Certification Practice Statement der D-TRUST CVCA-eID PKI

Version 2.0

Teil der Bundesdruckerei-Gruppe

COPYRIGHT UND NUTZUNGSLIZENZ

Certification Practice Statement
der D-TRUST CVCA-eID PKI

©2023 D-Trust GmbH

This work is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International License.

Anfragen zu einer sonstigen, in der vorgenannten Lizenz nicht enthaltenen Nutzungsart dieses CPS der D-Trust GmbH sind zu richten an:

D-Trust GmbH
Kommandantenstr. 15
10969 Berlin, Germany
Tel: +49 (0)30 259391 0
E-Mail: info@d-trust.net

Dokumentenhistorie

Version	Datum	Beschreibung
1.0	25.10.2019	▪ Initialversion
1.1	19.03.2020	▪ Bearbeitung des Observation Reports im Rahmen der Prüfung TR-03145-1 und TR-03145-4
1.2	02.07.2020	▪ Ergänzungen in den Abschnitten 4.2.2, 4.9.9 und 5.5.2
1.3	17.02.2021	▪ Behebung der offenen Punkte des Observation Reports im Rahmen der Prüfung TR-03145-1 und TR-03145-4 nach Austausch der HSMs. Diesbezügliche Anpassungen in den Abschnitten 4.7.1, 6.1.1 und 6.2.1
1.4	12.08.2021	▪ Jährliches Review des gesamten CPS ▪ Bekanntgabe der Einführung der folgenden hoheitlichen Online-Dienste: PIN-Rücksetzdienst und Ummelde-/Schreibdienst ▪ Ergänzungen bzw. Anpassungen in den Abschnitten 1.1, 1.1.3, 1.6.1, 1.6.2, 1.6.3, 2.2, 6.2.1, 6.2.8, 7.1.2
1.5	04.10.2021	▪ Ergänzungen im Abschnitt 1.1.3
1.6	14.12.2021	▪ Konkretisierung der Registrierung von Terminals in Abschnitt 3.2.3
1.7	05.12.2022	▪ Anpassungen an die CP CVCA eID, Version 2.4.1 vom 08.11.2021. ▪ Ergänzungen in den Abschnitten 1.1, 1.1.3, 1.3.3, 1.6.3, 2.2, 2.4, 3.2.3, 4.2.1, 4.5.2, 4.7.1, 5.2.1, 5.5.1, 5.5.2, 5.7.1, 5.7.2 und 6.6 ▪ Editorische Änderungen ▪ Jährliches Review des gesamten CPS
2.0	05.07.2023	▪ Ergänzungen und Anpassungen in den Abschnitten 1, 2, 4.7 und 5.6 und 9 ▪ Dieses CPS CVCA-eID wird der CP der D-Trust untergeordnet. Abschnitt 9 verweist damit auf die CP der D-Trust. ▪ Jährliches Review des gesamten CPS

Inhaltsverzeichnis

1. Einleitung ... 6
1.1 Überblick ... 6
1.2 Name und Kennzeichnung des Dokuments ... 10
1.3 PKI-Teilnehmer/ Instanzen ... 10
1.4 Verwendung von Zertifikaten ... 12
1.5 Administration der Policy ... 12
1.6 Begriffe und Abkürzungen ... 13
2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen ... 17
2.1 Verzeichnisse ... 17
2.2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen ... 17
2.3 Häufigkeit von Veröffentlichungen ... 18
2.4 Zugriffskontrollen auf Verzeichnisse ... 18
2.5 Zugang und Nutzung von Diensten ... 18
3. Identifizierung und Authentifizierung ... 19
3.1 Namensregeln ... 19
3.2 Initiale Überprüfung der Identität ... 20
3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying) ... 21
3.4 Identifizierung und Authentifizierung von Sperranträgen ... 22
4. Betriebsanforderungen ... 22
4.1 Zertifikatsantrag und Registrierung ... 22
4.2 Verarbeitung des Zertifikatsantrags ... 23
4.3 Ausstellung von Zertifikaten ... 24
4.4 Zertifikatsübergabe ... 24
4.5 Verwendung des Schlüsselpaars und des Zertifikats ... 25
4.6 Zertifikatserneuerung ... 25
4.7 Zertifikatserneuerung mit Schlüsselerneuerung ... 25
4.8 Zertifikatsänderung ... 26
4.9 Sperrung und Suspendierung von Zertifikaten ... 26
4.10 Statusabfragedienst für Zertifikate ... 29
4.11 Austritt aus dem Zertifizierungsdienst ... 29
4.12 Schlüsselhinterlegung und –wiederherstellung ... 29
5. Nicht-technische Sicherheitsmaßnahmen ... 29
5.1 Bauliche Sicherheitsmaßnahmen ... 30
5.2 Verfahrensvorschriften ... 30
5.3 Eingesetztes Personal ... 31
5.4 Überwachungsmaßnahmen ... 32
5.5 Archivierung von Aufzeichnungen ... 32
5.6 Schlüsselwechsel beim DV ... 33
5.7 Kompromittierung und Geschäftsweiterführung beim DV ... 33
5.8 Schließung des DV ... 34
6. Technische Sicherheitsmaßnahmen ... 34
6.1 Erzeugung und Installation von Schlüsselpaaren ... 35
6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module ... 36
6.3 Andere Aspekte des Managements von Schlüsselpaaren ... 37
6.4 Sicherheitsmaßnahmen in den Rechneranlagen ... 37
6.5 Technische Maßnahmen während des Life Cycles ... 37
6.6 Sicherheitsmaßnahmen für Netze ... 38
6.7 Zeitstempel ... 39
7. Profile von Zertifikaten und Sperrlisten ... 39
8. Auditierungen und andere Prüfungen ... 40

Teil der Bundesdruckerei-Gruppe

9. Sonstige finanzielle und rechtliche Regelungen 40

1. Einleitung

1.1 Überblick

Dieses Dokument ist das Certification Practice Statement (CPS) der von D-Trust GmbH betriebenen Vertrauensdienste zur Ausstellung von Berechtigungszertifikaten nimmt Bezug auf die CP (Zertifikatsrichtlinie) der D-Trust GmbH mit der OID 1.3.6.1.4.1.4788.2.200.1 und der Certificate Policy für die Country Verifying Certification Authority eID-Anwendung, Elektronischer Identitätsnachweis und Vor-Ort-Auslesen mit hoheitlichen eID-Dokumenten, Version 2.4.1 vom 08.11.2021 [CP CVCA-eID].

Das hier beschriebene Certification Practice Statement der D-TRUST CVCA-eID PKI wird abgekürzt mit „CPS CVCA-eID".

Die in diesem Dokument als Document Verifier (DV) benannten Rollen sind Trust Service Provider (TSP) der D-Trust im Sinne ihrer CP.

D-Trust ist gemäß Kapitel 3.2 [CP CVCA-eID] hoheitlicher und nicht-hoheitlicher registrierter Document Verifier (DV).

Als hoheitlicher DV (durch das Bundesministerium des Innern bestimmt, die gesetzlichen Grundlagen sind in §20a (1) [PAuswG] in Verbindung mit §36 (2) [PAuswV] dargelegt) erfolgt die Ausstellung von Zertifikaten für die zur Identitätsfeststellung berechtigen Behörden

- für das Auskunftsbegehren des Ausweisinhabers,
- zur Qualitätssicherung bei der Ausgabe des Ausweises bzw. anhand von Testausweisen,
- zur Änderungen der Daten der eID-Funktion im eID-Dokument sowie
- für hoheitliche Online-Dienste wie PIN-Rücksetzdienst und Ummelde-/Schreibdienst.

Die Terminals in den berechtigten Behörden können mit diesen Zertifikaten die oben genannten Aktionen durchführen.

Als nicht-hoheitlicher DV erfolgt die Ausstellung von Berechtigungszertifikaten für den elektronischen Identitätsnachweis gemäß §18 [PAuswG] und das Vor-Ort-Auslesen gemäß §18a [PAuswG] in den Bereichen eBusiness und eGovernment – die D-Trust wird im Folgenden als Berechtigungszertifikateanbieter (BerCA) bezeichnet. Nicht-hoheitliche Berechtigungszertifikate werden an Diensteanbieter (DA) ausgegeben, die erst nach der Ausstellung eines Bescheids durch die Vergabestelle für Berechtigungen (VfB) personenbezogene Daten auslesen können, die für ihren Dienste-Zweck durch die VfB genehmigt wurden. Inhaltliche Grundlagen der CVCA-eID PKI finden Sie im Kapitel 1 der [CP CVCA-eID].

Zur Nutzung von eIDAS-Anwendungen erfolgt die Anbindung der EU-Mitgliedsstaaten über nicht-hoheitlichen Instanzen der BerCA mittels eIDAS-Konnektoren. Ein Mitgliedstaat wird demnach wie ein Diensteanbieter angebunden. Zur zusätzlichen Signatur der Metadaten bei Abfragen von europäischen eID-Services erhält jeder Inhaber eines Berechtigungszertifikates ein Metadaten Signer-Zertifikat. Dieses Zertifikat erhält der eID-Service Provider und hinterlegt dieses im eID Service. Das Zertifikat wird auf Basis eines Zertifikats-Requests (CSR) des eID-Service Providers durch die BerCA ausgestellt. Die Schlüsselverwaltung obliegt dem eID-Service Provider. Ein Diensteanbieter erhält dieses Zertifikat mit seinem Berechtigungszertifikat. Dieses wird an den eID-Service Provider übermittelt, um im eIDAS-Konnektor eingesetzt zu werden. Dieses CPS geht auf die Besonderheiten des Betriebs der SubCA für Metadaten Signer-Zertifikate nur ein, wenn abweichende Verfahren genutzt werden.

Zertifikate, die in der CP [CP CVCA-eID] optional Anwendung finden, werden in dieser CPS seitens D-Trust GmbH nur dann beschrieben, wenn diese auch angeboten werden.

1.1.1 Document Verifer (DV)/ Vertrauensdiensteanbieter

Der Document Verifier (im Folgenden DV abgekürzt) als der Vertrauensdiensteanbieter (Trust Service Provider (TSP)), ist – auch im juristischen Sinne – die

D-Trust GmbH
Kommandantenstr. 15
10969 Berlin.

Der DV kann Teilaufgaben an Dritte auslagern.

Das Kommunikationspostfach für den hoheitlichen DV lautet:

E-Mail: support@bdr.de

Das Kommunikationspostfach für den nicht-hoheitlichen DV (BerCA) lautet:

E-Mail: berca@d-trust.net

Für die Einhaltung der Verfahren im Sinne dieses Dokuments bzw. etwaiger gesetzlicher oder zertifizierungstechnischer Anforderungen an den DV, bleibt der DV, vertreten durch die Geschäftsführung oder deren Beauftragte, verantwortlich.

Die D-Trust GmbH stellt auch Zertifikate für eigene Zwecke aus. Hierbei werden ebenfalls die entsprechenden gesetzlichen bzw. zertifizierungstechnischen Anforderungen eingehalten.

1.1.2 Über dieses Dokument

Diese CPS regelt den Betrieb der CA des Document Verifiers D-Trust, den Zertifizierungsprozess während der gesamten Lebensdauer der von ihr ausgestellten Zertifikate sowie das Zusammenwirken, Rechte und Pflichten der PKI-Teilnehmer.

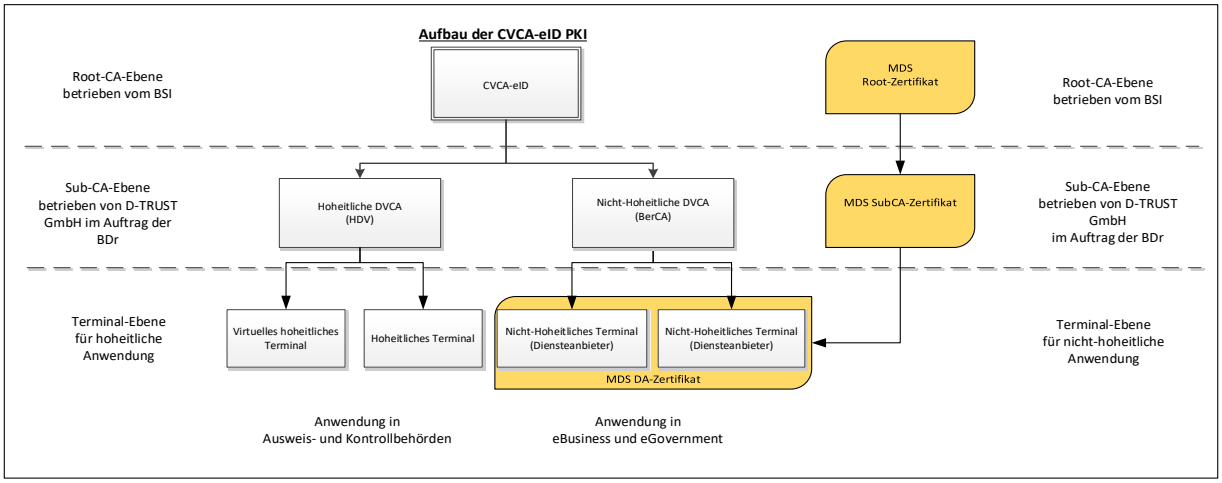
Es werden Mindestmaßnahmen festgelegt, die von allen PKI-Teilnehmern zu erfüllen sind.

Das gesamte CPS ist rechtsverbindlich, soweit dies im Rahmen der deutschen bzw. europäischen Gesetzgebung zulässig ist. Es enthält Aussagen über Pflichten, Gewährleistung und Haftung für die PKI-Teilnehmer. Soweit Garantien oder Zusicherungen betroffen sind, enthält dieses CPS ausschließlich die für diesen Bereich ausdrücklich eingeräumten Garantien oder Zusicherungen.

Die Kenntnis der in diesem CPS 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 PKI gewährte Vertrauens- und Sicherheitsniveau für Ihre Anwendungen geeignet ist.

Die Struktur dieses Dokumentes folgt dem Internet-Standard RFC 3647 „Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework".

1.1.3 Eigenschaften der PKI



Die Wurzelinstanz CVCA-eID wird entsprechend §32 [PAuswV] durch das Bundesamt für Sicherheit in der Informationstechnik betrieben.

Die hoheitlichen Document Verifier werden gemäß §36 (2) [PAuswV] durch das Bundesministerium des Innern bestimmt und stellen ausschließlich Zertifikate für die zur Identitätsfeststellung berechtigen Behörden (Ausweis- und Kontrollbehörden) aus (vgl. §36 (1) [PAuswV] und §20a [PAuswG]).

Die nicht-hoheitlichen Document Verifier (DV) erstellen Berechtigungszertifikate für den elektronischen Identitätsnachweis gemäß §18 [PAuswG] und das Vor-Ort-Auslesen gemäß §18a [PAuswG] in den Bereichen eBusiness und eGovernment und werden auch als Berechtigungszertifikateanbieter (BerCAs) bezeichnet.

Für den nicht-hoheitlichen Anwendungsbereich stellt die CVCA-eID zusätzlich ein selbst-signiertes Metadaten Signer Root-Zertifikat sowie Metadaten Signer SubCA-Zertifikate für die Document Verifier aus, um die Nutzung von eIDAS-Anwendungen gemäß eIDAS-Verordnung (siehe [eIDAS-VO]) zu ermöglichen. Dazu werden so genannte eIDAS-Konnektoren entsprechend der [eIDAS-Inter] eingesetzt.

Ein DV (BerCA) stellt für jeden bei ihm registrierten Diensteanbieter ein Metadaten Signer DA-Zertifikat aus, sofern der DA eIDAS-Anwendungen anbieten möchte. Erzeugung, Besitz und Nutzung der entsprechenden privaten Schlüssel erfolgt analog zu den privaten Schlüsseln der Terminal-Zertifikate[1]. Ein Diensteanbieter erhält dieses Zertifikat mit seinem Berechtigungszertifikat. Dieses wird an den eID-Service Provider übermittelt, um im eIDAS-Konnektor eingesetzt zu werden.

Die MDS-Zertifikate entsprechen dem X.509 Format gemäß [RFC5280] und werden in Zertifikatstypen gemäß Kapitel 1.2.2 der [CP CVCA-eID] unterschieden.

[1] d.h. zum Beispiel, wenn der Diensteanbieter den Betrieb des eID-Servers bei der D-Trust beauftragt, erzeugt und nutzt die D-Trust den Schlüssel im Auftrag des DA. Die D-Trust als eID-Server Provider kann somit unterschiedliche Schlüsselpaare für unterschiedliche DA verwalten.

Zusätzlich werden TLS-Zertifikate des Diensteanbieters hinterlegt. Alle oben genannten Zertifikate entsprechen den Anforderungen aus [eIDAS-Crypto] und der [TR-03116-2].

In folgender Tabelle sind die CA-Hierarchien unter Angabe des Anwendungsfalls und dessen Laufzeiten aufgeführt:

Ebene	**Zertifikatstyp eID** **Zertifikatslaufzeit** **Sperrliste**	**Zertifikatstyp MDS** **Zertifikatslaufzeit** **Sperrliste**
Root-CA	DECVCAeID 3 Jahre Keine CRL	DECVCAeID Metadata Signer Root Germany 6 Jahre CRL: BSI
Sub-CA	*Hoheitlich:* DVCA-AT: DEDVeIDBDR1 DVCA-AT: DEDVeIDBDR5 *Nicht-hoheitlich:* DVCA-AT: DEDVeIDDTR1 Max. 90 Tage Keine CRL	*Nicht-hoheitlich:* DEDVeIDDTR1 6 Jahre CRL: BSI
Berechtigungs-zertifikat	*Hoheitlich:* DEE01xxxx DE9xxxx 1+1 Tage *Nicht-hoheitlich:* DE0000xxx 1+1 Tage 1+3 Tage (eIDAS-MS) Keine CRL	*Nicht-hoheitlich:* DE0000xxx 3 Jahre CRL: D-Trust
Typ	CV-Zertifikat	X.509
Algorithmus Kurve	ECDSA Brainpool P256r1	ECDSA NIST Kurven secp256

Tabelle 1: CA-Hierarchie und Laufzeiten

Die Gültigkeitsdauer von Berechtigungszertifikaten wird gemäß §34 [PAuswV] geregelt. Das Bundesamt für Sicherheit in der Informationstechnik legt im Kapitel 4.7.1 der [CP CVCA-eID] angemessene Höchstgrenzen für die Gültigkeitszeiträume von Zertifikaten je nach Anwendungsbereich und PKI-Instanz fest. Die Gültigkeitsdauer für Berechtigungszertifikate für eIDAS-Mitgliedsstaaten weicht hiervon ab und ist im [Annex CP CVCA-eID] geregelt. Bei der Ausstellung von Zertifikaten werden diese Gültigkeitszeiträume berücksichtigt.

1.2 Name und Kennzeichnung des Dokuments

Dokumentname:	Certification Practice Statement der D-TRUST CVCA-eID PKI
Kennzeichnung (OID):	1.2.276.0.80.7.500.30
Version	2.0

1.3 PKI-Teilnehmer/ Instanzen

1.3.1 Zertifizierungsinstanzen

Nicht-hoheitliche beziehungsweise eID-Anwendung

Die DVCA (BerCA) ist für die Ausgabe von Berechtigungszertifikaten[2] an Diensteanbieter autorisiert. Zwischen Diensteanbieter und BerCA wird ein bilateraler Vertrag geschlossen. Wird nicht der eID-Service der D-Trust GmbH genutzt, muss zusätzlich ein bilateraler Vertrag zwischen der BerCa und dem eID-Service Provider des Diensteanbieters bestehen. Sowohl die Zugriffsrechte als auch die Gültigkeitsdauer der Berechtigung für Diensteanbieter werden von der Vergabestelle für Berechtigungszertifikate (VfB) gemäß §21 [PAuswG] vorgegeben. Die DVCA (BerCA) stellt entsprechend dem im Bescheid des VfB befristeten Zeitraum ein digitales Berechtigungszertifikat mit den in der [CP CVCA-eID] genannten Gültigkeiten aus. Die Berechtigung kann auf Antrag beim VfB wiederholt erteilt werden (entspricht einer Verlängerung der Berechtigung) oder auch zurückgezogen werden. Nutzt ein Diensteanbieter einen anderen eID-Service Provider, so ist ebenfalls ein bilateraler Vertrag erforderlich. Die D-Trust GmbH hat in diesem Fall einen Vertag mit dem eID-Service Provider, der die Rechte und Pflichten der Teilnehmer der PKI regelt.

Hoheitliche Anwendung (HDV)

Zwischen dem Bundesministerium des Innern und der Bundesdruckerei GmbH besteht ein Rahmenvertrag, in dem der Anwendungsbereich der hoheitlichen Document Verifier (HDV) geregelt ist. Die DVCA (HDV) für hoheitliche Anwendungen ist eine organisatorische Einheit, welche von der CVCA-eID zur Ausgabe von hoheitlichen Berechtigungszertifikaten (Terminalberechtigungszertifikaten) für ausschließlich hoheitliche Terminals in berechtigen Behörden zur Identitätsfeststellung gemäß §36 (1) [PAuswV]) eingesetzt werden. Die hoheitlichen Terminals sind Geräte, die zur Beantragung, Anzeige, Veränderung und Ausgabe von Personaldokumenten, in Behörden autorisiert sind. Gemäß §36 (2) [PAuswV] legt das Bundesministerium des Innern fest, welche Behörden dies sind.

---

[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.

1.3.2 Registrierungsinstanzen (Registration Authority, RA)

Eine Registrierungsinstanz ist für die Registrierung und Verwaltung der Zertifikatsnehmer zuständig. Gemäß Kapitel 1.4.2 der [CP CVCA-eID] müssen die Teilnehmer eindeutig und sicher identifiziert werden. Die Registrierungsinstanz erfüllt alle Aufgaben gemäß Kapitel 1.4.2 der [CP CVCA-eID].

Nicht-hoheitliche Anwendung (BerCA)

Für nicht-hoheitliche Aufgabenstellungen des elektronischen Identitätsnachweises verantwortet den Registrierungsdienst die „Vergabestelle für Berechtigungs-zertifikate (VfB)". Diese Aufgabe ist einer Institution der Bundesverwaltung zugeordnet und wird vom Bundesverwaltungsamt wahrgenommen.

Der Teilnehmerservice der BerCA gewährleistet die sichere Teilnehmeridentifikation im Rahmen des technisch etablierten Prozesses, beschrieben in Abschnitt 3.2.2 Identifizierung und Authentifizierung von Organisationen.

Die Registrierungstätigkeit der Registrierungsstelle der D-Trust beinhaltet die Prüfung des Bescheids der VfB und die Einrichtung des Diensteanbieters zum Erhalt von Berechtigungszertifikaten.

Hoheitliche Anwendung (HDV)

Jede Behörde ernennt schriftlich mindestens einen und maximal zwei Mitarbeiter/in zum EAC-Beauftragten und bestätigt diese/n durch einen Zeichnungsberechtigten, legitimiert durch ein Dienstsiegel der jeweiligen Behörde. Der EAC-Beauftragte erhält einen sicheren Zugang zum Service-Portal der Bundesdruckerei (https://support.bundesdruckerei.de), über das der EAC-Beauftragte der jeweiligen Behörde die benötigten Leistungen abrufen kann.

1.3.3 Zertifikatsnehmer (ZNE)

Ein Zertifikatsnehmer ist der Inhaber eines Zertifikats und im Besitz des zugehörigen privaten Schlüssels gemäß Kapitel 1.4.3 der [CP CVCA-eID].

Nicht-hoheitliche Anwendung (BerCA)

Zulässige Zertifikatsnehmer sind Diensteanbieter nach §2 Abs. 3 [PAuswG]. Diensteanbieter benötigen zur Erbringung ihrer Dienste Zugriff auf die eID-Funktion des elektronischen Personalausweises. Zu diesem Zweck beantragen sie ein Berechtigungszertifikat, welches ihnen den Zugriff ermöglicht. Ein Diensteanbieter kann einen eID-Service Provider beauftragen, den Zugriff auf die Authentisierungsfunktion technisch umzusetzen. Des Weiteren sind Diensteanbieter Zertifikatsnehmer der Metadaten Signer DA-Zertifikate, die ebenfalls vom DV ausgestellt werden.

Die Zertifikate werden an den Diensteanbieter oder seinen beauftragten eID-Service Provider übergeben und in dessen Anwendung eingesetzt.

Hoheitliche Anwendung (HDV)

Zulässige Zertifikatsnehmer sind die berechtigten Behörden, die gemäß §36 (2) [PAuswV] und §20a [PAuswG] durch das Bundesministerium des Innern festgelegt werden. Jede berechtigte Behörde autorisiert bestimmte Mitarbeiter zu EAC-Beauftragten (Schlüsselbeauftragter im Rahmen der PKI), welche den Bedarf der Behörde an Terminals und der zugehörigen Bedienerkarten bei der Bundesdruckerei (RA) abrufen können. Die jeweiligen Berechtigungszertifikate werden nach Inbetriebnahme des Terminals ausgestellt und über einen automatisierten Prozess im Terminal genutzt. Zur Inbetriebnahme ist in der jeweiligen Behörde

das Terminal mittels einer Bedienerkarte und einer PIN zu aktivieren. Der EAC-Beauftragte verantwortet die Nutzung der Terminals und der zugehörigen Bedienerkarten und damit der Terminalberechtigungszertifikate innerhalb seiner Behörde.

1.3.4 Zertifikatsnutzer (ZNU)

Zertifikatsnutzer verwenden die Zertifikate der CVCA-eID PKI, um Berechtigungen festzustellen und Signaturen zu prüfen, gemäß Kapitel 1.4.4 der [CP CVCA-eID].

1.3.5 Andere PKI-Teilnehmer

Es gilt der Kapitel 1.4 der [CP CVCA-eID].

1.3.6 Zugang zum Wirk- oder Testsystem

Jeder PKI-Teilnehmer kann neben dem Zugang zum Wirksystem auch das jeweilige Testsystem nutzen. Für nicht-hoheitliche Dienstanbieter wird der Zugang über den Vertrag geregelt.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendung von CV-Schlüsselpaar und CV-Zertifikat

Die innerhalb der CVCA-eID PKI erzeugten Zertifikate und Schlüssel dürfen nicht zu einem anderen Zweck verwendet werden, als die im Kapitel 4.6.1 der [CP CVCA-eID] genannten und im VfB Bescheid erlaubten Zwecke.

1.4.2 Erlaubte Verwendung von MDS-Schlüsselpaar und MDS-Zertifikat

Die erzeugten MDS-Zertifikate dürfen nur zu den in Kapitel 4.6.2 der [CP CVCA-eID] eingesetzt werden.

1.4.3 Verbotene Verwendungen von Zertifikaten

Andere Verwendungsarten als die im Kapitel 4.6.1 der [CP CVCA-eID] festgelegten, sind nicht zulässig.

1.5 Administration der Policy

1.5.1 Zuständigkeit für das Dokument

Dieses CPS wird im Auftrag der Bundesdruckerei GmbH durch die D-Trust GmbH gepflegt und aktualisiert. Der Beauftragte der Geschäftsführung der D-Trust GmbH übernimmt die Abnahme des Dokuments.

Dieses CPS wird jährlich durch den DV überprüft und gegebenenfalls aktualisiert. Zusätzlich führen Änderungen in Verfahrensweisen oder technischen Maßnahmen zu einer Änderung der CPS. Eine Änderung wird durch eine neue Versionsnummer dieses Dokumentes kenntlich gemacht.

Kontaktdaten siehe 1.1.1

1.5.2 Meldung von Sicherheitsvorfällen mit Zertifikaten

Als Sicherheitsvorfall wird jegliches erfolgreiche Umgehen von Sicherheitsmaßnahmen, unbefugter Zugriff auf sensible Daten oder der Missbrauch des privaten Schlüssels definiert (siehe auch 4.9.1 Bedingungen für eine Sperrung).

Die Vorgehensweise bei Kompromittierung oder anderen Sicherheitsvorfällen wird im Kapitel 5.2.3 der [CP CVCA-eID] für die verschiedenen Root, DV und Terminal-Ebenen beschrieben.

Jede Ebene hat unverzüglich die nächst höhere Instanz in der PKI zu informieren und wichtige Informationen wie Bericht über den Vorfall, Protokolldaten und in Relation stehende Betriebsdokumente zu übergeben.

Bei nicht-hoheitlichen Terminalbetreibern wird gleichzeitig die VfB informiert.

Der DV D-Trust stellt folgende E-Mail-Adresse für die Meldung von Sicherheitsvorfällen bereit:

security.incident@d-trust.net

1.5.3 Eingliederung dieses CPS

Dieses CPS ist der [CP CVCA-eID] untergeordnet und bestätigt die Erfüllung der erforderlichen Anforderungen. Das Bundesamt für Sicherheit in der Informationstechnik erhält dieses Dokument vor Inkrafttreten. Jede Änderung wird dem Bundesamt für Sicherheit in der Informationstechnik vorab mitgeteilt.

1.6 Begriffe und Abkürzungen

1.6.1 Begriffe und Namen

Hoheitliche Berechtigungs-zertifikate	Aus der hoheitlichen DVCA (HDV) ausgestellten Berechtigungszertifikate für zur Identitätsfeststellung berechtigte Behörden.
Nicht-hoheitliche Berechtigungs-zertifikate	Aus der nicht-hoheitlichen DVCA (BerCA) ausgestellte Zertifikate für Diensteanbieter.
Certificate Policy (CP)	Zertifikatsrichtlinie. In diesem Fall gilt die „Certificate Policy für die Country Verifying Certification Authority eID-Anwendung" vom BSI, abgekürzt [CP CVCA-eID].
Certification Practice Statement (CPS)	Umsetzungserklärung der CA. In diesem Fall der DVCA, als auch der SubCA für Metadaten Signer-Zertifikate.
Country Code	Länderkennzeichen
CVCA-eID	PKI nach [CP CVCA-eID]
Document Verifier (DV)	▪ Document Verifier ist der Trust Service Provider (TSP), d.h. der Vertrauensdiensteanbieter. ▪ Document Verifier ist Zertifikatsnehmer und Zertifizierungsinstanz der mittleren PKI-Ebene (siehe Kapitel 1.4 der [CP CVCA-eID])
DVCA (BerCA) - Nicht-hoheitlicher Anwendungsbereich	Im Auftrag der Bundesdruckerei GmbH von der D-Trust GmbH technisch und organisatorisch betriebene nicht-hoheitliche PKI unterhalb der CVCA-eID PKI.
DVCA (HDV) - Hoheitlicher Anwendungsbereich	Im Auftrag vom Bundesministerium des Innern organisatorisch von der Bundesdruckerei GmbH und technisch von der D-Trust GmbH betriebene hoheitliche PKI unterhalb der CVCA-eID PKI.
Holder Mnemonic	Inhaberkürzel eines CV Zertifikats
Kommunikations-zertifikate	X.509-Zertifikate zur Absicherung der Kommunikationsbeziehungen.
Registrierungs-stelle/-instanz (RA)	Einrichtung der PKI, die die Teilnehmeridentifizierung vornimmt, siehe Abschnitt 1.3.2.

	Sowohl für hoheitliche als auch nicht-hoheitliche Anwendungen wirken bei den Registrierungsaufgaben hoheitliche Körperschaften/Behörden mit und übernehmen Teilaufgaben der RA. Für hoheitliche Anwendungen sind es die Behörden, die durch das BMI bestimmt wurden und für nicht-hoheitliche Anwendung ist es die VfB). Die darüber hinaus gehenden RA Aufgaben werden von der Bundesdruckerei und der D-Trust GmbH umgesetzt.
Relying Party	Zertifikatsnutzer
Trustcenter	Der Sicherheitsbereich in den Räumen der D-Trust GmbH
Trust Service Provider (TSP)	Die Bezeichnungen „Trust Service Provider" (TSP) und „Document Verifier" (DV) werden synonym verwendet.
Zertifikatsnehmer	Zertifikatsnehmer erhalten Zertifikate, siehe Abschnitt 1.3.3 Zertifikatsnehmer. Eine Instanz der PKI, die von einer übergeordneten Instanz Zertifikate bezieht (siehe Abschnitt 1.4.3). Ausnahme bildet die CVCA-eID, die sich selbst Zertifikate ausstellt. Siehe [CP CVCA-eID]
Zertifikatsnutzer	Zertifikatsnutzer in der CVCA-eID PKI sind CVCA-eID, Document Verifier, Terminals, hoheitliche eID-Dokumente und eIDAS-Services gemäß [eIDAS-Inter], siehe Abschnitt 1.4.4 der [CP CVCA-eID].
Zertifikatsrichtlinie (CP)	Siehe Certificate Policy - (CP)
Zertifizierungs-stelle/ -instanz	Certification Authority – (CA), siehe Abschnitt 1.3.1

Weitere Regelungen sind in der CP des BSI im Kapitel 8.1 der [CP CVCA-eID] festgehalten.

1.6.2 Abkürzungen

BerCA	Certification Authority eines Berechtigungszertifikateanbieters
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority - Instanz der PKI, die Zertifikate an weitere PKI Teilnehmer ausstellt.
CAR	Certification Authority Reference
CC	Common Criteria for Information Technology Security Evaluation
CHR	Certificate Holder Reference
CP	Certificate Policy - Zertifikatsrichtlinie
CPS	Certification Practice Statement
CRL	Certificate Revocation List (Zertifikatssperrliste)
CSCA	Country Signing Certificate Authority
CSR	Certificate Signing Request bzw. Zertifikats-Request
DV	Document Verifier

eID	elektronischer Identitätsnachweis (Anwendung in elektronischen Ausweisdokumenten)
eID-Dokument	„eID-Dokument" wird als Oberbegriff für den elektronischen Personalausweis, den elektronischen Aufenthaltstitel und die eID-Karte für Unionsbürger sowie für die Smart-eID verwendet.
eIDAS-MS	EU Mitgliedsstaaten im Rahmen des eIDAS
HSM	Hardware Sicherheitsmodul
MDS	Metadaten Signer
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority - Registrierungsstelle
RFC	Requests for Comments Technischer Standard
SPOC	Single Point of Contact - Kommunikationsschnittstelle zur CVCA-eID
TLS	Transport Layer Security (Protokoll Verbindungsauthentisierung/Verschlüsselung)
TSP	Trust Service Provider
VfB	Vergabestelle für Berechtigungszertifikate

Weitere Regelungen sind im Kapitel 8.2 der [CP CVCA-eID] festgehalten.

1.6.3 Referenzen

[CP CVCA-eID]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Elektronischer Identitätsnachweis mit dem elektronischen Personalausweis, in der Version, 2.4.1
[Annex CP CVCA-eID]	Bundesamt für Sicherheit in der Informationstechnik, Vorgaben für die Ausgabe von Berechtigungszertifikaten an andere EU-Mitgliedsstaaten Version 1.0.1
[eIDAS-Crypto]	eIDAS - Cryptographic requirements for the Interoperability Framework TLS and SAML - https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/467109280/eIDAS%20Cryptographic%20Requirement%20v.1.2%20Final.pdf
[PAuswG]	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz – PAuswG)
[PAuswV]	Verordnung über Personalausweise, eID-Karten für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums und den elektronischen Identitätsnachweis (Personalausweisverordnung – PAuswV)
[RFC3647]	Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, November 2003
[RFC5280]	D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[TR-03110]	BSI: Technical Guideline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS-Token

[TR-03116-2]	BSI: Technische Richtlinie TR-03116-2 - Kryptografische Vorgaben für Projekte der Bundesregierung
[TR-03128]	Technische Richtlinie TR-03128 Diensteanbieter für die eID-Funktion Teil 1: Elektronischer Identitätsnachweis und Vor-Ort-Auslesen
[TR-03129]	BSI: Technical Guideline TR-03129 - PKI for the Extended Access Control (EAC), Protocol for the Management of Certificates and CRLs
[TR-03145]	BSI TR-03145 Secure Certification Authority operation
[TR-03145-1]	BSI: Technical Guideline TR-03145-1 - Secure CA operation, Part 1 - Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high'
[TR-03145-4]	BSI: Technical Guideline TR-03145-4 - Secure CA operation, Part 4 - Specific requirements for Authorization Certificate Authorities (BerCA) of the CVCA-eID PKI
[AGB]	Allgemeine Geschäftsbedingungen der D-Trust GmbH

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

2.1.1 Certificate Policy und Certification Practice Statement

Die CP der D-Trust und dieses CPS und alle vorherigen Versionen stehen im PDF/A-Format im Repository des DV öffentlich zur Verfügung:

https://www.d-trust.net/repository.

2.1.2 Zertifikatsverzeichnisse

Es werden Zertifikats-Verzeichnisse, wie in Kapitel 2.1 der [CP CVCA-eID] beschrieben, betrieben. Die ausgestellten Zertifikate der dort genannten Typen verbleiben für die Dauer der Laufzeit zuzüglich der in Kapitel 2.1 der [CP CVCA-eID] definierten Archivierungsdauer in den Verzeichnissen.

2.1.3 Sperrinformationen und Statusdienste

Die DVCAs stellen für CV-Zertifikate keine Online-Statusdienste der Zertifikate zur Verfügung.

Die aktuelle Sperrliste für Metadaten Signer-Zertifikate wird unter folgender Adresse öffentlich zur Verfügung gestellt:

www.d-trust.net/crl/dedveiddtr1.crl

2.2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.2.1 Certification Practice Statement

Der DV veröffentlicht folgende Informationen:

- dieses CPS wird im angegebenen Verzeichnis entsprechend Abschnitt 2.1 veröffentlicht.

Dieses CPS nimmt Bezug auf die Certificate Policy der CVCA-eID mit der OID 0.4.0.127.0.7.3.1.1.2.2 und dem Titel „Certificate Policy für die Country Verifying Certification Authority eID-Anwendung". Abgekürzt wird diese CP in zwei Varianten:

- [CP CVCA-eID] -> diese Abkürzung wird in der CP vom BSI selbst verwendet und
- [CP-eID] -> diese Abkürzung wird in den TR's verwendet.

2.2.2 Wurzelzertifikate

Die aktuellen Root-Zertifikate (CVCA, CSCA und Metadaten Signer Root-Zertifikat) sind auf der Webseite des BSI verfügbar:

https://www.bsi.bund.de/cvca-eID

2.2.3 Terminalbetreiber spezifische Zertifikate und weitere Datenobjekte

Die D-Trust GmbH als DVCA stellt sowohl dem hoheitlichen als auch dem nicht-hoheitlichen Terminalbetreiber folgende Zertifikate bereit, die nicht öffentlich zugänglich sind.

- Dem Terminalbetreiber/eID-Service Provider werden zu jeder Zeit alle für die eID-Authentisierung (siehe [TR-03110]) erforderlichen Zertifikate über die Kommunikationsschnittstelle gemäß [TR-03129] bereitgestellt:

- alle gültigen CVCA Zertifikate bzw. CVCA Link-Zertifikate,
- das eigene derzeit gültige DV-Zertifikat,
- das Metadaten Signer Root-Zertifikat und das SubCA Zertifikat. Metadaten Signer-Zertifikate werden nur im nicht-hoheitlichen Anwendungsbereich eingesetzt.
- alle ihm zugeordneten Zertifikate, die innerhalb der letzten 10 ½ Jahre gültig waren

▪ Weiterhin werden über dieselbe Kommunikationsschnittstelle folgende Listen und Zertifikate bereitgestellt:

- die aktuelle Masterlist,
- die aktuelle Defectlist,
- das aktuelle CSCA Zertifikat

Die zugehörige jeweils aktuelle Sperrliste (Certificate Revocation List, CRL) für die Passive Authentisierung gemäß [TR-03110] kann über den im CSCA Zertifikat angegebenen Sperrlisten-Verteilungspunkt
(CRL Distribution Point (CRL DP)) abgerufen werden.

Wenn eID-Dokumente als verloren bzw. gestohlen gemeldet werden, erfolgt die Meldung der Ausweissperrung an den eID-Sperrdienst, der dann die eID-Sperrliste für Diensteanbieter erstellt. Die eID-Sperrliste wird vom eID-Service des Diensteanbieters geprüft, und wenn eine Sperrung vorliegt, wird der betroffene Ausweis/ das eID-Dokument für eBusiness und eGovernment Transaktionen nicht zugelassen.

Bestehende eID-Revocation-Listen werden bei der Neuberechnung überschrieben. Sie werden in dem in [TR-03145-4], Annex 3 definierten ASN.1-Kodierungsregeln berechnet.

Der eID-Sperrdienst ist nicht Gegenstand der Berechtigungs-CA.

Siehe Kapitel 5.3 [TR-03127].

2.3 Häufigkeit von Veröffentlichungen

Es findet keine Veröffentlichung von Zertifikatsinformationen statt. Die DVCA stellt zu Revisionszwecken sicher, dass es jederzeit möglich ist, den aktuellen Bestand der ausgestellten Terminalberechtigungszertifikate festzustellen. Im Sinne der [CP CVCA-eID] Kapitel 2 werden zu jeder Zeit alle weiteren für die eID-Authentisierung erforderlichen Zertifikate für die Teilnehmer bereitgestellt.

Dies erfolgt über die Kommunikationsschnittstelle gemäß [TR-03129].

2.4 Zugriffskontrollen auf Verzeichnisse

Dieses CPS kann öffentlich und unentgeltlich 24x7 abgerufen werden. Der Verzeichnisdienst hat eine Verfügbarkeit von mindestens 98,5%. Der TSP stellt sicher, dass im Falle einer Störung die Ausfalldauer (downtime) maximal vier Stunden beträgt. Es gibt keine Zugriffsbeschränkungen für lesenden Zugriff. Änderungen der Verzeichnis- und Webinhalte werden ausschließlich vom DV vorgenommen.

Der aktuelle Bestand und der aktuelle Status der registrierten Terminals und ausgestellten Berechtigungen für Diensteanbieter werden nicht veröffentlicht. Die CVCA kann jederzeit eine Auskunft anfordern.

2.5 Zugang und Nutzung von Diensten

Diese Regelungen sind in der CP der D-Trust beschrieben.

Darüber hinaus haben die Systeme der CVCA-eID zur:

- Ausstellung von Berechtigungszertifikaten für eID-Dienstanbieter
- Ausstellung von Terminalzertifikaten für hoheitliche Terminals
- Bereitstellung von Zertifikaten
- Bereitstellung von Sperrinformationen

eine Verfügbarkeit von 98, 5% bezogen auf einen Berechnungszeitraum von 30 Tagen.

3. Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

DV-Zertifikat

Die DV-Zertifikate der DVCA (BerCA) und der DVCA (HDV) entsprechen dem in Abschnitt 3.1.1 der [CP CVCA-eID] geforderten Format. Das verwendete Betreiberkürzel lautet:

DVCA (BerCA - nicht-hoheitlich): DTR<>

DVCA (HDV - hoheitlich): BDR<>

Die Certificate Holder Reference (CHR) der Berechtigungszertifikate, bestehend aus den Elementen Country Code, Holder Mnemonic und Sequence Number, wird von der DVCA entsprechend [TR-03110] im Abschnitt A7.1 vergeben und zugewiesen. In Kapitel 3.1 [CP CVCA-eID] ist die zulässige Belegung der Felder genau beschrieben.

Der CHR eines DV-Zertifikats ist bezüglich des zugehörigen CVCA-Zertifikats eindeutig.

Terminal-Zertifikat

Ein Terminal-Zertifikat ist immer innerhalb der CVCA-eID PKI eindeutig über die Kombination der Werte der beiden folgenden Zertifikatsfelder identifizierbar (siehe [TR-03110] Abschnitt A7.1):

- Certification Authority Reference (CAR): Der Wert des CAR-Feldes entspricht dem des CHR-Feldes aus dem DV-Zertifikat des DVs, welcher das Terminal-Zertifikat signiert.
- Certificate Holder Reference (CHR): Den Inhalt des CHR-Feldes gibt die ausstellende DV unter Berücksichtigung der Anforderungen aus [TR-03110] vor.

Infolgedessen entspricht die CAR in einem Zertifikat dem CHR des korrespondierenden Zertifikats der ausstellenden Zertifizierungsstelle.

Der CHR eines Terminal-Zertifikats ist bezüglich des zugehörigen DV-Zertifikats eindeutig.

Darüber hinaus gelten für die Namensgebung die Anforderungen aus Kapitel 3.1 der [CP CVCA-eID].

3.1.2 Notwendigkeit für aussagefähige Namen

Terminals werden durch Country Code, Holder Mnemonic und Sequence Number [TR-03110]; Anhang A.7.1 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 „Arten von Namen" verwendet. Der Bezeichner im Feld Certificate Holder Reference (CHR) ist eindeutig und referenziert auf den Öffentlichen Schlüssel (Public Key) im Zertifikat. Die TR-03110; Part 3: Common Specifications; Version 2.21; A.7.Terminal Authentication; A.7.1. Public Key References konkretisiert diese Vorgaben zur Namensgebung.

3.1.5 Eindeutigkeit von Namen

Berechtigungszertifikate für Diensteanbieter 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 DVCA (BerCA) vergibt pro Bescheid auf ein Berechtigungszertifikat eine eindeutige Holder Mnemonic.

Berechtigungszertifikate für hoheitliche Terminals sind ebenfalls eindeutig der berechtigten Behörde zugeordnet. In den Stammdaten wird zusätzlich die Gerätenummer des jeweiligen Terminals gepflegt, so dass immer bekannt ist, welches Zertifikat in welchem Terminal verwendet wird.

Die sequenziell ausgestellten Berechtigungszertifikate erhalten jeweils eine eindeutige Seriennummer.

3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen

Keine Vorgaben.

3.2 Initiale Überprüfung der Identität

3.2.1 Nachweis für den Besitz des privaten Schlüssels

Der öffentliche Schlüssel der Terminalberechtigungszertifikate wird der DV (BerCA) bei der Beantragung innerhalb eines Zertifikats-Request (CSR) nach [TR-03110]; Part 3 Anhang D.3 übermittelt. Im Rahmen der Antragsprüfung wird durch Verifikation der inneren Signatur nachvollzogen, ob der Zertifikatsnehmer im Besitz des privaten Schlüssels ist.

3.2.2 Identifizierung und Authentifizierung von Organisationen

Die Identifikation und initiale Registrierung von hoheitlichen und nicht-hoheitlichen berechtigten Stellen (Behörden und Diensteanbieter) erfolgt nicht durch den Document Verifier D-Trust. Im Rahmen der Registrierung erfolgt ausschließlich die Prüfung des Dienstsiegels des Antragstellers über zur Verfügung gestellte Register (HDV) beziehungsweise die Prüfung eines Bescheids der VfB (BerCA).

Nicht-hoheitliche Anwendung (BerCA)

Im Vorfeld der Beantragung von Berechtigungszertifikaten durchlaufen Diensteanbieter respektive deren beauftragte eID-Service Provider mit der Zertifizierungsstelle einen vorbereitenden Prozess, der die initiale Teilnehmeridentifizierung umfasst. Auf dessen Basis stellt die VfB einen Bescheid aus und übermittelt diesen verschlüsselt an den DV. Auf Grundlage des Bescheids wird durch Mitarbeiter der Registrierung die Erstellung der erforderlichen Zertifikate im CA-System angelegt (RA BerCA). Jede Änderung der Registrierungsdaten sind vom Diensteanbieter unverzüglich dem VfB als auch der RA BerCA zu melden. Nach neuem VfB-Bescheid wird ein geändertes Berechtigungszertifikat ausgestellt.

Für eIDAS Anwendungen wird dadurch ebenfalls die Ausstellung des Metadaten Signer-Zertifikats legitimiert. Gleichgesetzt dem Bescheid ist die Registrierung eines EU-Mitgliedsstaats nach eIDAS durch das BSI.

Hoheitliche Anwendung (HDV)

Die Bundesdruckerei pflegt kontinuierlich die Stammdaten der berechtigten Behörden/Organisationen. Ergänzung/Änderung erfolgt über den „Fragenbogen für Personalausweis- und Passbehörden". Der Antrag auf ein Terminal und damit auf die benötigten CV-Zertifikate erfolgt durch die benannte Rolle des EAC-Beauftragten, bestätigt mit dem Dienstsiegel. Es erfolgt damit die Beauftragung der Ausstellung einer Operatorkarte auf eine Organisation (Behörden). Nach Prüfung der Berechtigung in den Stammdaten und der Ansprechpartnerübersicht/EAC-Beauftragten erfolgt die Zuordnung eines neuen Terminals, welches in der Lage ist CV-Zertifikate abzurufen (Bundesdruckerei Stammdatenpflege). Änderungen werden direkt an die Bundesdruckerei adressiert (Bundesdruckerei Stammdatenpflege).

Nach initialer erfolgreicher Registrierung werden CSRs über automatisierte Prozesse akzeptiert (Vergleiche Abschnitt 3.2.1).

Die Bearbeitung einer Registrierung erfolgt innerhalb von 3 Werktagen, sofern alle erforderlichen Informationen vorliegen.

3.2.3 Identifizierung und Authentifizierung von Terminals

Nicht-hoheitlicher DV (BerCA)

Nur Diensteanbieter mit einem gültigen Berechtigungszertifikat vom VfB (Vergabestelle für Berechtigungszertifikate) gemäß §21, §21a oder §21b [PAuswG] sind berechtigt nicht-hoheitliche Terminals zu betreiben.

Hoheitlicher DV (HDV)

Nur zur Identitätsfeststellung berechtige Behörden wie Ausweis- und Kontrollbehörden gemäß §36 (1) [PAuswV] und §20a [PAuswG]) sind berechtigt hoheitliche Terminals zu betreiben.

Zur Registrierung von sowohl hoheitlichen als auch von nicht-hoheitlichen Terminals werden die Vorgaben aus Kapitel 3.2.3 „Registrierung von Terminals" der [CP CVCA-eID] eingehalten.

3.2.4 Identifizierung und Authentifizierung natürlicher Personen

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

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

3.3.1 Routinemäßige Anträge zur Schlüsselerneuerung

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 DVCA zugewiesenen Inhalt nach dem Abschnitt 3.1.1 Arten von Namen.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Es gilt der Kapitel 5.2 der [CP CVCA-eID].

4. Betriebsanforderungen

4.1 Zertifikatsantrag und Registrierung

4.1.1 Berechtigung zur Antragstellung

Nicht-hoheitlicher DV (BerCA)

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

Die BerCA führt mit dem Diensteanbieter respektive dessen eID-Service Provider einen Test zur Ausstellung von Berechtigungszertifikaten (Test-Terminalberechtigungszertifikate) auf Basis von Testschlüsseln gemäß [Anhang C.2 „Certificate Requests" in [TR-03110] -Part 3: Common Specifications] durch.

Voraussetzung für den Beginn des Testverfahrens ist das Durchlaufen des Identifizierungsprozesses nach Abschnitt 3.2.2 „Identifizierung und Authentifizierung von Organisationen" durch den Diensteanbieter respektive dessen eID-Service Provider.

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

Hoheitlicher DV (HDV)

Die Berechtigung des Terminalbetreibers zum Betrieb eines hoheitlichen Terminals ist gemäß §36 (2) [PAuswV] und §20a [PAuswG] geregelt – Zitat:

„Das Bundesministerium des Innern, für Bau und Heimat bestimmt, welche Stellen hoheitliche Berechtigungszertifikate an welche zur Identitätsfeststellung berechtigten Behörden ausgeben dürfen, und veröffentlicht dies im Bundesanzeiger."

Voraussetzung für die Einrichtung einer neuen Instanz ist das Durchlaufen des Identifizierungsprozesses nach Abschnitt 3.2.2 „Identifizierung und Authentifizierung von Organisationen" durch die jeweilige berechtigte Behörde.

4.1.2 Registrierungsprozess und Zuständigkeiten

Die Registrierungsinformationen über den Terminalbetreiber werden im Registrierungsverzeichnis des DV vor dem Ausstellen des initialen Zertifikats erfasst.

Die Einhaltung des Registrierungsprozesses entsprechend der Abschnitte 3.2 „Initiale Überprüfung der Identität", 3.3 „Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying)" und 4.1.1 „Berechtigung zur Antragstellung", die Übermittlung der Berechtigungszertifikate an die Teilnehmer sowie deren Archivierung gemäß Abschnitt 6.3.1 „Archivierung öffentlicher Schlüssel" werden gewährleistet.

Für nicht hoheitliche CV-Zertifikate aus der BerCA erfolgt eine Prüfung der URL des Kunden als auch des zugehörigen TLS-Zertifikates. Die URL ist im Subject des CV-Zertifikats enthalten. Das

verwendete TLS-Zertifikat wird durch den Kunden an den DV D-Trust übergeben, um notwendige Prüfungen gemäß [CP CVCA-eID] Kapitel 4.1.1.2.1 durchzuführen.

Der Diensteanbieter/eID-Service Provider (nicht-hoheitlicher DV) verantwortet:

- die Generierung von Terminal-Schlüsselpaaren mit Hilfe des sicheren Kryptographie-moduls,
- die Durchführung der in Kapitel 3 aufgeführten Identifizierungs- und Authentifizierungsprozeduren,
- die Prüfung von erhaltenen Terminalberechtigungszertifikaten beziehungsweise der überlassenen Berechtigungen auf Korrektheit.

Die berechtigte Behörde (hoheitlicherDV) verantwortet

- die Erzeugung von Terminal-Schlüsselpaaren mit Hilfe des sicheren Kryptographie-moduls in den standortgebundenen Terminals (Operatorkarte & Pin)
- Beachtung der Einsatzbedingungen und Regelungen für den Schutz der Operatorkarte und Pin
- die Durchführung der in Kapitel 3 aufgeführten Identifizierungs- und Authentifizierungsprozeduren.

Beachte dazu auch Kapitel 3.2.3 „Registrierung von Terminals" der [CP CVCA-eID].

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Die Identifizierung der Terminals erfolgt nach Kapitel 3.2.3 der [CP CVCA-eID]. Für eIDAS-Mitgliedsstaaten ist die Identifizierung im [Annex CP CVCA-eID] geregelt.

Die verwendete CA ist für den Anwendungsfall der Erstellung von Berechtigungszertifikaten entwickelt worden und basiert auf dem Verfahren der kontinuierlichen „Neu-Ausstellung" von erforderlichen Zertifikaten für einen definierten Zeitraum. Nach der initialen Registrierung ist dies ein automatisiertes Verfahren. Zertifikate werden erstellt und sind nach dessen Erstellung im eID-Service und bei hoheitlichen Terminals sofort nutzbar. Dafür sendet entweder das hoheitliche Terminal oder der eID-Service Provider einen CSR an die Berechtigungs-CA und erhält das Zertifikat zurück. Die Prüfung der äußeren Signatur des CSR erfolgt auf Basis des vorherigen noch gültigen Zertifikats. Eine Zertifizierung des im CSR enthaltenen öffentlichen Schlüssels erfolgt ausschließlich bei erfolgreicher Prüfung der äußeren Signatur und der Eignung der kryptographischen Parameter des im CSR enthaltenen öffentlichen Schlüssels.

Für hoheitliche Terminals gilt zusätzlich: Für die Inbetriebnahme eines Terminals ist durch den Anwender eine Operatorkarte zu stecken bzw. aufzulegen und eine Pin einzugeben. Diese Interaktion ist immer notwendig, wenn das CV-Zertifikat abgelaufen ist und das Terminal länger als 48h nicht verwendet wurde bzw. das Terminal vom Stromnetz abgekoppelt war.

MDS-Zertifikate werden für Diensteanbieter ausgestellt, die über einen VfB-Bescheid verfügen. Diese senden einen Request im PKCS#10 Format an das Funktionspostfach der BerCA.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Zur Registrierung eines Terminalbetreibers hält sich der DV an seine Pflichten aus Kapitel 3.2.3.4 der [CP CVCA-eID].

Die Beantragung und Ausstellung eines initialen Zertifikats erfolgt gemäß Kapitel 4.4 der [CP CVCA-eID].

Führt der initiale Zertifikats-Request zu einem negativen Ergebnis, weil dafür kein gültiges Zertifikat (d.h. vorhergehendes CV-Zertifikat) vorliegt, mit dem der Antrag authentisiert werden kann (z.B. weil der Schlüsselspeicher defekt ist), klärt der DV die Ursache für den Fehler und behebt diesen, wenn dieser in seinem Zuständigkeitsbereich liegt. Der DV informiert den Antragsteller/ Zertifikatsnehmer über das Ergebnis seiner Fehleranalyse und fordert einen neuen Zertifikats-Request an. Anschließend werden die Registrierungsinformationen erneut ausgetauscht und geprüft bis ein positives Ergebnis erzielt wird.

Beim Importieren eines Berechtigungszertifikates ruft der eID-Server beim DVCA die gültige Zertifikatskette ab und prüft das erhaltene Berechtigungszertifikat gegen die gültige Zertifikatskette auf Korrektheit und importiert dieses nach positiver Prüfung in sein Zertifikatsverwaltungssystem.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Für alle Zertifikatsanträge mit äußerer Signatur (RequestSignerzertifikat oder Folgeantrag) erfolgt die Bearbeitung unverzüglich. Für alle initialen Anträge ohne äußere Signatur gilt die maximale Bearbeitungszeit von 3 Werktagen gemäß [CP CVCA-eID] Kapitel 4.4.1.2.

4.3 Ausstellung von Zertifikaten

4.3.1 Vorgehen des DV bei der Ausstellung von Zertifikaten

Die Ausstellung von Zertifikaten folgt den Vorgaben aus der [CP CVCA-eID] Kapitel 4.4.

Die vollständige Antragsdokumentation wird vom DV abgelegt. Die Antragsunterlagen und/oder Requests werden sicher und vollständig bis zum Ablauf der Frist nach Abschnitt 0 verwahrt.

Für Zertifikatsanträge aus eIDAS-Mitgliedsstaaten ist der Ablauf im [Annex CP CVCA-eID] geregelt.

4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausstellung des Zertifikats

Es erfolgt keine gesonderte Benachrichtigung des Zertifikatsnehmers nach der Fertigstellung des Zertifikats.

4.4 Zertifikatsübergabe

4.4.1 Verhalten bei der Zertifikatsübergabe

Nach Einrichtung des Terminals (hoheitlich) oder der Berechtigung für einen Diensteanbieter (BerCA) kann nach erfolgreicher Authentifikation ein Zertifikats-Request über die mit TLS gesicherte Verbindung an die DVCA gesendet werden. Die DVCA übergibt über diese gesicherte Verbindung das Berechtigungszertifikat an das Terminal beziehungsweise an den eID-Service Provider oder bei eIDAS-Mitgliedsstaaten an die Middleware-Komponente im jeweiligen Mitgliedstaat.

Eine Abnahme durch den Kunden erfolgt nicht.

4.4.2 Veröffentlichung des Zertifikats durch den DV

Die Zertifikate werden nach der Produktion nicht veröffentlicht.

4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats

Weitere PKI Teilnehmer werden über die Ausstellung der Zertifikate nicht unterrichtet.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Zertifikatsnehmer und Endanwender dürfen ihre privaten Schlüssel ausschließlich für die Anwendungen nutzen, die in Übereinstimmung mit den im Zertifikat angegebenen Nutzungsarten stehen.

Nach Ablauf des Gültigkeitszeitraums oder nach Sperrung des Zertifikats dürfen die zugehörigen privaten Schlüssel nicht mehr genutzt werden.

Für Zertifikatsnehmer gelten die Bestimmungen aus Abschnitt 1.4.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Öffentliche Schlüssel von Zertifikatsnehmern werden ausschließlich innerhalb des Verbunds im Zuge der Authentifizierung verwendet. Es findet keine Publikation in öffentlichen Verzeichnissen statt.

4.6 Zertifikatserneuerung

Es gelten die Anforderungen aus Abschnitt 4.7.

4.7 Zertifikatserneuerung mit Schlüsselerneuerung

Eine Zertifikatserneuerung ist die erneute Ausstellung eines Zertifikats, das auf den Inhaltsdaten des ursprünglichen Zertifikats beruht. Für die erneuerten Zertifikate gilt die zum Zeitpunkt der Erneuerung aktuelle [CP CVCA-eID] und die aktuelle CPS der D-Trust CVCA-eID PKI. Die Erneuerung folgt den Vorgaben aus der [CP CVCA-eID] bzw. dem [Annex CP CVCA-eID].

Die DVCA basiert auf dem Verfahren der kontinuierlichen „Neu-Ausstellung" von erforderlichen Zertifikaten für einen definierten Zeitraum. Zertifikate werden erstellt und sind nach dessen Erstellung im eID-Service und bei hoheitlichen Terminals sofort nutzbar. Dafür sendet entweder das hoheitliche Terminal oder der eID-Service Provider einen CSR an die Berechtigungs-CA und erhält das Zertifikat zurück. Die äußere Signatur des CSR erfolgt auf Basis des vorherigen noch gültigen Zertifikats. Die Schlüsselverwaltung obliegt dem Terminal beziehungsweise dem eID-Service Provider.

Für CA-Schlüssel der DVCA erfolgt gemäß Kapitel 4.7 der [CP CVCA-eID] alle 90 Tage oder kürzer eine Erneuerung.

Für die neuen Zertifikats-Request werden jeweils neue Schlüssel in einem HSM in einer gesicherten Umgebung erstellt. Auf Basis dieses CSR erfolgt die Ausstellung eines neuen SubCA-Zertifikates durch die CVCA des BSI.

4.7.1 Bedingungen für eine Zertifikatserneuerung

Haben sich grundsätzliche Änderungen an den Nutzungsbedingungen ergeben, wird der Zertifikatsnehmer darüber informiert. Der Zertifikatsnehmer bestätigt die neuen Bedingungen.

Bei einem Antrag auf Zertifikatserneuerung kann – im Gegensatz zu einem neuen Antrag auf ein Zertifikat – der Vorgang der initialen Identifizierung entfallen.

Voraussetzung ist, dass das Zertifikat für denselben Endanwender ausgestellt wird. Das zu erneuernde Zertifikat muss zum Zeitpunkt der elektronischen Antragstellung auf Zertifikatserneuerung noch gültig sein oder geprüfte Daten und Nachweise sind für die Erneuerung vorhanden und verwendbar. Zusätzlich wird ein Zertifikat erneuert, wenn die Zugriffsrechte geändert werden sollen oder der Gültigkeitszeitraum endet

Ein Zertifikats-Request für eine Zertifikatserneuerung wird abgelehnt, wenn der Antragsteller gesperrt ist bzw. der Request mit einem ungültigen Schlüssel signiert ist. Eine Zertifikatserneuerung erfolgt ausschließlich nach erfolgreicher Prüfung der äußeren Signatur und weiterer Prüfungen der kryptographischen Eigenschaften des zu zertifizierenden Schlüssels.

Eine Erneuerung von MDS-Zertifikaten und CV-Zertifikaten ist in Abschnitt 4.2.1 beschrieben. Ein Zertifikats-Request kann nur mit einem neuen Schlüsselpaar erzeugt werden. Bei CV-Zertifikaten verwendet der eID-Server automatisiert ein neues Schlüsselpaar zur Generierung eines neuen Zertifikats-Requests.

4.7.2 Berechtigung zur Zertifikatserneuerung

Jeder Zertifikatsnehmer, der (nach Abschnitt 4.1.1) berechtigt ist, einen Zertifikatsantrag zu stellen, kann eine Zertifikatserneuerung beantragen.

4.7.3 Bearbeitung eines Antrags auf Zertifikatserneuerung

Zertifikatsnehmer, die berechtigt sind, Anträge auf Zertifikatserneuerung zu stellen, nutzen eine produktspezifisch bereitgestellte Onlineschnittstelle des DV zur Antragstellung.

Über die entsprechenden Schnittstellen gestellte Anträge werden automatisiert auf Berechtigung und Inhalt geprüft.

4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Zertifikatsnehmer werden nicht benachrichtigt.

4.7.5 Verhalten bei der Ausgabe einer Zertifikatserneuerung

Das erzeugte Zertifikat wird über die bereitgestellte Online-Schnittstelle nach TR-03129 zur Verfügung gestellt. Weiterhin gelten die in Abschnitt 4.4.1 festgelegten anwendbaren Regelungen.

4.7.6 Veröffentlichung der Zertifikatserneuerung durch den DV

Es gelten die in Abschnitt 4.4.2 festgelegten Regelungen.

4.7.7 Benachrichtigung anderer PKI-Teilnehmer über die Erneuerung des Zertifikats

Keine Vorgaben.

4.8 Zertifikatsänderung

Zertifikatsänderungen werden nicht angeboten.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Bedingungen für eine Sperrung/Deaktivierung

Zertifikatsnehmer, betroffenen Dritte oder eine sonstige dritte Partei sind aufgefordert, die Sperrung/Deaktivierung des Terminals bzw. Diensteanbieters zu beantragen, wenn der Verdacht besteht, dass private Schlüssel kompromittiert wurden oder Inhaltsdaten des Zertifikats nicht mehr korrekt sind.

Das Sperren von Berechtigungszertifikaten ist aufgrund der kurzen Laufzeit von 48 Stunden nicht vorgesehen. Jedoch können hoheitliche Terminals und Diensteanbieter jederzeit deaktiviert werden und sind dann von der Nutzung des Berechtigungszertifikates ausgeschlossen.

Folglich werden, wenn Gründe für eine Sperrung/Deaktivierung vorliegen, keine neuen Berechtigungszertifikate mehr ausgestellt und das betroffene Terminal bzw. Diensteanbieter wird je nach Fall zeitweise oder wenn nötig komplett deaktiviert. Die Sperrung/Deaktivierung eines Terminals/Diensteanbieters wird bei folgenden Ereignissen durchgeführt:

- auf Verlangen des Zertifikatsnehmers bzw. betroffenen Dritten
- Ungültigkeit von Angaben/Berechtigungen im Zertifikat bzw. falsche Angaben zu den Metadaten
- unbefugter Zugriff auf sensible Daten wie z.B. privater Schlüssel, Registrierungseinträge und Registrierungsdaten sowie nicht-öffentliche Informationen über Infrastruktur, Konfiguration und Organisation des Gesamtsystems
- wenn der DV seine Tätigkeit beendet und diese nicht von einem anderen DV fortgeführt wird.
- bei Beendigung der Teilnahme an der CVCA-eID PKI
- wenn der Diensteanbieter den DV wechselt. Hier ist neben dem CV-Zertifikat auch ein vorhandenes MDS-Zertifikat zu sperren.
- bei ausgelagertem Betrieb des eID-Servers: Der Diensteanbieter wechselt den Betreiber seines eID-Servers. Hier ist ein vorhandenes MDS-Zertifikat zu sperren.
- Verlust oder Diebstahl eines Terminals

Unabhängig davon kann der DV Sperrungen veranlassen, wenn:

- der private Schlüssel der ausstellenden oder einer übergeordneten CA kompromittiert wurde,
- Schwächen in den verwendeten kryptographischen Algorithmen bekannt werden, die ernste Risiken für die erlaubten Anwendungen während der Zertifikatslaufzeit darstellen,
- die eingesetzte Hard- und Software Sicherheitsmängel aufweist, die ernste Risiken für die erlaubten Anwendungen während der Zertifikatslaufzeit darstellen,
- die eindeutige Zuordnung des Schlüsselpaars zum Zertifikatsnehmer nicht mehr gegeben ist,
- ein Zertifikat aufgrund falscher Angaben erwirkt oder anderweitig missbraucht wurde,
- der Kunde nach zweimaliger Mahnung mit dem Entgelt in Verzug ist bzw. gegen die anwendbare AGB verstoßen hat,
- das Vertragsverhältnis gekündigt oder in sonstiger Weise beendet wurde.
- Die VfB über einen erneuten Bescheid die Berechtigungen für einen Diensteanbieter entzieht.

4.9.2 Berechtigung zur Sperrung/Deaktivierung

Der DV ist sperrberechtigt.

Der Diensteanbieter hat stets die Berechtigung die Deaktivierung seiner Dienste zu beantragen. Die Deaktivierung wird bei berechtigter Beauftragung von der DV (BerCA) ausgeführt. Die VfB wird darüber informiert.

Die VfB ist berechtig eine Deaktivierung eines Diensteanbieters zu veranlassen.

Eine hoheitliche Behörde kann jederzeit die Deaktivierung eines Terminals ihres Standortes ausführen lassen. Diese Beauftragung übernimmt der EAC-Beauftragte. Die Deaktivierung wird von der Bundesdruckerei ausgeführt.

4.9.3 Verfahren für einen Sperrantrag

Das reguläre Sperren von Berechtigungszertifikaten ist aufgrund der kurzen Laufzeit von 48 Stunden nicht vorgesehen. Hoheitliche Terminals und Diensteanbieter können jederzeit deaktiviert werden. Ab diesem Zeitpunkt werden keine neuen Berechtigungszertifikate ausgestellt.

Hoheitliche Terminals deaktiviert der Service der BDr gemäß folgendem Ablauf:

- Meldung durch berechtigte Behörde (schriftlich oder über ein online Serviceportal)
- Prüfung der Sperrberechtigung durch Prüfung des Ansprechpartners
- Deaktivierung des Terminals im Serviceportal. Bei Verlust wird das Terminal zusätzlich ausgebucht und kann nicht mehr reaktiviert werden.
- Das CV-Zertifikat ist maximal noch 48 Stunden gültig. Daher verbleibt ein Terminal nach der Deaktivierung noch mindestens 48 Stunden in der Behörde bevor es zur BDR zurückgesandt wird.

Diensteanbieter werden von der BerCA gemäß folgendem Ablauf deaktiviert:

- Erhalt eines neuen VfB-Bescheids mit Entzug der Berechtigungen ODER Ablauf der Vertragslaufzeit
- Prüfung des Bescheids/Vertragslaufzeit
- Deaktivierung des Diensteanbieters in der BerCA (es wird kein neues CV-Zertifikat mehr ausgestellt)

4.9.4 Fristen für einen Sperrantrag

Die Sperrung/Deaktivierung erfolgt unverzüglich, sobald Gründe zur Sperrung bekannt werden. Dabei ist dasjenige Verfahren zu nutzen, welches die schnellste Bearbeitung des Sperrantrags erwarten lässt.

4.9.5 Zeitspanne für die Bearbeitung des Sperrantrags durch den DV

Die Sperrung/Deaktivierung erfolgt in den regulären Arbeitszeiten umgehend nach erfolgreicher Autorisierung des Sperrantragstellers.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Die erfolgreiche Deaktivierung kann im Service Center der Bundesdruckerei abgefragt bzw. online über das Kunden Serviceportal direkt nachgeschaut werden.

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Für CV-Zertifikate werden keine Sperrlisten erstellt. Siehe [CP CVCA-eID] Kapitel 5.2.1.

Sperrlisten werden nur für MDS-Zertifikate veröffentlicht. Die CRL wird täglich aktualisiert.

4.9.8 Maximale Latenzzeit für Sperrlisten

Sperrlisten für MDS-Zertifikate werden unmittelbar nach ihrer Erzeugung bereitgestellt. Ihre Veröffentlichung kann bis 60 Minuten dauern.

4.9.9 Online-Verfügbarkeit von Sperrinformationen

Die Sperrliste für MDS-Zertifikate wird unmittelbar nach dem Widerruf eines MDS-Zertifikats neu erstellt. Es kann bis zu 60 Minuten dauern bis diese öffentlich sichtbar ist.

4.9.10 Notwendigkeit zur Online-Prüfung von Sperrinformationen

Es gibt keine Pflicht zur Online-Prüfung von Sperrinformationen, es gilt jedoch Abschnitt 4.5.2.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Keine Vorgaben.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Keine Vorgaben.

4.9.13 Bedingungen für eine Suspendierung

Suspendierungen von Zertifikaten werden nicht angeboten.

4.10 Statusabfragedienst für Zertifikate

4.10.1 Funktionsweise des Statusabfragedienstes

Statusabfragedienste von Zertifikaten werden nicht angeboten.

4.10.2 Verfügbarkeit des Statusabfragedienstes

Keine Vorgaben.

4.10.3 Optionale Leistungen

Keine Vorgaben.

4.11 Austritt aus dem Zertifizierungsdienst

Die Gültigkeit eines Zertifikats endet mit dem im Zertifikat vermerkten Termin. Schlüsselerneuerung kann gemäß Abschnitt 3.3 beantragt werden. Die vertraglichen Hauptleistungspflichten des DV sind damit vollständig erfüllt.

Im Fall des bevorstehenden Ablaufs des VfB-Bescheids für einen Diensteanbieter informiert diesen die BerCA 2 Monate vor Ablauf des Bescheids per E-Mail.

4.12 Schlüsselhinterlegung und –wiederherstellung

Schlüsselhinterlegung wird nicht vom DV angeboten.

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel

Schlüsselhinterlegung wird nicht vom DV angeboten.

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Schlüsselhinterlegung wird nicht vom DV angeboten.

5. Nicht-technische Sicherheitsmaßnahmen

Der Inhalt dieses Kapitels bezieht sich auf die CAs, die bei der D-Trust GmbH im Rahmen von [TR-03145] betrieben werden. Die D-Trust GmbH betreibt ein zertifiziertes Informationssicherheits-managementsystem (ISMS) gemäß ISO/IEC 27001. Der Betrieb der CA unterliegt diesem ISMS. Eine Auslagerung von Tätigkeiten an externe Dienstleister findet im Anwendungsbereich nicht statt.

5.1 Bauliche Sicherheitsmaßnahmen

Für die baulichen Sicherheitsmaßnahmen liegt eine detaillierte Dokumentation vor, die bei berechtigtem Interesse in den relevanten Teilen eingesehen werden kann. Das Sicherheitskonzept wurde durch eine anerkannte Konformitätsbewertungsstelle geprüft.

Ferner wurde dem Sicherheitsbereich des Trustcenters der D-Trust GmbH durch den TÜV-IT die Anwendung und Umsetzung der „Infrastrukturmaßnahmen für hohen Schutzbedarf – Level 3" beurkundet (gemäß Prüfkriterienkatalog für „Trusted Site Infrastructure"). Mit diesem TÜV-IT-Zertifikat „Trusted Site Infrastructure" werden alle Infrastruktur-relevanten Aspekte bewertet. Diese Prüfung wird alle zwei Jahre wiederholt. Das genannte Zertifikat bestätigt der D-Trust GmbH diesen hohen Sicherheitsstandard dieser Sicherheitsmaßnahmen.

Die CAs der hier behandelten PKI werden vom DV unter den gleichen Bedingungen betrieben wie die CAs der D-Trust GmbH zur Ausstellung qualifizierter Zertifikate.

5.2 Verfahrensvorschriften

5.2.1 Rollenkonzept

Teil der Dokumentation ist ein Rollen- und Berechtigungskonzept, in dem Mitarbeiter einer oder mehrere Rollen durch das Management des DV (TSP) zugeordnet werden und entsprechende Berechtigungen durch einen gesteuerten Prozess erhalten. Die Berechtigungen der einzelnen Rollen beschränken sich auf diejenigen, die sie zur Erfüllung ihrer Aufgaben benötigen. Die Zuordnung der Berechtigungen wird regelmäßig durch das Sicherheitsmanagement revisioniert und umgehend nach Entfall des Bedarfs entzogen.

Rollen mit Sicherheitsverantwortung für den Betrieb des TSP, genannt „Trusted Roles", (mit unter anderem den Aufgaben des Sicherheitsbeauftragten, System Administrator, System Operator, System Auditor, Registration Officer, Revocation Officer und Validation Specialist) werden in den Berechtigungskonzepten der D-Trust festgelegt. Diese Rollen dürfen nur von fachkundigen und zuverlässigen Mitarbeitern übernommen werden. Mitarbeiter, die diese Rolle erhalten, werden gesondert unterwiesen und müssen die Übernahme der Rolle aktiv bestätigen.

Für die jeweiligen Rollen werden Stellenbeschreibungen erstellt. Diese legen die Aufgaben, das geforderte Mindestmaß an Qualifikation und Erfahrungen für die jeweilige Rolle fest. Ein Mitarbeiter, kann eine bzw. mehrere Rollen ausfüllen, vorausgesetzt die Rollen schließen sich nicht gegenseitig aus. Zusätzlich muss ein Mitarbeiter nachweisen, dass er die nötige Qualifikation und Erfahrung für diese Rolle erworben hat.

Mitarbeiter werden regelmäßig geschult, um ihre Rollen und damit verbundenen Verantwortlichkeiten zu erfüllen. Vom Informationssicherheitsmanagement regelmäßig veranlasste Sensibilisierungsmaßnahmen unterstützen die Einhaltung geltender Sicherheitsvorgaben. Mitarbeiter können sich im Rahmen von Schulungen die Qualifikation für weitere Rollen erwerben.

Die Anforderungen an die Rollen werden in Stellenbeschreibungen dokumentiert und können von den Mitarbeitern jederzeit eingesehen werden.

Im Falle von sich ausschließenden Rollen, kann ein Mitarbeiter nur eine dieser Rollen übernehmen (Vier-Augen-Prinzip). Eine Risikobewertung findet regelmäßig statt.

Mitarbeiter, die im Bereich der Zertifizierungs- und Sperrdienste tätig sind, agieren unabhängig und sind frei von kommerziellen und finanziellen Zwängen, die ihre Entscheidungen und Handlungen beeinflussen könnten. Die organisatorische Struktur des TSP berücksichtigt und unterstützt die Mitarbeiter in der Unabhängigkeit ihrer Entscheidungen.

5.2.2 Mehraugenprinzip

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.

Sicherheitskritische Systeme zur Zertifikatsausstellung sind zusätzlich durch eine Multi-Faktor-Authentisierung geschützt.

5.2.3 Identifikation und Authentifizierung für einzelne Rollen

Das Rollenkonzept wird durch technische und organisatorische Maßnahmen, wie beispielsweise Zutrittsberechtigungen und Abfrage von Wissen, durchgesetzt. Die durchführende Person muss sich, bevor sie Zugriff auf sicherheitskritische Anwendungen erhält, erfolgreich authentifizieren. Über Event-Logs kann die durchführende Person nachträglich einer Aktion zugeordnet werden; sie ist rechenschaftspflichtig.

5.2.4 Rollenausschlüsse

Das Rollenkonzept sieht diverse Rollenausschlüsse vor, um Interessenskonflikte zu verhindern, das Mehraugenprinzip zu erzwingen und schädliches Handeln vorzubeugen.

5.3 Eingesetztes Personal

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

Der DV gewährleistet, dass die im Bereich des Zertifizierungsdienstes tätigen Personen über die für diese Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen.

Die Identität, Zuverlässigkeit und Fachkunde des Personals wird vor Aufnahme der Tätigkeit überprüft.

5.3.2 Sicherheitsprüfungen

Personen, die in sicherheitsrelevanten Bereichen des DV tätig sind, müssen unter anderem regelmäßig polizeiliche Führungszeugnisse vorlegen.

Übergreifend betreibt der DV ein nach ISO 27001 zertifiziertes ISMS. Im Rahmen der angewandten Personalverfahren werden den Mitarbeitern entsprechend sicherheitsrelevante Vorgaben bzw. Verhaltensregeln zugänglich gemacht.

5.3.3 Schulungen

Der DV schult Personen, die im Zertifizierungsdienst tätig sind.

Regelmäßige und anlassbezogene Schulungen gewährleisten die Kompetenz in den Tätigkeitsbereichen sowie die allgemeine Informationssicherheit.

Schulungen und Leistungsnachweise werden dokumentiert.

5.3.4 Häufigkeit von Schulungen und Belehrungen

Der DV schult Personen, die im Zertifizierungsdienst tätig sind zu Beginn ihres Einsatzes und bei Bedarf.

5.3.5 Häufigkeit und Folge von Job-Rotation

Rollenwechsel werden dokumentiert. Die entsprechenden Mitarbeiter werden geschult.

5.3.6 Maßnahmen bei unerlaubten Handlungen

Der DV schließt unzuverlässige Mitarbeiter von den Tätigkeiten im Zertifizierungsdienst aus.

5.3.7 Anforderungen an freie Mitarbeiter

Entfällt; freie Mitarbeiter werden nicht eingesetzt.

5.3.8 Ausgehändigte Dokumentation

Umfangreiche Verfahrensanweisungen definieren für alle Produktionsschritte die zuständigen Mitarbeiterrollen und -rechte sowie entsprechende manuelle und maschinelle Prüfungen. Durch die sicherheitstechnische Infrastruktur der D-Trust GmbH ist gewährleistet, dass von diesen definierten Verfahren im Produktionsbetrieb nicht abgewichen werden kann.

5.4 Überwachungsmaßnahmen

5.4.1 Überwachung des Zutritts

Der DV betreibt umfangreiche Überwachungsmaßnahmen (beispielsweise durch Videoüberwachung) zur Absicherung der Zertifizierungsdienstleistungen und deren zugrundeliegenden IT-Systemen und Dokumenten.

Die Überwachungsmaßnahmen werden durch organisatorische Regelungen ergänzt. Beispielsweise sieht die Besucherregelung unter anderem vor, dass Besucher mindestens 24 Stunden vor dem Besuch namentlich angemeldet sein müssen. Im Bereich des Trustcenters müssen Besucher stets in Begleitung eines Mitarbeiters des DV sein.

5.4.2 Überwachung von organisatorischen Maßnahmen

Ein weiterer Bestandteil ist die Überwachung von organisatorischen Maßnahmen.

Hierzu gehört eine regelmäßige Risikoanalyse, die die Bedrohung für den Betrieb des DV umfassend analysiert sowie Anforderungen und Gegenmaßnahmen definiert. Ferner ist eine Bewertung des Restrisikos enthalten, in der die Vertretbarkeit des Restrisikos aufgezeigt und ggf. akzeptiert wird.

Weiterhin werden relevante Assets angemessen erfasst, sowie entsprechende Änderungen dieser Assets überprüft bzw. wenn anwendbar durch das vom Management beauftragte Personal des DV freigegeben.

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen

Es wird zwischen Aufzeichnungen in elektronischer Form und papierbasierten unterschieden.

Archiviert werden die vollständigen Antragsunterlagen, Bescheide, Dokumente zu Verfahrensrichtlinien (CP, CPS), Zertifikate, Sperrdokumentation, elektronische Dateien und Protokolle zum Zertifikatslebenszyklus. Dabei werden die Vorgänge zeitlich erfasst. Wenn anwendbar, umfasst dies auch die entsprechenden Systemprotokolle, die im Rahmen der genannten Ereignisse entstehen.

Weiterhin werden sicherheitsrelevante Ereignisse entsprechend aufgezeichnet. Die Systemzeit wird täglich mit dem deutschen DCF77-Zeitsignal und verlässlichen Zeitservern (NTP) im Internet synchronisiert.

5.5.2 Aufbewahrungsfristen für archivierte Daten

Dokumente zur Antragstellung und Prüfung werden mindestens zehn Jahre und bis zum Jahresende aufbewahrt. Für Zertifikate werden die Aufbewahrungsfristen entsprechend Kapitel 2.1 der [CP CVCA-eID] eingehalten.

Event-Logs der IT-Systeme werden mindestens 6 Monate gespeichert. Die Speicherdauer von personenbezogenen Videoaufzeichnungen und Aufzeichnungen der administrativen Tätigkeiten beträgt 90 Tage.

Für das Archivierungssystem wird die Systemzeit täglich mit dem deutschen DCF77-Zeitsignal und verlässlichen Zeitservern (NTP) im Internet synchronisiert.

5.5.3 Sicherung des Archivs

Die Systeme auf denen die Archivierung erfolgt, befinden sich in gesicherten Räumen und unterliegen dem Rollen- und Zutrittskontrollkonzept des DVs.

5.5.4 Datensicherung des Archivs

Vertraulichkeit und Integrität der Daten werden gewahrt. Die Ablage der Dokumentation erfolgt unverzüglich, so dass sie nachträglich nicht unbemerkt verändert werden kann. Die europäischen und deutschen Datenschutzanforderungen werden eingehalten.

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

Keine Vorgaben.

5.5.6 Archivierung (intern / extern)

Die Archivierung erfolgt ausschließlich intern beim DV.

5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen

Das Verfahren zur Beschaffung und Verifikation von Archivinformationen unterliegt dem Rollenkonzept des DV.

5.6 Schlüsselwechsel beim DV

Alle 90 Tage oder kürzer werden neue CA-Schlüssel generiert, um mittels eines Zertifikats-Requests neue DV Zertifikate bei der RootCA vom Bundesamt für Sicherheit in der Informationstechnik anzufordern. Nach Erhalt der DV Zertifikate wird die SubCA in Betrieb genommen. Die in diesem Kontext durchgeführten Tätigkeiten erfolgen im Vier-Augen-Prinzip.

5.7 Kompromittierung und Geschäftsweiterführung beim DV

5.7.1 Behandlung von Vorfällen und Kompromittierungen

Der DV verfügt gemäß Kapitel 5.2 [CP CVCA-eID] über ein Notfallkonzept sowie einen Wiederanlaufplan, die den beteiligten Rollen bekannt sind und von ihnen im Bedarfsfall umgesetzt werden. Die Verantwortlichkeiten sind klar verteilt und bekannt.

Sollte eine Systemwiederherstellung erforderlich sein, sind die Verantwortlichkeiten und entsprechenden „Trusted Roles" im Berechtigungskonzept der D-Trust deklariert und den jeweiligen Mitarbeitern bekannt. Siehe Abschnitt 5.2.1.

5.7.2 Wiederherstellung nach Kompromittierung von Ressourcen

Das Sicherheitskonzept beschreibt die Durchführung von Recovery-Prozeduren.

Die Recovery-Prozeduren für die Wiederherstellung der Betriebsfähigkeit des TSP sind definiert. Es erfolgt ein tägliches Backup und ein Backup nach Veränderungen. Backups werden in einem anderen Brandabschnitt aufbewahrt. Die Wiederherstellungen von kritischen CA-Systemen werden im Rahmen von Notfallübungen regelmäßig getestet.

5.7.3 Kompromittierung des privaten CA-Schlüssels

Im Fall einer Kompromittierung oder der Bekanntgabe von Unsicherheit von Algorithmen oder assoziierten Parametern, veranlasst der DV folgendes:

- Information der CVCA und des VfB als auch involvierte Zertifikatsnehmer werden über den Vorfall und dessen Auswirkungen informiert.
- Außerbetriebnahme der betroffenen SubCA.
- Es wird mit neuen Schlüsseln eine neue Sub-CA beantragt und in Betrieb genommen.
- Diensteanbieter müssen ebenfalls mit neuen initialen Zertifikats-Requests neue Zertifikate beantragen.

Aus der Analyse der Gründe für die Kompromittierung werden, wenn möglich, Maßnahmen ergriffen, um zukünftige Kompromittierungen zu vermeiden. Unter Berücksichtigung der Gründe für die Kompromittierung werden neue CA-Signaturschlüssel generiert und neue CA-Zertifikate ausgestellt.

5.7.4 Möglichkeiten zur Geschäftsweiterführung nach Kompromittierung und Desaster

In einem Notfall entscheidet der DV je nach Art des Vorfalls, ob ein Recovery des in Abschnitt 6.2.3 beschriebene Backups der CA durchgeführt oder bei Kompromittierung gemäß Abschnitt 0 verfahren wird.

5.8 Schließung des DV

Bei Beendigung der Dienste von CAs informiert der DV alle Zertifikatsnehmer und die CVCA-eID und beendet alle Zugriffsmöglichkeiten von Unterauftragnehmern des DV in Bezug auf die betroffenen CAs. Alle noch gültigen und von den betroffenen CAs ausgestellten Zertifikate werden gesperrt. Betroffene private CA-Schlüssel werden zerstört. Die Anforderungen zur Schließung des DV sind in Kapitel 5.4 [CP CVCA-eID] geregelt.

Im Fall einer geplanten Betriebseinstellung informiert der DV alle Endanwender, Zertifikatsnehmer und Dritte vorab mit einer Frist von 6 Monaten.

Die Dokumente zur Antragstellung werden an die Bundesdruckerei GmbH übergeben und unter äquivalenten Bedingungen weitergeführt.

Der DV unterstützt eine Migration auf eine andere BerCA. Eine Migration der in den nicht hoheitlichen Zertifikaten genutzten Terminal Sektoren wird nach den in der [CP CVCA-eID] Kapitel 4.1.1.2.3 unterstützt.

Mit Beendigung des Betriebes werden alle Funktionalitäten der CAs eingestellt.

Die D-Trust GmbH verfügt über einen fortlaufend aktualisierten Beendigungsplan.

6. Technische Sicherheitsmaßnahmen

Die Beschreibungen dieses Kapitels beziehen sich auf die PKI-Dienste, die in diesem CPS behandelt werden und bei der D-Trust GmbH betrieben werden.

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

Die Anforderungen an die Speicherung von CA-Schlüsseln sind in Kapitel 6.1 und 6.2 [CP CVCA-eID] definiert. Für die DVCA der D-Trust werden HSMs vom Modell Utimaco CP5 eingesetzt, die gemäß EAL4+ nach dem Schutzprofil (Protection Profile) prEN 419 221-5 entsprechend den Anforderungen nach Sicherheitslevel 2 CC zertifiziert sind.

CA-Schlüssel werden in einem CC-evaluierten Hardware Security Module (HSM) Utimaco CP5 erzeugt. Das HSM befindet sich im Hochsicherheitsbereich des Trustcenters. Bei der Schlüsselerzeugung wird die Durchsetzung des Rollenkonzepts und somit das Vier-Augen-Prinzip organisatorisch sichergestellt. Jeder Zertifikats-Request wird mit einem neuen Schlüsselpaar erzeugt. Nach der Erzeugung von neuen Schlüsselpaaren für einen geltenden Anwendungsbereich werden die alten Schlüssel gelöscht.

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Private Schlüssel für die Berechtigungszertifikate werden beim Zertifikatsnehmer erzeugt. Eine Lieferung privater Schlüssel entfällt. Jeder Zertifikats-Request muss mit einem neuen Schlüsselpaar erzeugt werden.

Die Schlüssel für die DV-Zertifikate werden durch die DVCA erzeugt.

Der private Schlüssel zum „Sector Public Key" werden sicher gespeichert und dem Dienstenabieter nicht bekanntgegeben.

6.1.3 Lieferung öffentlicher Schlüssel an den DV

Im hoheitlichen Anwendungsfall wird ein Zertifikats-Request vom Terminal über eine Operator-Karte an die DVCA gestellt. Der initiale Zertifikats-Request wird von einem im Terminal enthaltenen Security Authentication Module signiert. Jeder Folgerequest erhält eine äußere Signatur mit dem Vorgängerzertifikat.

Im nicht-hoheitlichen Anwendungsfall wird ein Zertifikats-Request vom eID-Server im Auftrag des Diensteanbieters an die DVCA gestellt. Der initiale Zertifikats-Request des Diensteanbieters wird nur in einem kurzen Zeitraum akzeptiert. Jeder Folgerequest erhält eine äußere Signatur mit dem Vorgängerzertifikat.

Für MDS-Zertifikate muss ein Request im PKCS#10-Format an den DV übermittelt werden. Es erfolgt die Prüfung der fehlerfreien Übertragung über einen Abgleich des Hashwertes.

Die entsprechende Response gibt das vollständige Zertifikat zurück.

Weitere Details der Verfahren sind im Kapitel 4.4.2 der [CP CVCA-eID] definiert.

6.1.4 Schlüssellängen

Für CV-Zertifikate werden derzeit Schlüssel aus der Kurve „Brainpool P256r1" und für MDS-Zertifikate aus der Kurve „NIST Kurven secp256r1" verwendet.

6.1.5 Festlegung der Schlüsselparameter und Qualitätskontrolle

Signatur- und Verschlüsselungsalgorithmus sind in TR-03110 definiert.

6.1.6 Schlüsselverwendungen

Die Schlüsselverwendung ist im Kapitel 1.4 definiert.

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

Während des gesamten Lebenszyklus (einschließlich Lieferung und Lagerung) werden die Module durch technische und organisatorische Maßnahmen vor unbefugter Manipulation geschützt.

Werden die privaten Schlüssel für die Berechtigungszertifikate im Verantwortungsbereich des Zertifikatsnehmers erstellt, so hat dieser ebenfalls dafür zu sorgen, dass eine ausreichende Qualität bei der Schlüsselerzeugung gewährleistet ist (siehe Kapitel 4.6 [CP CVCA-eID].

6.2.2 Zugriffssicherung zu privaten Schlüsseln

Das HSM, auf dem die CA-Schlüssel aufbewahrt werden, befindet sich in der sicheren Umgebung des Trustcenters. Die privaten CA-Schlüssel können nur im Vier-Augen-Prinzip und von den zuständigen Rollen und für die zulässigen Nutzungsarten verwendet werden.

6.2.3 Backup privater Schlüssel

Es ist ein Backup der privaten CA-Schlüssel vorhanden. Ein CA-Schlüssel-Backup erfordert für diese Tätigkeit am HSM zwei autorisierte Personen und findet in der sicheren Umgebung des Trustcenters statt. Für das Backupsystem gelten die gleichen Voraussetzungen und Sicherungsmaßnahmen wie für das Produktivsystem. Eine Wiederherstellung privater Schlüssel erfordert ebenfalls zwei autorisierte Personen. Eine Kopie der privaten CA-Schlüssel wird auf einem verschlüsselten Datencontainer im Safe aufbewahrt. Dabei werden die Anforderungen aus Kapitel 6.2 [CP CVCA-eID] eingehalten.

6.2.4 Archivierung privater Schlüssel

Private Schlüssel werden nicht archiviert.

6.2.5 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Ein Transfer privater CA-Schlüssel in oder aus dem HSM erfolgt nur zu Backup- und Wiederherstellungszwecken. Ein Vier-Augen-Prinzip wird organisatorisch sichergestellt. Beim Export/Import des Schlüsselmaterials in ein anderes HSM schützt ein Transportschlüssel den privaten CA-Schlüssel.

6.2.6 Speicherung privater Schlüssel in kryptographischen Modulen

Die privaten CA-Schlüssel liegen verschlüsselt im HSM vor.

6.2.7 Zerstörung privater Schlüssel

Nach Beendigung der Verwendung der privaten CA-Schlüssel zum Zweck der Zertifizierung werden diese gelöscht. Dies erfolgt durch Löschen auf dem HSM und gleichzeitigem Löschen der auf Datenträgern angelegten Backups. Bei Stilllegung des HSMs werden die privaten Schlüssel auf dem Gerät gelöscht.

6.2.8 Beurteilung kryptographischer Module

Der DV betreibt geeignete hard- und softwarebasierte Schlüsselgeneratoren um die Qualität der Schlüssel zu sichern. Die Hardware-Sicherheitsmodule (HSM) werden speziell für Anwendungen wie z. B. das Identitätsmanagement und die Ausgabe und Verwaltung von eID-Dokumenten eingesetzt. Das HSM ist nach EAL4+ gemäß Schutzprofil (Protection Profile) prEN 419 221-5 CC-evaluiert. Diese werden als geeignet bewertet.

Die Anforderungen an Zufallszahlen sind ebenfalls aus dem Key-Life-Cycle gemäß Kapitel 6 [CP CVCA-eID] zu entnehmen.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel werden in Form der erstellten Zertifikate archiviert.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die Gültigkeitsdauer der CA-Schlüssel und Zertifikate sind in Kapitel 4.7 [CP CVCA-eID] definiert und werden entsprechend umgesetzt.

6.4 Sicherheitsmaßnahmen in den Rechneranlagen

6.4.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Die vom DV eingesetzten Computer, Netze und andere Komponenten stellen in der eingesetzten Konfiguration sicher, dass nur Aktionen durchgeführt werden können, die nicht im Widerspruch zum CPS und [TR-03145-1] bzw. [TR-03145-4] stehen.

Die Computersicherheit des DV wird für exponierte Systeme u.a. durch mehrstufige Sicherheitssysteme zum Zwecke des perimetrischen Virenschutzes, Endpoint-Protection und integritätssichernde Werkzeuge sichergestellt.

Es wird sichergestellt, dass sicherheitsrelevante Softwareupdates in angemessener Zeit auf den relevanten Systemen installiert werden. Abweichungen hiervon werden vom DV angemessen dokumentiert und ggf. im Risikomanagement des DV adressiert.

Zertifikatsnehmer und Zertifikatsnutzer müssen vertrauenswürdige Computer und Software verwenden.

6.4.2 Beurteilung von Computersicherheit

Die für die CA-Schlüssel eingesetzten Computer, Netze und andere Komponenten wurden durch anerkannte Prüf- und Bestätigungsstellen regelmäßig geprüft und unterliegen einem entsprechenden Monitoring.

6.4.3 Monitoring

Zur Sicherstellung der Verfügbarkeit erfolgt ein kontinuierliches Monitoring der relevanten Systeme. Jede Störung wird erfasst, dokumentiert und gemäß ihrer Auswirkung mit einem Schweregrad gekennzeichnet und daraufhin priorisiert. Die Behandlung von kritischen Meldungen erfolgt im Rahmen des Prozesses Incident Management. Meldungen zu sicherheitsrelevanten Ereignissen werden an eine zentrale Stelle übermittelt und gemäß Kritikalität ausgewertet.

Bei Störungen mit Verfügbarkeitsverlust eines Services werden die betroffenen Parteien mindestens alle 24 Stunden über den aktuellen Status zur Störungsbeseitigung informiert.

6.5 Technische Maßnahmen während des Life Cycles

6.5.1 Sicherheitsmaßnahmen bei der Entwicklung

Bei der Entwicklung aller vom DV oder im Auftrag des DVs durchgeführter Systementwicklungsprojekte werden Sicherheitsanforderungen im Entwurfsstadium analysiert. Die gewonnenen Erkenntnisse werden als Anforderungen bei der Entwicklung festgelegt.

6.5.2 Sicherheitsmaßnahmen beim Computermanagement

Ausschließlich entsprechend dem Rollenkonzept autorisiertes Personal darf Computer, Netze und andere Komponenten administrieren. Es findet eine regelmäßige Auswertung von Logfiles auf Regelverletzungen, Angriffsversuche und andere Vorfälle statt. Überwachungsmaßnahmen beginnen mit Inbetriebnahme eines Gerätes und enden mit dessen Entsorgung.

6.5.3 Sicherheitsmaßnahmen während des Life Cycles

Eingesetzte Geräte werden gemäß Herstellerangaben betrieben. Vor Inbetriebnahme werden sie eingehend geprüft und kommen nur zum Einsatz, wenn zweifelsfrei feststeht, dass sie nicht manipuliert wurden. Bei Verdacht auf Manipulation einer Komponente, wird eine ggf. geplante Aktion an der Komponente nicht durchgeführt und der Vorfall gemeldet. Um kurzfristig und koordiniert auf eventuelle sicherheitsrelevante Vorfälle reagieren zu können, definiert der DV klare Eskalationsrichtlinien für die einzelnen Rollen.

Kapazitätsanforderungen und -auslastungen sowie Eignung der beteiligten Systeme werden überwacht und bei Bedarf angeglichen. Ausgetauschte Geräte oder obsolete Datenträger werden derart außer Betrieb genommen und entsorgt, dass Funktionalitäts- oder Datenmissbrauch ausgeschlossen wird. Änderungen an Systemen, Software oder Prozessen durchlaufen einen dokumentierten Change-Management-Prozess. Sicherheitskritische Änderungen werden durch den Sicherheitsbeauftragten geprüft. Nach Ablauf der Gültigkeit von CAs werden die privaten Schlüssel vernichtet.

Elektronische Daten oder papiergebundene Protokolle dokumentieren alle relevanten Ereignisse, die den Life-Cycle der CA sowie der ausgestellten Zertifikate und generierten Schlüssel beeinflussen und werden auf langlebigen Medien revisionssicher gespeichert. Die Medien des Unternehmens werden entsprechend ihrer Klassifizierung im Rahmen der Dokumentationsrichtlinie des DVs zuverlässig vor Schaden, Entwendung, Verlust oder Kompromittierung geschützt.

Penetrationstests werden durch eine unabhängige und fachkundige Stelle regelmäßig durchgeführt. Weiterhin werden regelmäßig Schwachstellenscans veranlasst.

6.6 Sicherheitsmaßnahmen für Netze

Im Betrieb der CAs wird ein Netzkonzept realisiert, welches sicherstellt, dass die relevanten CA-Systeme in besonders gesicherten Netzwerkzonen betrieben werden. Die Netzwerkarchitektur des DV beinhaltet ein mehrstufiges Konzept der Netzwerksicherheitszonen. Für das Netzkonzept liegt eine detaillierte Dokumentation vor, die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann.

Zum Schutz der Prozesse des DV werden beispielsweise Firewall und Intrusion Detection / Prevention Mechanismen eingesetzt, die nur explizit erlaubte Verbindungen zulassen. Der DV betreibt Netzsegmente unterschiedlichen Schutzbedarfs und trennt dabei Mitarbeiter- und Internet-nahe Netze sorgfältig von Servernetzwerken. Die Systeme unterliegen regelmäßigen Revisionen, die Verantwortlichen sind berichtspflichtig. Auffälligkeiten werden durch technische Systeme und organisatorische Prozesse gemeldet und in einem definierten Incidentverfahren und daran ansetzenden Prozessen behandelt.

Die Verfügbarkeit der Internetanbindung ist durch Redundanz abgesichert. Es bestehen zwei ständige Verbindungen zum Provider auf zwei unterschiedlichen Streckenführungen. Beim Ausfall des Zugangspunktes des Providers erfolgt die automatische Umschaltung auf die zweite Anbindung.

Datenverkehr mit hohem Schutzbedarf außerhalb der durch den DV geschützten Netzwerke, für den Integrität oder Vertraulichkeit sichergestellt werden muss, wird durch kryptographische Mechanismen geschützt.

Die physische Sicherheit der durch den DV betriebenen und genutzten Netze ist sichergestellt und wird den baulichen Gegebenheiten und ihren Veränderungen angepasst.

6.7 Zeitstempel

Der DV betreibt einen Zeitstempeldienst. Zeitstempel werden im Rahmen dieses CPS jedoch nicht angeboten.

7. Profile von Zertifikaten und Sperrlisten

7.1 Zertifikatsprofile

7.1.1 CV-Zertifikate

Die Zertifikatsprofile entsprechen der TR-03110 und der [CP CVCA-eID]

CV-Zertifikate für den nichthoheitlichen Einsatz enthalten folgende Erweiterungen:

- Certificate Description
- Terminal Sector

Beide Erweiterungen werden entsprechend Kapitel 4.1.1.2 [CP CVCA-eID] benutzt.

7.1.2 MDS-Zertifikate

Der Aufbau von MDS-Zertifikaten ist in der [CP CVCA-eID] festgelegt.

MDS-Zertifikate enthalten folgende Felder im Subject:

Feld	OID	Parameter
countryName	2.5.4.6	*DE*
organizationName	2.5.4.10	*<Name des Dienstanbieters>*
organizationalUnitName	2.5.4.11	*Metadata Signer DA Certificate Germany*
commonName	2.5.4.3	*DE<HolderMnemonic>*
serialNumber	2.5.4.5	*<Antragsnummer>*

MDS-Zertifikate enthalten folgende *kritische* Erweiterungen:

Erweiterung	OID	Parameter
KeyUsage	2.5.29.15	*digitalSignature*

MDS-Zertifikate können folgende *unkritische* Erweiterungen enthalten:

Erweiterung	OID	Parameter
authorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash des Ausstellersschlüssels
subjectKeyIdentifier	2.5.29.14	160-bit SHA-1 Hash des Subject Public Key

Erweiterung	OID	Parameter
cRLDistributionPoints	2.5.29.31	Adresse(n) der CRL-Ausgabestell(n)e
certificatePolicies	2.5.29.32	OIDs der unterstützten CPs

7.1.3 Sperrlisten

Sperrlisten werden nur für Metadaten Signer Diensteanbieter-Zertifikate (MDS DA-Zertifikate) erstellt. Für CV-Zertifikate werden keine Sperrlisten erstellt.

Für Metadaten Signer DA-Zertifikate wird ein Auskunftsdienst (CRL) gemäß [RFC5280] angeboten. Die CRL wird täglich aktualisiert.

8. Auditierungen und andere Prüfungen

Revisionen, Revisionsgegenstände und Prozesse sind detailliert in der Dokumentation der D-Trust GmbH beschrieben. Das Rollenkonzept dokumentiert die Qualifikation und die Stellung des Revisors.

Die Dokumentation wird regelmäßig durch eine unabhängige Konformitätsbewertungsstelle geprüft. Bei begründetem Interesse können diese Dokumente in den relevanten Teilen eingesehen werden.

CP und CPS erfüllen für Zertifikate die Anforderungen gemäß [TR-03145-1] bzw. [TR-03145-4]. Ein regelmäßiges Assessment durch einen qualifizierten und unabhängigen Dritten belegt die Kompatibilität.

Es finden regelmäßige Wiederholungsprüfungen statt. Sollten sich die Verfahren als nicht mehr konform zu den aktuellen Richtlinien erweisen, unterlässt der DV das Ausstellen o. g. Zertifikate bis die Richtlinienkonformität wiederhergestellt und entsprechend überprüft wurde.

Diese Auditierung findet jährlich statt.

Darüber hinaus finden regelmäßig interne Audits statt.

9. Sonstige finanzielle und rechtliche Regelungen

Bezüglich der entsprechenden Regelungen wird auf Kapitel 9 in der CP der D-Trust verwiesen.