeit der privaten Schlüssel werden diese automatisch gelöscht.

6.2.10 Beurteilung kryptographischer Module

Siehe Abschnitt 6.2.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Alle öffentlichen Schlüssel der CVCA-eID (einschließlich Link-Zertifikate), der BerCA und alle von der BerCA signierten öffentlichen Schlüssel werden in Form der erstellten Terminalberechtigungszertifikate im Verzeichnisdienst gespeichert. Die Terminalberechtigungszertifikate bleiben dort bis zum Ende ihrer Gültigkeit sowie für zwei weitere Jahre gespeichert.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die Gültigkeitsdauer der Schlüssel und Zertifikate wird vorgegeben in der [CP-eID].

Die CVCA-eID ist 3 Jahre gültig.

Die BerCA ist 3 Monate gültig.

Für Terminalberechtigungszertifikate gelten die folgenden Gültigkeitszeiträume:

Terminal	**Anwendung**	**Gültigkeitszeitraum**	
		Nutzung	**Überlappung**
Remote-Terminal Diensteanbieter	Online-Authentisierung (Lesen der eID-Daten)	1 Tag	1 Tag
Remote-Terminal Diensteanbieter	Online-Authentisierung (Verifizieren von Alter und Wohnort)	1 Monat	2 Tage
Remote-Terminal Diensteanbieter	Online-Authentisierung (Nachladen QES)	1 Monat	2 Tage
Offline Terminal Automatenbetrieb	Offline-Authentisierung (Altersverifikation)	1 Monat	1 Woche
Offline Terminal Automatenbetrieb	Offline-Authentisierung (Lesen der eID-Daten)	In Abstimmung mit der Root	

6.4 Aktivierungsdaten

Siehe Abschnitt 6.2.7.

6.5 Sicherheitsmaßnahmen für die Rechneranlagen

Die Zertifizierungsstelle hat als Zertifizierungsdiensteanbieter mit Anbieterakkreditierung ein umfassendes Sicherheitsmanagementsystem implementiert. Für die BerCA wurde ein Sicherheitskonzept [SiKo-BerCA] erstellt. Darüber hinaus gilt Abschnitt 5.1

6.6 Zeitstempel

Entfällt.

6.7 Validierungsmodel

Es gilt die [CP-eID].

7. Profile von Zertifikaten, Sperrlisten und OCSP

7.1 Zertifikatsprofile

Die BerCA stellt die Zertifikats-Requests nach dem in Abschnitt 7.1 – nicht-hoheitlicher Bereich – der [CP-eID] geforderten Formaten und Profilen. Die verwendete CHR ist in Abschnitt 3.1 beschrieben. Der Gültigkeitszeitraum ist in Abschnitt 6.3.2 definiert. Die BerCA prüft, dass die Hash-Werte der korrekten Kommunikationszertifikate des Diensteanbieters in die ProviderInfo innerhalb der Certificate Extensions des Terminalberechtigungszertifikats gemäß [TR-03110] Anhang C.3 aufgenommen werden.

In den Terminalberechtigungszertifikaten werden dem Diensteanbieter jeweils die minimal erforderlichen Zugriffsrechte gewährt.

7.2 Sperrlistenprofile

In der CVCA-eID PKI werden keine Sperrlisten ausgestellt.

Es wird jedoch ein Sperrdienst (im Sinne einer internen Sperrliste gemäß [CP-eID]) geführt, um nicht routinemäßige Wiederholungsanträge nach Abschnitt 3.3 erkennen zu können. Für die internen Sperrlisten bestehen keine Profilvorgaben.

7.3 Profile des Statusabfragedienstes (OCSP)

In der CVCA-eID PKI werden keine Statusabfragedienste eingesetzt.

8. Überprüfungen und andere Bewertungen

8.1 Inhalte, Häufigkeit und Methodik

Für die BerCA gelten die Prüfungsanforderungen gemäß Abschnitt 8 – nicht-hoheitlicher Bereich – der [CP-eID]. Die D-Trust GmbH als Betreiber der BerCA unterwirft sich den Prüfungsanforderungen und wirkt bei der Durchführung der Prüfungen mit.

8.2 Reaktionen auf identifizierte Mängel

Es gilt Abschnitt 8.2 – nicht-hoheitlicher Bereich – der [CP-eID].

9. Sonstige finanzielle und rechtliche Regelungen

9.1 Preise

Keine Angaben.

9.2 Finanzielle Zuständigkeiten

9.2.1 Versicherungsdeckung

Die Zertifizierungsstelle verfügt über eine Versicherungsdeckung gemäß § 12 SigG sowie Versicherungen bezüglich Betriebs- und Produkthaftung.

9.2.2 Andere Ressourcen für Betriebserhaltung und Schadensdeckung

Keine Angaben.

9.2.3 Versicherung oder Gewährleistung für Endnutzer

Keine Angaben.