20. Juni 2016

PrimeSign Certification Practice Statement für qualifizierte Zertifikate

DI Thomas Knall
DI Sandra Kreuzhuber
Dr. Klaus Stranacher

Version 1.0.0

PrimeSign GmbH, Wielandgasse 2, A–8010 Graz

tel. +43 316 25830, fax: +43 316 25830-11, IBAN: AT781200010004860457, BIC: BKAUATWW
mail: office@prime-sign.com, web: www.prime-sign.com

Firmenadresse:

PrimeSign GmbH
Wielandgasse 2, A-8010 Graz, Austria

Inhaltsverzeichnis

Dokumenthistorie

TABELLE 1: DOKUMENTHISTORIE

Version	Datum	Autor	Änderungen	Status
0.1.0	24.05.2016	Thomas Knall, Sandra Kreuzhuber, Klaus Stranacher	Initialversion	Entwurf
0.2.0	01.06.2016	Jan Herold	Qualitätssicherung und Kommentare	Entwurf
0.3.0	08.06.2016	Thomas Knall, Sandra Kreuzhuber, Klaus Stranacher	Überarbeitungen und Anpassungen	Entwurf
0.4.0	15.06.2016	Siegried Gruber	Qualitätssicherung und Kommentare	Entwurf
0.5.0	17.06.2016	Thomas Knall, Sandra Kreuzhuber, Klaus Stranacher	Überarbeitungen und Anpassungen	Finaler Entwurf
1.0.0	20.06.2016	Thomas Rössler	Überarbeitung, Freigabe und Veröffentlichung	Veröffentlicht

1 Einleitung

1.1 Überblick

Das vorliegende Dokument repräsentiert das Certification Practice Statement (CPS) der von der PrimeSign GmbH betriebenen (qualifizierten) Public Key Infrastruktur (PKI).

Anmerkung: Das vorliegende Dokument nutzt die Terminologie die mittels der Verordnung (EU) 910/2014 (eIDAS VO) [EIDAS] festgelegt wurde.

Anmerkung: Das vorliegende CPS beinhaltet auch sämtliche ergänzenden Informationen aus der entsprechenden CP, um das vorliegende Dokument möglichst eigenständig und in sich geschlossen zu halten.

Die PrimeSign GmbH betreibt als qualifizierter Vertrauensdiensteanbieter – im Folgenden VDA genannt – einen Vertrauensdienst für die Ausstellung von qualifizierten Zertifikaten zur Nutzung mit (qualifizierten) elektronischen Signaturen und (qualifizierten) elektronischen Siegeln[1].

Die Gliederung dieses Dokuments orientiert sich an dem internationalen Standard für Zertifizierungsrichtlinien [RFC 3647] der Internet Society und erfüllt die entsprechenden Anforderungen folgender Standards des Europäischen Instituts für Telekommunikationsnormen:

- ETSI EN 319 411-1 V1.1.1 (2016-02): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [ETSI EN 319 411-1]
- ETSI EN 319 411-2 V2.1.1 (2016-02): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing [ETSI EN 319 411-2]

1.2 Name und Kennzeichnung des Dokuments

Name der Richtlinie:	PrimeSign Certification Practice Statement für qualifizierte Zertifikate zur Nutzung mit qualifizierten Signaturen und qualifizierten Siegeln.
Version:	1.0.0
Datum:	20.06.2016

[1] Qualifizierte Zertifikate zur Nutzung mit qualifizierte Siegeln werden seitens des VDA erst ausgegeben, wenn die entsprechenden rechtlichen Voraussetzungen in Kraft getreten sind.

Object Identifier: 1.2.040.0.39.1.2.1.1.0.0
1.2.040.0.39(primesign).1(Dokumentation).2(CPS für qualifizierte Zertifikate).1(CA spezifisch).1.0.0(vorliegende Version)

Die OID 1.2.040.0.39 ist auf die Firma PrimeSign GmbH registriert.

1.3 PKI Teilnehmer

In diesem Abschnitt werden die PKI Teilnehmer und ihre Aufgaben skizziert. Detaillierte Informationen können in Folge den weiteren Abschnitten entnommen werden.

1.3.1 Zertifizierungsstellen

Die Zertifikatshierarchie des VDA für qualifizierte Zertifikate ist in drei Ebenen gegliedert. Die oberste Ebene bildet die Qualifizierte Root CA. Davon abgeleitet werden in der zweiten Ebene entsprechende qualifizierte CAs, die in weitere Folge (und somit in Ebene 3) die qualifizierten Endanwenderzertifikate ausstellen. Abbildung 1 bietet eine schematische, exemplarische Darstellung der Zertifikatshierarchie.

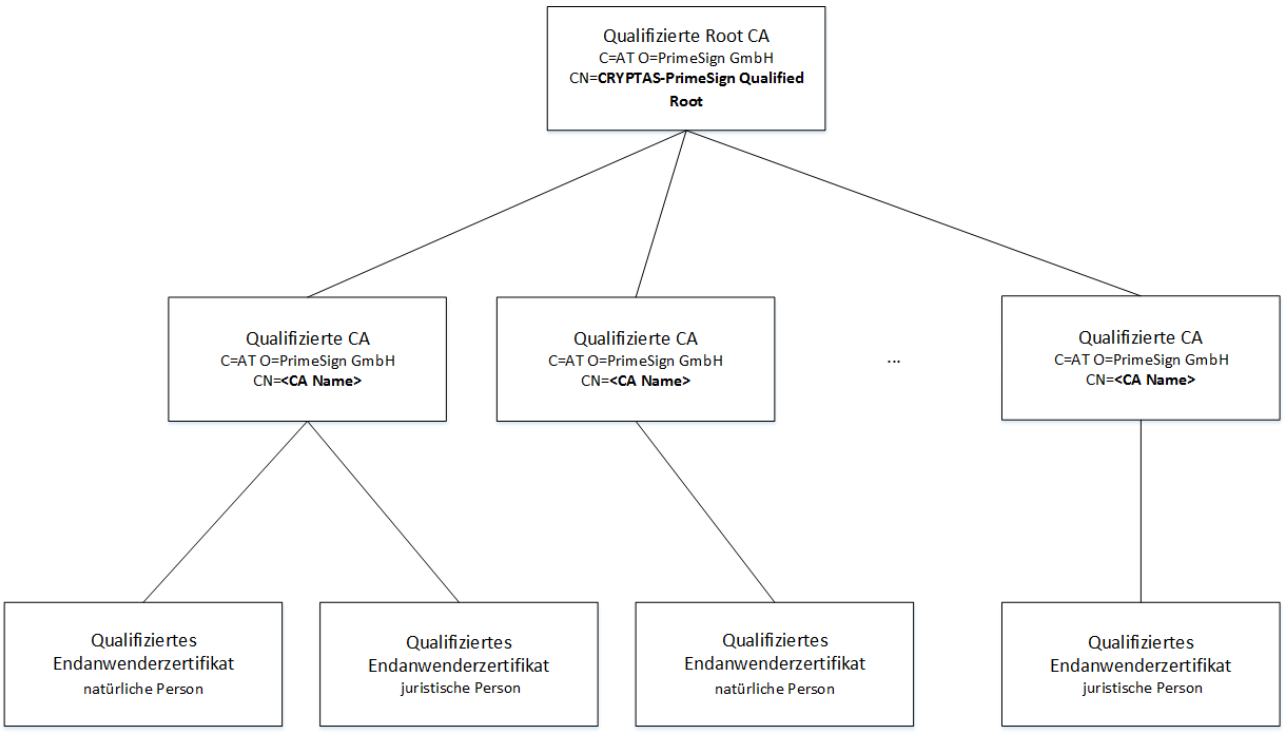

ABBILDUNG 1: ZERTIFIKATSHIERARCHIE

Das Root-Zertifikat sowie die darunterliegenden CA-Zertifikate werden vom VDA ausgestellt. In dieser Zertifikatshierarchie werden lediglich qualifizierte Endanwenderzertifikate ausgestellt.

Der VDA stellt qualifizierte Zertifikate für elektronische Signaturen an natürliche Personen sowie qualifizierte Zertifikate für elektronische Siegel an juristische Personen aus. Die Unterscheidung

zwischen einem qualifizierten Zertifikat für elektronische Signaturen bzw. elektronische Siegel erfolgt durch Verwendung der Zertifikatserweiterung *QCStatement*. Für nähere Informationen zum verwendeten Zertifikatsprofil siehe Abschnitt 7.1. Soweit diese zur Ausstellung qualifizierter Zertifikate verwendet werden, kommen die Bestimmungen dieses Dokuments zur Anwendung.

Der VDA behält es sich vor, weitere qualifizierte CA-Zertifikate (d.h. weitere CAs zur Ausstellung von qualifizierten Endanwenderzertifikaten) je nach Bedarf für spezielle Nutzungsszenarien oder für geschlossene Organisationen auszustellen.

Weiters steht es dem VDA frei, bei Bedarf zusätzlich fortgeschrittene Zertifikate auszustellen, jedoch erfolgt dies in einer weiteren Zertifikatshierarchie mit einem eigenen Root-Zertifikat.

1.3.2 Registrierungsstellen

In der Registrierungsstelle wird die Registrierung von Zertifikatserwerbern durch einen so genannten Registration Officer (RO) durchgeführt. Alternative Registrierungsmöglichkeiten können, sofern sie dieselbe Qualität hinsichtlich der Identifizierung des Zertifikatserwerbers und der Überprüfung der Daten des Zertifikaterwerbers ermöglichen, zusätzlich angeboten werden. Für die Registrierung sind dabei insbesondere folgende Tätigkeiten notwendig: sichere und eindeutige Identifizierung der Zertifikatserwerber, Überprüfung und Bearbeitung der Daten des Zertifikatserwerbers sowie schließlich die Weiterleitung dieser geprüften Daten an die entsprechende Zertifizierungsstelle.

1.3.3 Widerrufs- und Sperrdienst

Zertifikatsinhaber können jederzeit an den VDA einen Antrag auf Widerruf oder Sperre ihres Zertifikates stellen. Dies erfolgt über den Widerrufs- und Sperrdienst. Abschnitt 3.4 und 4.8 enthalten nähere Informationen zum Ablauf eines Widerrufs bzw. einer Sperre.

1.3.4 Zertifikatserwerber und Zertifikatsinhaber (Signator)

Anträge auf Ausstellung eines Zertifikates können sowohl von natürlichen Personen wie auch von juristischen Personen durch eine vertretungsbefugte natürliche Person eingebracht werden. Zertifikatsinhaber ist in Folge jene Person, auf die das Zertifikat ausgestellt ist. Der Zertifikatsinhaber ist der Hauptanwender, der eine qualifizierte elektronische Signatur oder ein qualifiziertes elektronisches Siegel aufbringt.

1.3.5 Sonstige Teilnehmer

Sonstige Teilnehmer sind vor allem die Empfänger bzw. Nutzer eines Zertifikats. Sie vertrauen dabei auf die angegebenen Daten im Zertifikat, die sie beispielsweise im Zuge der Überprüfung der Gültigkeit einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels gewinnen.

1.4 Zertifikatsverwendung

Mit der Ausstellung des qualifizierten Zertifikats basierend auf dieser Richtlinie wird von der Zertifizierungsstelle der Schlüssel des Signators zertifiziert. Dieser Schlüssel darf ausschließlich für das Erstellen von qualifizierten elektronischen Signaturen oder qualifizierten elektronischen Siegeln genutzt werden.

Elektronische Signaturen, die auf einem unter dieser Richtlinie ausgestellten Zertifikat für elektronische Signaturen basieren und mit einer qualifizierten Signaturerstellungseinheit erstellt wurden, sind qualifizierte elektronische Signaturen gemäß Artikel 3 Z 27 Verordnung (EU) 910/2014 [EIDAS].

Elektronische Siegel, die auf einem unter dieser Richtlinie ausgestellten Zertifikat für elektronische Siegel basieren und mit einer qualifizierten Siegelerstellungseinheit erstellt wurden, sind qualifizierte elektronische Siegel gemäß Artikel 3 Z 27 Verordnung (EU) 910/2014 [EIDAS].

1.5 Pflege des CPS

1.5.1 Zuständigkeit für das Dokument

Dieses Dokument wurde von der PrimeSign GmbH erstellt und herausgegeben. Die PrimeSign GmbH ist für die Pflege, Verwaltung und Organisation des Dokuments verantwortlich.

1.5.2 Kontaktinformation

Die Kontaktaufnahme kann über folgende Wege erfolgen:

PrimeSign GmbH
Wielandgasse 2, 8010 Graz

Niederlassung Wien:
PrimeSign GmbH, Franzosengraben 8, 1030 Wien

Telefon: +43 316 25 830
Web: https://prime-sign.com
Email: office@prime-sign.com

1.5.3 Verantwortlicher für die Anerkennung anderer CP

Die PrimeSign GmbH entscheidet über die Anerkennung andere CPS.

1.6 Begriffe und Abkürzungen

TABELLE 2: BEGRIFFE UND ABKÜRZUNGEN

AGB	Allgemeine Geschäftsbedingungen
AO	Audit Officer
ASN.1	Abstract Syntax Notation One
BKA	Bundeskanzleramt
CA	Certification Authority (Zertifizierungsstelle)
CARL	Widerrufsliste für CA-Zertifikate
CEO	Chief Executive Officer
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
eIDAS	Verordnung (EU) 910/2014
EAL	Evaluation Assurance Level
ETSI	European Telecommunications Standards Institute (Europäisches Institut für Telekommunikationsnormen)
FIPS	Federal Information Processing Standard
GMT	Greenwich Mean Time
HSM	Hardware Security Module
ISO	International Organization for Standardization
LCO	Legal Compliance Officer
LCRO	Liaison and Chief Registration Officer
LDAP	Lightweight Directory Access Protocol

OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastruktur
PO	Policy Officer
QSCD	Qualified Signature Creation Device
Remote Signing	Elektronische Fernsignatur gemäß [EIDAS]
RKSV	Registrierkassensicherheitsverordnung
RO	Registration Officer
RVO	Revocation Officer
SA	System Administrator
SIR	SIR definiert eine Schnittstelle bzw. einen Prozess, welche elektronische Identitätsnachweise ausgewählter, zuverlässiger Quellen des öffentlichen Bereichs sammelt und diese dem VDA für die Ausstellung eines qualifizierten Zertifikats über eine definierte Web-Service Schnittstelle zur Verfügung stellt.
SO	Security Officer
VDA	Qualifizierter Vertrauensdiensteanbieter PrimeSign GmbH
VPN	Virtual Private Network

2 Verantwortlichkeiten für Veröffentlichungen und Verzeichnisse

2.1 Verzeichnisse

2.1.1 Zentraler Verzeichnisdienst

Es wird ein zentraler Verzeichnisdienst betrieben, in dem Zertifikate veröffentlicht sind. Der Verzeichnisdienst kann dabei via LDAP abgefragt werden und ist unter folgender URL öffentlich erreichbar:

- ldap://ldap.tc.prime-sign.com/

2.1.2 Auskunftsdienst über den Zertifikatsstatus

Statusinformationen zu den herausgegebenen Zertifikaten können via CRL oder OCSP abgefragt werden. Diese Auskunftsdienste sind über folgende URLs erreichbar:

- OCSP: http://ocsp.tc.prime-sign.com/ocsp
- Verteilungspunkt für die (CRLs): http://tc.prime-sign.com/crls

2.2 Veröffentlichung von Informationen

Sämtlichen öffentlichen Informationen werden auf der Webseite des VDA unter folgender Adresse veröffentlicht:

- http://tc.prime-sign.com

Zu diesen Informationen zählen insbesondere:

- Certificate Policy (CP)
- Certification Practice Statement (CPS)
- Root-Zertifikat
- CA-Zertifikat
- Sperr- und Widerrufsinformationen
- Allgemeine Geschäftsbedingungen (inkl. Informationen zu Haftung, Haftungsbeschränkungen und Schadenersatzansprüche)

Das Dokument Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung [TP], das die Grundlage für das vorliegende Dokument bildet, ist vertraulich und ist daher nicht öffentlich zugänglich.

2.3 Häufigkeit von Veröffentlichungen

Die Veröffentlichung des CPS erfolgt immer unmittelbar nach Erstellung bzw. Freigabe des Dokuments.

Die Veröffentlichung eines Zertifikats erfolgt unmittelbar nach der Erstellung des Zertifikats, sofern der Zertifikatsinhaber der Veröffentlichung zugestimmt hat. Jede Änderung des Zertifikatsstatus wird ebenfalls unverzüglich in den Statusinformationen veröffentlicht.

2.4 Zugriffskontrollen auf Verzeichnisse

Der Zugriff auf den zentralen Verzeichnisdienst ist nur lesend möglich. Bei Listenabfragen kann eine bestimmte Mengenbegrenzung erfolgen.

Der Zugriff auf den Auskunftsdienst über den Zertifikatsstatus ist ebenfalls nur lesend, aber ansonsten unbeschränkt möglich.

3 Identifizierung und Authentifizierung

3.1 Namensregeln

Für die Ausstellung von Zertifikaten an natürliche Personen wird der Name des Zertifikatsinhabers durch folgende Attribute im Feld *subject* dargestellt:

Vorgeschriebene Attribute:

- countryName (C) – Land gemäß [ISO 3166]
- givenName (GN) – Vorname der natürlichen Person
- surname (SN) – Familienname der natürlichen Person
- pseudonym (PN) (optional, nur erlaubt falls kein *givenName* und *surname* im Zertifikat angegeben)
- commonName (CN) – Gebräuchlicher Name
- serialNumber – Seriennummer, welche die Eindeutigkeit des Subjektstrings (dargestellt als Subject Distinguished Name) innerhalb der CA sicherstellt. Die im Feld *subject* enthaltene Seriennummer ist zufällig generiert und nicht notwendigerweise ident zur Seriennummer des Zertifikats. Zwei oder mehrere Zertifikate desselben Zertifikatsinhabers weisen nicht dieselbe Seriennummer im Zertifikat auf.

Optionale Attribute:

- organizationName (O) – Offizielle Bezeichnung der Organisation, der der Zertifikatsinhaber angehört
- organizationalUnit (OU) – Organisationseinheit innerhalb der Organisation, der der Zertifikatsinhaber angehört
- organizationIdentifier – Registernummer der Organisation gemäß der amtlichen Eintragung, z.B. Firmenbuchnummer, Vereinsregisternummer

Das Attribut *countryName* gibt das Land an, das das Identifikationsdokument ausgestellt hat, mit dem der Zertifikatsinhaber identifiziert wird. Ist ein *organizationName* im Zertifikat angegeben, so gibt *countryName* den Sitz der Organisation an.

Das Attribut *commonName* besteht aus den Attributen *surname* und *givenName* des Zertifikatsinhabers oder dem angegebenen Pseudonym (Natürliche Personen ohne Pseudonym: “Vorname Familienname”, optional mit vorangestelltem Titel Natürliche Personen mit Pseudonym: “Pseudonym”). Die Schreibweise des Namens der natürlichen Person in den Attributen *surname* und *givenName* muss mit der Schreibweise im für die Identifizierung verwendeten Identifikationsdokument übereinstimmen. Wird anstatt des Namens im Zertifikat ein Pseudonym verwendet, so darf dieses weder anstößig sein noch darf eine Verwechslungsgefahr mit Namen oder Kennzeichnen (z.B. Markennamen) bestehen.

Für die Kodierung von Namensbestandteilen wird der Zeichensatz UTF-8 unterstützt.

Die Seriennummer wird als positive Integer Zahl dargestellt und von der CA eindeutig für jeden Subject Distinguished Name zugewiesen.

Optional kann der Zertifikatsinhaber im Attribut *organizationName* die offizielle Bezeichnung der Organisation, der der Zertifikatsinhaber angehört angeben. Das Attribut *organizationalUnit* beschreibt die Organisationseinheit (beispielsweise Abteilung oder Bereich) der angegebenen Organisation. Die Zugehörigkeit zur Organisation wird dabei vor Aufnahme ins Zertifikat gemäß Abschnitt 3.2.1 geprüft. Im Rahmen dieser Prüfung ist eine Bestätigung einer für die jeweilige Organisation betretungsbefugten Person vorzulegen, dass der Zertifikatserwerber eine Zuordnung zur Organisation im Zertifikat eintragen darf.

Falls erwünscht, kann die E-Mail-Adresse des Zertifikatsinhabers in das Zertifikat aufgenommen werden. Die E-Mail-Adresse wird in der optionalen Zertifikatserweiterung *Subject Alternative Name* dargestellt. Die E-Mail-Adresse darf nur ins Zertifikat aufgenommen werden, falls der Zertifikatsinhaber im Zuge der Registrierung den Zugriff auf die angegebene E-Mail-Adresse bestätigt hat.

Für die Ausstellung von Zertifikaten an juristische Personen wird der Name des Zertifikatsinhabers durch folgende Attribute im Feld *subject* dargestellt:

Vorgeschriebene Attribute:

- countryName (C) – Sitz der juristischen Person (beispielsweise des Unternehmens oder des Vereins)
- organizationName (O) – vollständig registrierter Name der juristischen Person
- organizationIdentifier[2] – Registernummer der Organisation gemäß der amtlichen Eintragung, z.B. Firmenbuchnummer, Vereinsregisternummer
- commonName (CN) – Offizielle Bezeichnung der Organisation (Unternehmen, Verein, Behörde etc.) oder gegebenenfalls eine sinnvolle Abkürzung
- serialNumber – Seriennummer, welche die Eindeutigkeit des Subjektstrings (dargestellt als Subject Distinguished Name) innerhalb der CA sicherstellt. Die im Feld *subject* enthaltene Seriennummer ist nicht ident zur Seriennummer des Zertifikats.

[2] Das Attribut *organizationIdentifier* wird als Datentyp SemanticsIdentifier im Zertifikat dargestellt. Siehe ETSI 319 412-1 für die Kodierungsregeln.

3.2 Initiale Überprüfung der Identität

3.2.1 Natürliche Personen

Bei der Antragsstellung muss der Zertifikatserwerber seine Identität persönlich gegenüber dem Registration Officer (RO) unter Verwendung eines gültigen, amtlichen Lichtbildausweises nachweisen.

Bei Bedarf und nach technischer Möglichkeit steht dem Zertifikatserwerber die Möglichkeit zur Verfügung seine Identität mittels sicherer Distanz-Identifikationsverfahren, bei denen der Zertifikatswerber nicht vorort bei einem Registration Officer erscheinen muss, nachzuweisen. Konventionelle, zulässige Distanz-Identifikationsverfahren sind etwa Verfahren auf Basis einer postalen Zustellung zu eigenen Handen (Post-Identifikationsprozess), bei denen die sichere Identitätsüberprüfung im Zuge der Zustellung eines Schriftstücks durch die Mitarbeiter des Zustelldienstes erfolgt. Alternative, vor allem elektronische Distanzverfahren sind möglich und können abhängig von deren technischer Machbarkeit und rechtlicher Zulässigkeit (vor dem Hintergrund des vorliegenden Dokuments) vom ZDA eingerichtet und angeboten werden.

Zusätzlich steht die Möglichkeit zur Verfügung, ein neues qualifiziertes Zertifikat mittels bereits vorhandener eindeutiger starker elektronischer Identität (gemäß Artikel 24 Abs 1 lit c iVm Art 24 Abs 1 lit a und b Verordnung (EU) 910/2014 [EIDAS]; Sicherheitsniveau substantiell oder hoch) bzw. mit einer bestehenden qualifizierten Signatur oder mit geeigneten anderen zulässigen elektronischen Nachweisen (etwa behördlichen Identitätsbestätigungen, etc.), die über eine dem Stand der Technik und den Vorgaben dieses Dokumentes entsprechende Umsetzung des SIR-Verfahrens erbracht werden, zu beantragen.

Alle im Zertifikat eingetragenen Daten werden bei der Registrierung mit größter Sorgfalt überprüft. Zum Einsatz kommen hierbei nur Identifizierungsmethoden, die auf nationaler Ebene anerkannt sind und gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten. Die gleichwertige Sicherheit muss von einer Konformitätsbewertungsstelle bestätigt werden.

Ist der Zertifikatserwerber eine natürliche Person müssen insbesondere auch folgende Angaben überprüft werden:

- Vollständiger Name
- Geburtsdatum und Geburtsort

Auch bei Zertifikaten, die anstatt des Namens ein Pseudonym enthalten, wird durch den VDA die reale Identität des Zertifikatserwerbers, insbesondere dessen vollständiger Name, überprüft und festgehalten.

Bei Angabe von Organisationsdaten im Zertifikat, muss der Zertifikatserwerber die Einwilligung der Organisation bzw. die Autorisierung der Organisation durch Vorlage geeigneter Dokumente nachweisen. Folgende Daten bzw. Dokumente müssen dazu vorgebracht und überprüft werden:

- Vollständiger Name und Rechtsform der assoziierten juristischen Person
- Registereintragung zur assoziierten juristischen Person (z.B. Firmenbucheintragung)
- Sitz der Organisation
- Bestätigung der Organisationszugehörigkeit
- Autorisierung durch die vertretungsbefugten Organe der Organisation, die bestätigen, dass die antragstellende natürliche Person im Zertifikat eine Zuordnung zur Organisation eintragen darf

3.2.2 Juristische Personen

Im Falle einer Zertifikatsantragsstellung für eine juristische Person muss der Vertreter der juristischen Person seine diesbezügliche Berechtigung nachweisen und sich gegenüber dem VDA authentifizieren (siehe Anforderungen aus Abschnitt 3.2.1 für die Authentifizierung von natürlichen Personen). Weiters werden alle im Zertifikat anzugebenden Daten der juristischen Person überprüft. Insbesondere müssen folgende Daten der juristischen Person vorgelegt und überprüft werden:

- Vollständiger Name der juristischen Person
- Registereintragung der juristischen Person (z.B. Firmenbuch)
- Falls im Zertifikat eine Assoziierung mit einer weiteren Organisation vorgenommen werden soll, gelten dieselben Anforderungen wie für die Assoziierung von natürlichen Personen mit einer Organisation (siehe Abschnitt 3.2.1).

3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung

Die Schlüsselerneuerung bezeichnet die erneute Generierung von Zertifikaten und Schlüsseln für das selbe Subject, beispielsweise nach Ablauf der Gültigkeit, nach einem Widerruf oder bei Änderung von Daten des Zertifikatsinhabers. Eine Rezertifizierung auf Basis des gleichen Schlüsselmaterials wird vom VDA nicht unterstützt.

Für die Neuausstellung kann, falls sich keine der im Zertifikat angegebenen Daten geändert haben, eine Identifizierung und Authentifizierung auf Basis eines bereits bestehenden gültigen Zertifikats erfolgen, jedoch nur falls dieses weder gesperrt noch widerrufen ist. Bei Änderung von Daten erfolgt in jedem Fall die Identifizierung und Authentifizierung äquivalent zur Erstausstellung.

Im Zuge der Neuausstellung muss der Zertifikatserwerber sämtliche vertragliche Bedingungen in deren aktuellen Fassung erneut akzeptieren.

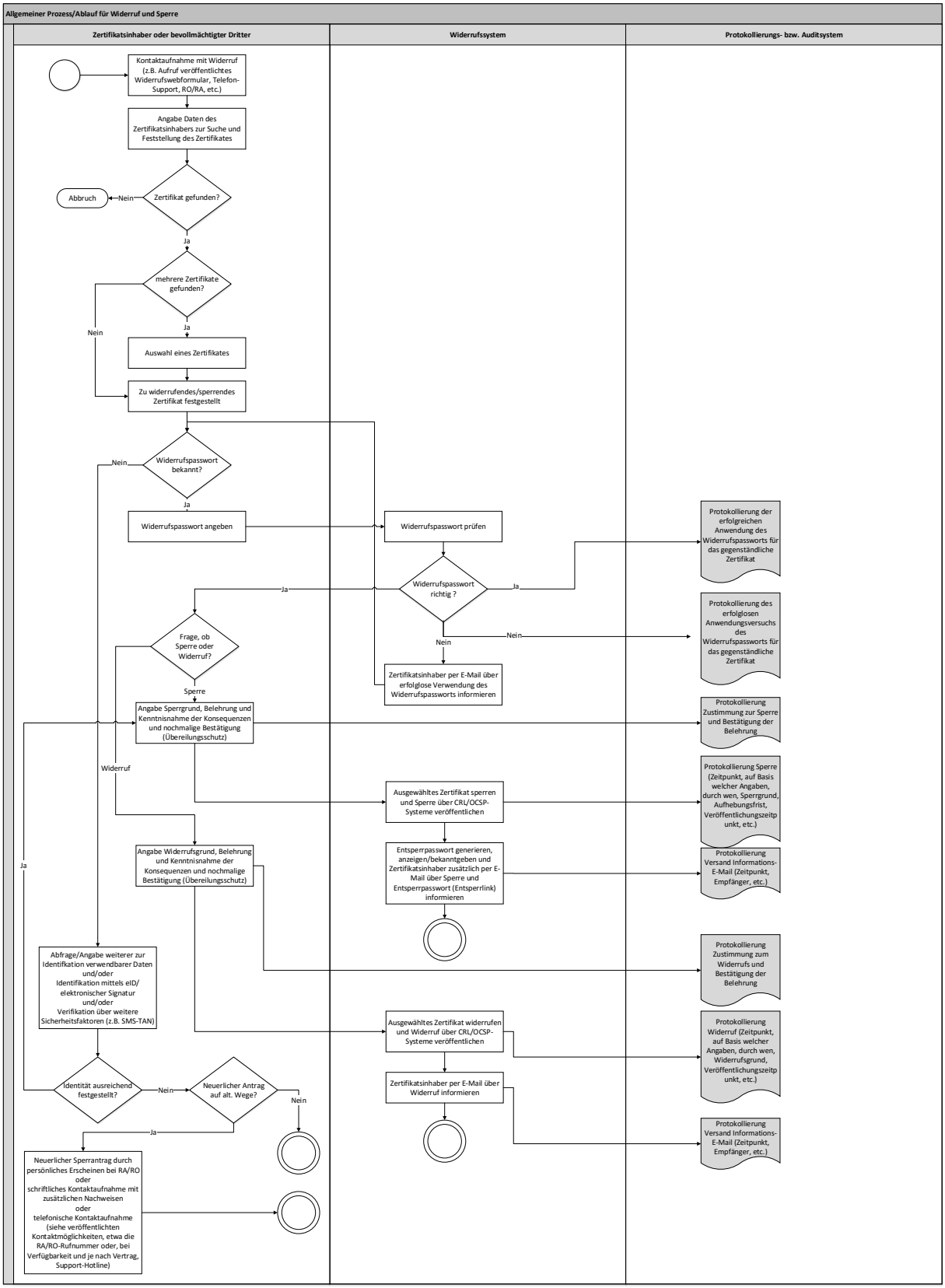

ABBILDUNG 2 ABLAUF SPERRE BZW. WIDERRUF

3.4 Identifizierung und Authentifizierung von Anträgen auf Sperrung und Widerruf

Zertifikatsinhaber oder berechtigte Dritte können Zertifikate sperren oder widerrufen. Ein Widerruf ist permanent und kann nicht aufgehoben werden. Eine Sperre kann hingegen innerhalb von zehn Tagen wieder aufgehoben werden. Wird die Sperre nicht innerhalb dieser Frist aufgehoben geht diese automatisch in einen Widerruf über.

Prinzipiell können vom VDA folgende Möglichkeiten zur Beantragung einer Sperre bzw. eines Widerrufs zur Verfügung gestellt werden:

- Sperre bzw. Widerruf über den telefonischen Widerrufsdienst,
- persönlich beim RO,
- über eine Webschnittstelle,
- sonstige Distanzverfahren (z.B. auf Basis einer elektronischen Identität, einem Post-Identifikationsverfahren oder anderen schriftlichen Verfahren in Papierform)

Die aktuell angebotenen Möglichkeiten zur Beantragung einer Sperre bzw. eines Widerrufs sind auf der Website des VDA zu finden.

Je nach gewählter Möglichkeit bestehen unterschiedliche Anforderungen an die Identifizierung und Authentifizierung des Antragstellers.

In jedem Fall ist eine Sperre, Aufhebung einer Sperre oder Widerruf eines Zertifikates durch den Zertifikatsinhaber auch ohne Widerrufspasswort möglich, wenn er sich persönlich oder über ein Distanzverfahren (hierbei insbesondere auf elektronischem Wege unter Zuhilfenahme einer akzeptablen elektronischen Identität oder eines bestehenden, der Person zweifelsfrei zuordenbarem qualifizierten Zertifikates, etc.) als Zertifikatsinhaber zweifelsfrei identifizieren kann. Maßgeblich für eine erfolgreiche Identifikation und demnach Akzeptanz eines derartigen Antrags, ungeachtet ihrer Art (persönlich, über die Distanz bzw. elektronisch), sind die Qualitätsansprüche, die für die Registrierung eines Zertifikatsinhabers in den gegenständlichen Dokumenten Certificate Policy [CP] und Certification Practice Statement festgelegt wurden.

Für nähere Informationen zur Veröffentlichung von Sperre und Widerruf, einer Liste von Gründen für die Durchführung einer Sperre bzw. eines Widerrufes sowie einer Auflistung zur Sperre bzw. zum Widerruf berechtigter Personen siehe Abschnitt 4.8 und 4.9.

3.4.1 Allgemeiner Ablauf von Sperre bzw. Widerruf

Abbildung 2 skizziert den allgemeinen Ablauf zur Initiierung einer Sperre bzw. eines Widerrufs.

Die Antragsstellung kann telefonisch, über ein Webformular, in Papierform, sowie persönlich erfolgen. In einem ersten Schritt erfolgt die Suche und Feststellung des betroffenen Zertifikats. Dazu benötigt der Antragssteller Daten des zu sperrenden Zertifikats (Seriennummer, im Zertifikat dargestellter Namen etc.). Falls mehrere Zertifikate eines Zertifikatsinhabers anhand des Namens gefunden werden, erfolgt die Auswahl des betroffenen Zertifikats.

Der Antragsteller benötigt zur Autorisierung einer Sperrung oder eines Widerrufs das gewählte Widerrufspasswort bzw. zur Aufhebung einer Sperrung das bei der Sperrung zugeteilte Sperraufhebungspasswort.

Erfolgt die Angabe eines inkorrekten Widerrufspassworts so wird der Zertifikatsinhaber aus Sicherheitsgründen per E-Mail über die erfolglose Verwendung des Widerrufspassworts informiert, um ihn über einen allfälligen unberechtigten Widerrufsversuch in Kenntnis zu setzen. Erfolgt die korrekte Eingabe des Widerrufspasswortes so wird der Antragssteller über die Folgen von Sperre bzw. Widerruf informiert und hat zum Zwecke der Protokollierung den Grund für die Sperre bzw. den Widerruf anzugeben. Er erfolgt die Bestätigung der Kenntnisnahme der Belehrung.

Das betroffene Zertifikat wird gesperrt bzw. widerrufen und die aktualisierte Widerrufsstatusinformation veröffentlicht. Zusätzlich wird der Zertifikatsinhaber per E-Mail über die erfolgte Sperre bzw. den erfolgten Widerruf informiert. In jedem Fall und insbesondere wenn der Antragsteller die Sperre elektronisch durchführt, wird dem Zertifikatsinhaber ein Sperraufhebungspasswort per E-Mail an die vom Zertifikatsinhaber bei der Registrierung hinterlegte E-Mail-Adresse versendet. Veranlasst ein Antragsteller die Sperre persönlich vor Ort oder telefonisch, so wird ihm auch das Sperraufhebungspasswort zusätzlich direkt mitgeteilt. Das Sperraufhebungspasswort wird dabei vom VDA automatisch generiert. Eine Aufhebung der Sperre ist nur unter Angabe des Sperraufhebungspasswortes möglich. Nach Ablauf der zehntägigen Frist erfolgt automatisch der Übergang von der Sperre des Zertifikats hin zum Widerruf.

Sollte dem Antragssteller das Widerrufspasswort nicht bekannt sein, so erfolgt zur Plausibilisierung der Berechtigung des Antragstellers die Abfrage persönlicher Daten bzw. der Antragsteller hat sich über geeignete Methoden zu authentifizieren (siehe Anforderungen an die Authentifizierung im Zuge der Zertifikatsausstellung in Abschnitt 3.2).

Konnte die Identität des Antragsstellers und dessen Berechtigung zur Durchführung einer Sperre bzw. eines Widerrufs ausreichend nachgewiesen werden so erfolgt die Belehrung des Antragsstellers und die anschließende Durchführung der Sperre bzw. des Widerrufs ident zum Prozess bei korrekter Angabe des Widerrufspasswortes.

Besonderheiten:

Mitarbeiter der Rolle RVO (z.B. Mitarbeiter der telefonischen Rufannahme) verfügen lediglich über die Berechtigung eine Sperre bzw. einen Widerruf unter Angabe des korrekten Widerrufspasswortes auszulösen. Sollte dem Antragsteller das Widerrufspasswort nicht bekannt sein, so leitet ein Mitarbeiter der Rolle RVO die Kontaktdaten des Antragstellers an einen Mitarbeiter des VDA mit der Rolle RO weiter (siehe Rollenkonzept Abschnitt 5.2). Außerhalb der Geschäftszeiten des VDA stehen dazu ausgewählte Mitarbeiter im Bereitschaftsdienst zur Verfügung. Der Mitarbeiter mit der Rolle RO kontaktiert den Antragsteller innerhalb von 2 Stunden, um gemeinsam mit dem Antragsteller das betroffene Zertifikat zu identifizieren, eine Plausibilitätsprüfung der Berechtigung des Antragstellers vorzunehmen und die Sperre bzw. den Widerruf wie oben angeführt durchzuführen. Ist dieses besondere telefonische Verfahren nicht erfolgreich – etwa mangels eines erfolgreichen Identitätsnachweises (Plausibilisierung) oder aus anderen Gründen nicht möglich oder nicht verfügbar – so ist der Antragsteller angehalten andere Antragswege zu bemühen oder persönlich vorstellig werden.

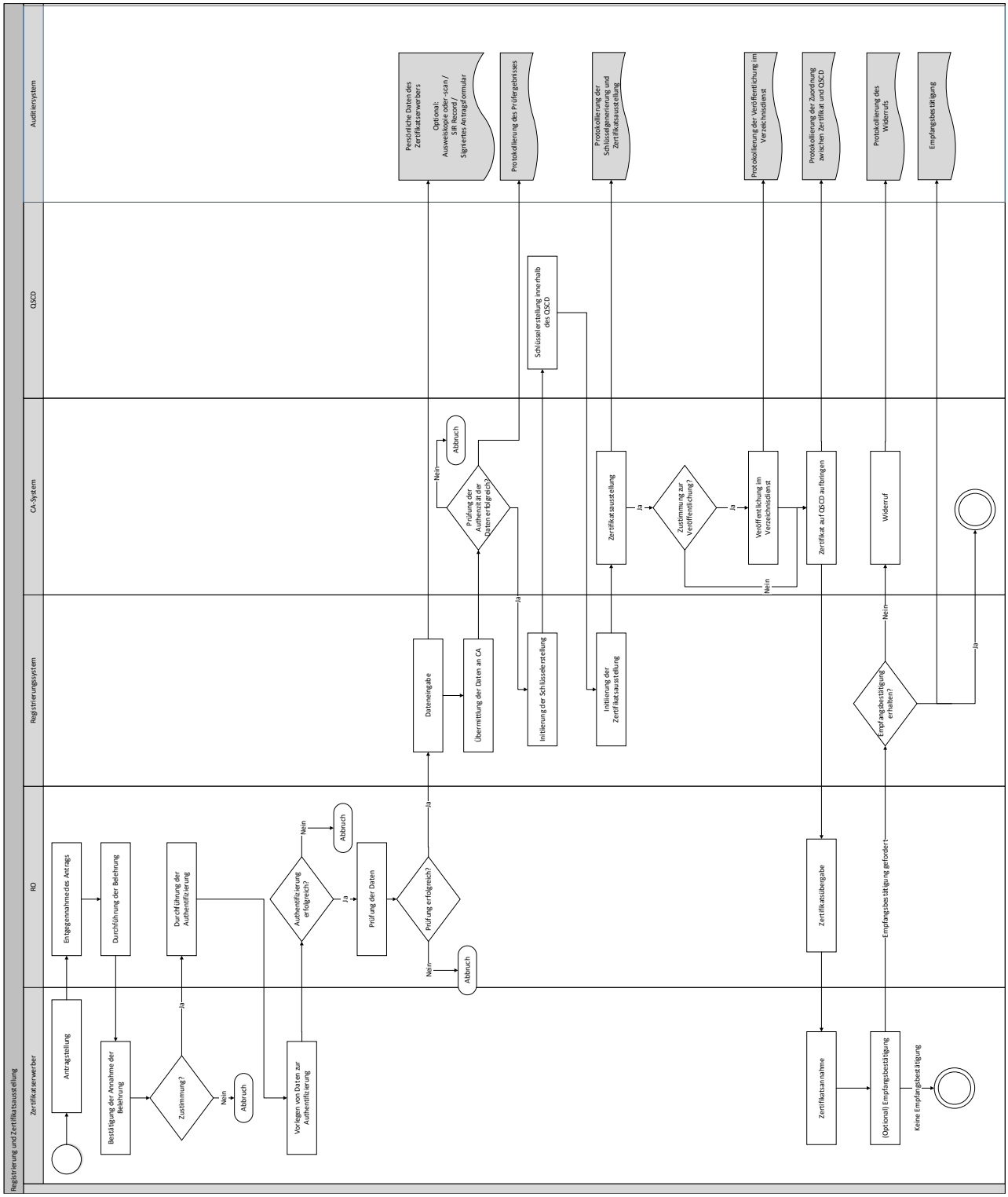

ABBILDUNG 3: PROZESS DER ANTRAGSSTELLUNG UND ZERTIFIKATSAUSSTELLUNG

4 Betriebsanforderungen

Abbildung 3 illustriert den gesamten Prozess von der Antragstellung bis zur Übergabe und Veröffentlichung des Zertifikats. In den folgenden Abschnitten werden die einzelnen Prozessphasen näher beschrieben.

4.1 Zertifikatsantrag und Registrierung

Anträge auf Ausstellung eines Zertifikates können sowohl von natürlichen Personen für sich selbst, wie auch für juristischen Personen durch eine vertretungsbefugte natürliche Person schriftlich oder über elektronische Antragsformulare oder persönlich in der Registrierungsstelle gegenüber einem RO gestellt werden. Unter Antrag wird verstanden, wenn der Zertifikatserwerber selbst oder durch Dritte seine Personendaten an die Registrierungsstelle bekannt gibt, um ein Signaturzertifikat (QSCD, wie Smartcard oder Remote QSCD) zu beantragen.

Zertifikatsanträge dürfen nur vom VDA oder einer vertrauenswürdigen Registrierungsstelle, welche vertraglich verpflichtet ist die Anforderungen des Registrierungsprozesses zu erfüllen, angenommen werden. Bei der Verwendung von externen Dienstleistern zur Durchführung des Registrierungsprozesses erfolgt der Datenaustausch mit dem VDA über gesicherte Kanäle, wobei die Authentizität der übertragenen Daten sichergestellt wird.

4.2 Bearbeitung des Zertifikatsantrags

Nach Antragstellung erfolgt die Bearbeitung des Zertifikatsantrags durch den RO. Der RO führt in einem ersten Schritt die Unterrichtung gemäß Artikel 24 Abs 2 lit d eIDAS-VO des Zertifikatserwerbers durch. Diese umfasst die Rechte und Pflichten gemäß Signaturvertrag, die Einwilligung zur Aufbewahrung von Daten der Registrierung und im Zuge des Lebenszyklus des Zertifikats anfallenden Daten, die Allgemeinen Geschäftsbedingungen und die vorliegenden Dokumente Certificate Policy [CP] und Certification Practice Statement. Die Bestätigung der Kenntnisnahme der vorgelegten Dokumente sowie die Zustimmung zum Signaturvertrag ist Voraussetzung für eine weitere Bearbeitung des Zertifikatsantrags. Der Zertifikatserwerber muss entscheiden, ob eine Veröffentlichung des Zertifikats im Verzeichnisdienst des VDA erfolgen soll.

Der RO führt die Identitätsprüfung des Zertifikatserwerbers sowie die Prüfung der Korrektheit der im Zertifikat anzugebenen Daten durch. Diese Daten können beispielsweise die Zugehörigkeit zu einer Organisation beinhalten. Zur Überprüfung der Identität der natürlichen oder juristischen Person kann ein persönliches Erscheinen des Zertifikatserwerbers notwendig sein oder alternative Nachweisformen, wie im Wege eines Distanzverfahrens (sofern vom VDA angeboten) oder auf Basis von Identitätsnachweisen aus authentischen Quellen (SIR-Verfahren, sofern vom VDA angeboten) beigebracht, genutzt werden (siehe Abschnitt 3.2). Bezüglich der im Zertifikat enthaltenen Daten finden die Regeln zur Namensgebung Anwendung (siehe Abschnitt 3.1).

Treten bei der Prüfung der Identität oder der Prüfung der Korrektheit der vom Zertifikatserwerber angegebenen Daten oder den Ausweis- und Nachweisdokumenten Unstimmigkeiten auf, die der Zertifikatserwerber nicht zeitnah und restlos ausräumt, wird der Zertifikatsantrag abgelehnt.

Im Zuge der Registrierung ist vom Zertifikatserwerber auch das gewählte Widerrufspasswort bekanntzugeben.

Nach erfolgreicher Prüfung werden die Daten des Zertifikatserwerbers durch den RO im Registrierungssystem des VDA eingetragen und an das CA-System des VDA übermittelt. Das CA-System prüft die Authentizität der übermittelten Daten und initiiert die Schlüsselerstellung innerhalb des QSCD. Die Schlüsselerstellung erfolgt in jedem Fall innerhalb des QSCD. Nach erfolgter Schlüsselerstellung wird das Zertifikat im CA-System erstellt, mit dem entsprechenden CA-Schlüssel signiert und auf das QSCD aufgebracht. Der Prozess der Zertifikatsausstellung und –aufbringung ist zur jeweiligen Registrierung des Zertifikatserwerbers zuordenbar und wird vor Manipulationen geschützt ausgeführt. Es erfolgt die Veröffentlichung des Zertifikats im Verzeichnisdienst. Sollte der Zertifikatserwerber einer Veröffentlichung nicht zustimmen, so entfällt diese.

4.3 Zertifikatsannahme

Nach Ausstellung des Zertifikats und Aufbringen des Zertifikats erfolgt die Übergabe an den Zertifikatsinhaber, beispielsweise in Form einer Smartcard oder den Zugangsdaten zu einem Remote-QSCD (Remote Signing). Diese kann entweder persönlich oder durch ein Zustellverfahren, bei dem die Prüfung der Identität des berechtigen Empfängers anhand von Ausweisdaten durch das Zustellorgan erfolgt, an die bei der Registrierung angegebene Lieferadresse erfolgen.

Im Zuge der Übergabe bestätigt der Zertifikatserwerber den Empfang des Zertifikates gegenüber dem VDA.

Optional kann der VDA vom Zertifikatserwerber eine Empfangsbestätigung fordern. Sollte diese vom Zertifikatserwerber nicht an den VDA übermittelt werden, erfolgt aus Sicherheitsgründen ein Widerruf des ausgestellten Zertifikats. Der Widerruf kann nicht rückgängig gemacht werden. Der VDA protokolliert die Empfangsbestätigung gemeinsam mit sämtlichen im Zuge der Antragstellung angegebenen Daten des Zertifikatserwerbers.

4.4 Verwendung des Schlüsselpaars und des Zertifikats

4.4.1 Nutzung durch den Zertifikatsinhaber

Der Zertifikatsinhaber verpflichtet sich die im Signaturvertrag und den Allgemeinen Geschäftsbedingungen des VDA enthaltenen Nutzungsbedingungen zu befolgen.

Insbesondere ergeben sich folgende Verpflichtungen des Zertifikatsinhabers:

- Korrekte Angabe der für die Registrierung notwendigen Daten

- Prüfung der im Zertifikat enthaltenen Daten nach Zustellung bzw. bei der Annahme des Zertifikats
- Gebot der Vorsicht um unbefugten Gebrauch des privaten Schlüssels zu verhindern
- Geheimhaltung der Aktivierungsdaten (PIN)
- Sichere Verwahrung und Schutz des QSCD: zum Beispiel
    - Im Falle der Verwendung einer Smartcard: sichere Verwahrung der Smartcard
    - Im Falle der Verwendung eines Remote-QSCD: sichere Verwahrung der Zugangsdaten (z.B. Wissen und Besitz)
- Qualifizierte Zertifikate dürfen lediglich für die Erstellung elektronischer Signaturen bzw. elektronischer Siegel verwendet werden
- Beachtung der im Signaturvertrag und den AGB definierten Regeln zur Schlüsselverwendung, insbesondere soll der Zertifikatsinhaber lediglich geeignete Komponenten zur Signatur- bzw. Siegelerstellung (Kartenleser, Betriebssystem, Software, etc.) verwenden. Der VDA kann zudem eine Liste an empfohlenen Komponenten und Verfahren veröffentlichen. Bei der Verwendung anderer Komponenten oder Verfahren haftet der VDA nicht für allfällige Schäden, die durch diese verursacht werden.
- Unverzügliche Benachrichtigung des VDA bei
    - Änderung von im Zertifikat angegebenen Informationen
    - Abhandenkommens oder Kompromittierung von Schlüsselmaterial
    - Verlust der alleinigen Kontrolle über das Schlüsselmaterial
- Unverzügliches Aussetzen der Verwendung des Zertifikats im Falle von Kompromittierung von Schlüsselmaterial oder nach einem Widerruf des Zertifikats
- Befolgung von Anweisungen des VDA infolge einer Kompromittierung von CA oder Subject Schlüsseln

Es steht dem VDA frei, bei Missachtung oben genannter Verpflichtungen Zertifikate des Zertifikatsinhabers zu widerrufen. Dem Zertifikatsinhaber gebührt in diesem Fall kein Kostenersatz.

4.4.2 Nutzung durch sonstige Teilnehmer

Jeder Empfänger bzw. Nutzer, der ein unter dieser CPS ausgestelltes Zertifikat zur Überprüfung einer Signatur oder zum Zwecke der Authentifizierung verwendet, muss

- überprüfen, ob das Zertifikat entsprechend den vermerkten Nutzungsarten (Schlüsselverwendung) verwendet wird,
- vor der Nutzung eines Zertifikats dessen Gültigkeit überprüfen, in dem er unter anderem die gesamte Zertifikatskette bis zum Wurzelzertifikat validiert,
- den Widerrufsstatus der beteiligten Zertifikate über den Statusabfragedienst (OCSP) oder die öffentliche Widerrufsliste (CRL) prüfen und

- sicherstellen, dass das Zertifikat ausschließlich für autorisierte und legale Zwecke in Übereinstimmung mit dieser CPS eingesetzt wird.

4.5 Zertifikatserneuerung

Der VDA bietet keine Zertifikatserneuerung auf Basis von altem Schlüsselmaterial an. Es erfolgt die Ausstellung eines neuen Zertifikats mit neu generiertem Schlüsselmaterial. Es gelten die Bestimmungen für die Erstausstellung.

4.6 Zertifikatserneuerung mit Schlüsselerneuerung

Es erfolgt die Ausstellung eines neuen Zertifikats mit neu generiertem Schlüsselmaterial. Es gelten die Bestimmungen für die Erstausstellung.

4.7 Zertifikatsänderungen

Bei Änderung von im Zertifikat angegebenen Daten des Zertifikatinhabers wird ein neues Zertifikat ausgestellt. Es gelten die Bestimmungen für die Erstausstellung.

4.8 Widerruf und Sperre von Zertifikaten

Der VDA sieht ein zweistufiges Widerrufskonzept vor: Zertifikate können entweder vorübergehend gesperrt oder endgültig widerrufen werden. Wobei die Sperre eine temporäre Aufhebung der Zertifikatsgültigkeit darstellt und im Unterschied zu einem Widerruf innerhalb einer 10-tägigen Frist wieder aufgehoben werden kann. Eine Sperre geht nach 10 Tagen automatisch in einen Widerruf über. Der Zertifikatsinhaber wird von einer erfolgten Sperre oder einem erfolgten Widerruf per E-Mail informiert.

Folgende Gründe führen zu einem Widerruf eines Zertifikats:

- Verlust oder Diebstahl des privaten Schlüssels (z.B. der Smartcard)
- QSCD (z.B. Smartcard) ist defekt und kann nicht mehr zur Signaturerstellung eingesetzt werden
- Kompromittierung des privaten Schlüssels
- Angaben im Zertifikat sind nicht mehr korrekt
- Schlüssel oder verwendete Algorithmen entsprechen nicht mehr den aktuellen Sicherheitsanforderungen
- Missbrauch durch Zertifikatsinhaber oder Dritte
- Gesetzliche Vorschriften
- Verstoß des Zertifikatsinhabers gegen die CP/CPS oder die Allgemeinen Geschäftsbedingungen des VDAs
- Vertragsverhältnis beendet
- VDA erlangt Kenntnis vom Ableben des Zertifikatsinhabers

Ein Widerruf kann von folgenden Personen und Institutionen initiiert werden:

- Zertifikatsinhaber oder eine andere Person, die das Widerrufspasswort kennt,
- Zertifikatsinhaber oder eine vertretungsbefugte Person, die den Umstand für einen Widerruf und seine Berechtigung für diesen glaubhaft machen kann (z.B. Berechtigung durch geeigneten Nachweis der Identität, Berechtigung im Falle des Ablebens des Zertifikatsinhabers),
- bei Zuordnung einer natürlichen Person zu einer Organisation, eine vertretungsbefugte natürliche Person der Organisation,
- bei Ausstellung eines Zertifikats einer juristischen Person, eine vertretungsbefugte natürliche Person der juristischen Person,
- der VDA selbst

Folgende Gründe führen zu einer Sperre eines Zertifikats:

- Verdacht auf Verlust oder Diebstahl des privaten Schlüssels (z.B. der Smartcard)
- Verdacht auf Defekt des QSCD (z.B. Smartcard)
- Verdacht auf Kompromittierung oder Missbrauch des privaten Schlüssels

Eine Sperrung kann von folgenden Personen und Institutionen veranlasst werden:

- Zertifikatsinhaber oder eine andere Person, die das Widerrufspasswort kennt,
- Zertifikatsinhaber oder eine vertretungsbefugte Person, die den Umstand für eine Sperre und seine Berechtigung für diese glaubhaft machen kann,
- bei Zuordnung zu einer Organisation, ein Vertretungsbefugter der Organisation,
- der VDA selbst.

Nur Personen, die das vereinbarte Sperraufhebungspasswort bzw. das Widerrufspasswort kennen, können die Sperre eines Zertifikats aufheben. Ein erfolgter Widerruf kann unter keinen Umständen aufgehoben werden und eine Re-Aktivierung des Zertifikats ist ausgeschlossen.

Im Falle einer Sperre enthält die Widerrufsliste das gesperrte Zertifikat bzw. aus der Antwort des OCSP Responders ist ersichtlich, dass das betroffene Zertifikat gesperrt ist. Nach Aufhebung einer Sperre wird das betroffene Zertifikat aus der Widerrufsliste entfernt und der OCSP Responder retourniert einen uneingeschränkten Zertifikatsstatus.

Der Zertifikatsinhaber ist verpflichtet unmittelbar nachdem dieser Kenntnis über den zur Sperre bzw. zum Widerruf führenden Umstand erlangt, die Sperre bzw. den Widerruf beim VDA durchzuführen.

Die Aktualisierung der Widerrufsstatusinformation erfolgt an Werktagen, ausgenommen Samstag, von 9 bis 17 Uhr spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes

bzw. Sperrgrundes. Außerhalb dieser Zeit längstens innerhalb von sechs Stunden. Der Widerrufsstatus ist mit seiner Veröffentlichung wirksam.

4.9 Abfragedienst zum Zertifikatsstatus

CA-Zertifikate

Beim Widerruf eines CA-Zertifikats erfolgt ein Eintrag in der Widerrufsliste für CA-Zertifikate (CARL). Diese wird mindestens einmal jährlich sowie im Anlassfall von der Root-CA ausgestellt. Im Falle der Verwendung von Cross-Zertifizierung erfolgt die Ausstellung einmal pro Monat.

Endbenutzerzertifikate

Bei einer erfolgten Sperrung oder bei Widerruf eines Zertifikats erfolgt ein Eintrag in der Widerrufsliste. Nach Aufhebung einer Sperrung wird die entsprechende Eintragung in der nächsten Widerrufsliste entfernt.

Die Widerrufsliste ist vom VDA elektronisch signiert. Statusinformationen sind auch nach Ablauf der zeitlichen Gültigkeit des Zertifikats über die Widerrufsliste verfügbar.

Die Veröffentlichung der aktualisierten Widerrufsliste erfolgt spätestens alle 3 Stunden und beinhaltet den geplanten Zeitpunkt der Veröffentlichung der nächsten Widerrufsliste. Eine aktualisierte Widerrufsliste kann auch bereits vor dem genannten Zeitpunkt veröffentlicht werden.

Im Falle von Systemdefekten, Servicearbeiten oder anderen Faktoren, die außerhalb dem Einflussbereich des VDA liegen, wurde ein Notfallszenario erstellt, um Widerrufe innerhalb der angegebenen Zeit durchführen zu können und um zu verhindern, dass Abfragedienste zum Zertifikatsstatus nicht länger als 3 Stunden nicht verfügbar sind. Für nähere Informationen siehe Abschnitt 5.7.

Eine Spezifikation der Widerrufsliste ist in Abschnitt 0 verfügbar.

Zusätzlich kann der Zertifikatsstatus über einen OCSP-Dienst abgefragt werden. Der öffentlich zugängliche OCSP-Responder des VDA ist rund um die Uhr verfügbar. Um die Authentizität der Statusantwort zu gewährleisten, werden Antworten des OCSP-Dienstes vom VDA signiert. Die Veröffentlichung von Sperr- und Widerrufsinformationen über OCSP erfolgt unmittelbar nach der Sperrung bzw. dem Widerruf.

Eine Schnittstellenspezifikation des OCSP-Dienstes ist in Abschnitt 7.3 verfügbar.

Spätestens alle 24 Stunden wird die für den OCSP-Dienst und für die Ausstellung der Widerrufsliste verwendete Uhrzeit mit einer vertrauenswürdigen Zeitquelle synchronisiert.

Der VDA ist bemüht sämtliche Methoden zur Abfrage des Widerrufsstatus konsistent zu halten. In Ausnahmefällen kann es zwischen Übernahme des Widerrufsgrundes im System und somit Übernahme des aktualisierten Status im OCSP-Dienst und Aktualisierung der Widerrufsliste für maximal 1 Stunde zu Abweichungen in der Widerrufsstatusinformation kommen.

Der VDA ist bemüht folgende Antwortzeiten einzuhalten:

- Widerrufslisten können unter normaler Netzauslastung innerhalb von 10 Sekunden über eine analoge Telefonleitung bezogen werden
- Widerrufsstatusinformationen werden vom OCSP-Responder unter normaler Netzauslastung innerhalb von 10 Sekunden über eine analoge Telefonleitung beantwortet

4.10 Abmeldung vom Vertrauensdienst

Die Gültigkeit eines Zertifikats endet spätestens mit dem im Zertifikat angegebenen Datum. Der Zertifikatsinhaber kann sich vor jedoch vor Ablauf der Gültigkeit vom Vertrauensdienst abmelden. Eine Abmeldung bedingt einen Widerruf der betroffenen Zertifikate.

4.11 Hinterlegung und Wiederherstellung von Schlüsseln

Private Schlüssel von qualifizierten Zertifikaten werden nicht hinterlegt und können daher nicht wiederhergestellt werden.

5 Nicht-technische Sicherheitsmaßnahmen

5.1 Bauliche Sicherheitsmaßnahmen

5.1.1 Standorte

Die für den Betrieb als qualifizierter Vertrauensdiensteanbieter notwendigen Dienstleistungen werden an folgenden Standorten und Örtlichkeiten erbracht:

TABELLE 3: DIENSTLEISTUNGEN UND STANDORTE

Dienstleistung	**Standorte**
Firmensitz	PrimeSign GmbH Wielandgasse 2 A-8010 Graz Niederlassung Wien: PrimeSign GmbH Franzosengraben 8 A-1030 Wien
Qualifiziertes Trustcenter	Raiffeisen Rechenzentrum GmbH Raiffeisen-Platz 1 A- 8074 Graz-Raaba Im qualifizierten Trustcenter werden die hochkritischen Aktivitäten, wie z.B. Zertifikatsgenerierung und die Bereitstellung von Widerrufstatusinformationen physisch gegen nicht autorisierten Zugriff geschützt ausgeführt.
Kartenproduktion	Die eingesetzten Smartcards werden am Standort des VDA personalisiert. Der VDA behält es sich vor, bei Bedarf die Personalisierung direkt vom Kartenhersteller oder durch qualifizierte Dienstleister bzw. Registration Authorities vornehmen zu lassen.
Call-Center	Immerwährend: Hotline der Cryptas Unternehmensgruppe

	CRYPTAS IT Security GmbH Franzosengraben 8 A-1030 Wien Bei Bedarf wird der telefonische Annahmedienst für den Sperr- und Widerrufsdienst an das zertifizierte Sicherheitscallcenter der Firma Securitas Sicherheitsdienstleistungen GmbH (Franzosengraben 8, A-1030 Wien), oder einen gleichwertigen Dienstleister, ausgelagert.

5.1.2 Zutritt

Das qualifizierte Trustcenter wird in einem [ISO 27001] und [ISO 20000] zertifizierten Rechenzentrum betrieben. Zusätzlich entspricht das Rechenzentrum der europäischen Norm [EN 50600] und deckt dadurch höchste Anforderungen hinsichtlich Gebäudesicherheit, Verfügbarkeit und Energieeffizienz ab. Das Rechenzentrum ist durch ein Außenbereichs- und Fassadensicherungssystem inkl. elektronischem Zutrittssystem und Videoüberwachung gesichert. Zusätzlich ist der Zutritt in den Hochsicherheitsbereich (in dem sich das Trustcenter befindet) nur mittels Vereinzelungsschleuse über eine 3-Faktor-Authentifizierung möglich. Die zutrittsberechtigten Personen müssen hierbei zuvor beim Betreiber des Rechenzentrums registriert und erfasst werden. Der Zutritt ist dabei täglich von 00:00 bis 24:00 gesichert. Über sämtliche Zutritte wird ein Protokoll vom Rechenzentrumsbetreiber geführt.

5.1.3 Stromversorgung und Klimatisierung

Das qualifizierte Trustcenter hat eine Stromversorgung und Klimatisierung internationalen Standards entsprechend. Das Rechenzentrum und das Trustcenter verfügen über eine redundante Stromversorgung inkl. Stromersatzversorgung.

Die Rechenzentrumsinfrastruktur beinhaltet eine redundant ausgelegte Klimaanlage zur Steuerung der Raumtemperatur und Luftfeuchtigkeit in den Serverräumen. Von Seiten des Rechenzentrumbetreibers wird eine Raumtemperatur von 22°C innerhalb der Kältegänge über einen Zeitraum von 24 Stunden bei 100% Leistung (wobei Temperaturschwankungen von +/- 10% möglich sind) zugesichert. Des Weiteren wird eine durchschnittliche relative Luftfeuchtigkeit von 50% innerhalb der Kältegänge über einen Zeitraum von 24 Stunden bei 100% Leistung mit möglichen Schwankungen +/- 10% gewährleistet.

5.1.4 Wasserschäden

Der Standort des qualifizierten Trustcenters ist durch angemessene bauliche Maßnahmen vor Wasserschäden geschützt. Der Standort befindet sich im Erdgeschoß eines separaten Gebäudes, das sich auf dem höchsten Punkt des Geländes befindet. Zusätzlich ist das Erdgeschoß um ca. 30cm erhöht.

5.1.5 Brandschutz

Das qualifizierte Trustcenter ist durch eine hochsensible Brandfrüherkennungsanlage gesichert und besitzt eine Direktalarmleitung zu den lokalen Einsatzkräften. Zusätzlich ist eine Stickstofflöschanlage installiert. Auch gelten im gesamten Rechenzentrum eigene Richtlinien zur Vorsorge von Bränden.

5.1.6 Aufbewahrung von Datenträgern

Datenträger, die kritische Informationen beinhalten – wie beispielsweise Backups – werden in vor Wasser und Brand geschützten Räumen oder Tresoren aufbewahrt und gegen unbefugten Zugriff gesichert.

5.1.7 Abfallentsorgung

Sämtliche Daten (auf elektronischen Datenträgern, auf Papier, etc.) werden fachgerecht vernichtet (d.h. physikalisch unbrauchbar gemacht) und entsorgt.

5.1.8 Redundante Auslegung

Das qualifizierte Trustcenter ist dem aktuellen technischen Stand entsprechend redundant ausgelegt um eine Hochverfügbarkeit für einen 24x7 Betrieb zu gewährleisten.

5.2 Verfahrensvorschriften

5.2.1 Rollen und Aufgaben

Im folgenden Abschnitt werden die unterschiedlichen Rollen beschrieben. Es erfolgt eine Auflistung der den jeweiligen Rollen zugeordneten Tätigkeiten und Verantwortlichkeiten.

Abbildung 4 illustriert die für den Betrieb der vom VDA angebotenen Dienste notwendigen Rollen.

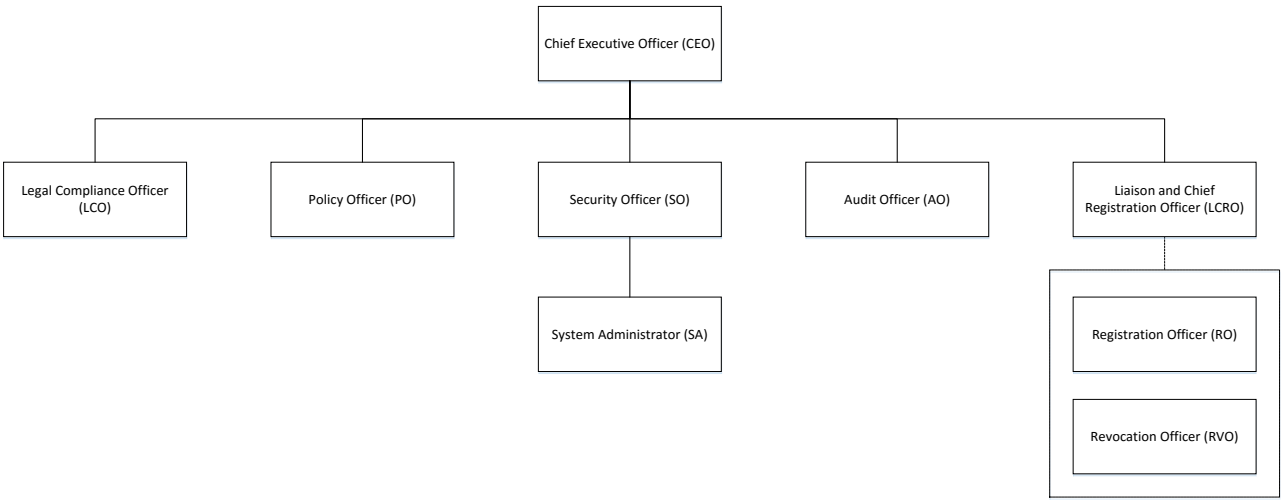

ABBILDUNG 4: ROLLEN IM BETRIEB DES VDA

Die Registrierung also auch Annahme von Anträgen auf Widerruf und Sperre kann bei Bedarf an geeignete Erfüllungsgehilfen delegiert werden, sofern sowohl organisatorisch als auch vertraglich sichergestellt ist, dass die notwendigen Sicherheitsanforderungen vom Erfüllungsgehilfen erfüllt werden und die eingesetzten Mitarbeiter des Erfüllungsgehilfen über die notwendige Qualifizierung verfügen (siehe Abschnitt 5.3).

Alle weiteren Rollen werden von Mitarbeitern des VDA oder Mitarbeitern von verbundenen Unternehmen, bzw. an von diesen beauftragte und entsprechend qualifizierte Dienstleister, eingenommen.

In Tabelle 4 werden die generellen Tätigkeitsfelder der einzelnen Rollen aufgelistet.

TABELLE 4: ROLLEN UND AUFGABENGEBIETE

Rolle	**Aufgaben**
Chief Executive Officer (CEO)	Unternehmensleitung Marketing und vertriebliche Leitung Rechtliche und finanzielle Tätigkeiten Schnittstelle zur Aufsichtsbehörde Zugang zum Hochsicherheitsbereich des Rechenzentrums
Legal Compliance Officer (LCO)	Rechtliche Tätigkeiten Vertragsrecht

	Laufende Prüfung der Einhaltung der gesetzlichen Anforderungen
Policy Officer (PO)	Definition der Sicherheitsanforderungen Durchführung von Schulungen Sicherheitsüberprüfungen der Mitarbeiter Vergabe von RO und RVO Berechtigungen Überprüfung der Einhaltung von Datenschutzbestimmungen
Security Officer (SO)	Analyse der Hardware- und Softwareanforderungen Beschaffungsprozesse Konzeptionierungstätigkeiten Zugang zum Hochsicherheitsbereich des Rechenzentrums Verwaltung der HSMs Austausch von Hardware- und Softwarekomponenten Wiederherstellung von Backups
Audit Officer (AO)	Durchführung interner Audits Prüfung der Einhaltung der Sicherheitsbestimmungen und gesetzlichen Anforderungen
Liaison and Chief Registration Officer (LCRO)	Kontakt zu anderen Unternehmen bzw. Erfüllungsgehilfen Schulung RO und RVO
System Administrator (SA)	Laufende Systembetreuung z.B. Neustart von Diensten Bereitschaftsdienst Monitoring Erstellung von Backups im laufenden Betrieb

Registration Officer (RO)	Mitarbeiter in der Registrierungsstelle Entgegennahme von Zertifikatsanträgen Registrierung und Authentifizierung von Zertifikatserwerbern Belehrung der Zertifikatserwerber Authentifizierung von Zertifikatsinhabern für die Durchführung von Sperre, Widerruf oder Aufhebung einer Sperre jeweils ohne Wissen des dazugehörigen Passwortes
Revocation Officer (RVO)	Mitarbeiter im Widerrufsdienst Annahme von Anträgen auf Sperre, Widerruf oder Aufhebung einer Sperre Durchführung von Widerruf und Sperre nur bei bekanntem Widerrufs- bzw. Sperraufhebungspasswortes

Mitarbeiter der Rollen CEO und SO verfügen über permanenten Zugang zum Hochsicherheitsbereich des Rechenzentrums.

Mitarbeiter der Rolle SA verfügen über eingeschränkten Remote-Zugang zum Produktivsystem des VDA. Diese können im Bedarfsfall Dienste des VDA neustarten, verfügen jedoch nicht über die Berechtigung Konfigurationen der Dienste zu modifizieren oder selbständig Zertifikate auszustellen.

Mitarbeiter der Rollen RO und RVO können auf interne Dienste des VDA, wie beispielsweise das Registrierungssystem oder das System zur Initiierung einer Sperre oder eines Widerrufs zugreifen, verfügen aber über keinen Remote-Zugang zum Produktivsystem des VDA.

5.2.2 Rollentrennung

Mitarbeiter der Rolle AO sind nicht in den laufenden Betrieb des VDA eingebunden und wirken nicht an der Konzeptionierung und der Definition der Sicherheitsanforderungen des VDA mit. Mitarbeiter der Rolle AO sind für die Überprüfung der Einhaltung der Sicherheitsbestimmungen im Zuge interner Audits zuständig. Für die Dauer der Audits handeln diese nicht weisungsgebunden. Diese können im Rahmen des Audits für eine beschränkte zeitliche Dauer Zugang zum Hochsicherheitsbereich des Rechenzentrums und insbesondere auch zum Produktivsystem, sowie zu sämtlichen Protokolldaten des VDA erhalten.

5.2.3 Tätigkeiten

Nachfolgende Tabellen bieten eine Übersicht über die im Betrieb des VDA anfallenden Tätigkeiten und die dazu erforderlichen Rollen. Es erfolgt eine Unterscheidung in hochkritische und allgemeine Tätigkeiten. Die Durchführung hochkritischer Tätigkeiten erfordert immer das Vieraugenprinzip.

TABELLE 5: HOCHKRITISCHE TÄTIGKEITEN

Tätigkeit	**Zugelassene Rollen**
Generierung, Löschung und Anwendung von Root-CA Schlüsselmaterial	SO, CEO (Vieraugenprinzip mit mind. 1 CEO)
Ausstellung von CA-Zertifikaten	SO, CEO (Vieraugenprinzip mit mind. 1 CEO)
Widerruf von CA-Zertifikaten	SO, CEO (Vieraugenprinzip mit mind. 1 CEO)
Anfertigung einer Sicherung der Schlüssel der HSM im Backup-HSM	SO, CEO (Vieraugenprinzip)
Wiederherstellung von Schlüsselmaterial aus dem Backup-HSM	SO, CEO (Vieraugenprinzip)
Austausch der HSM	SO, CEO (Vieraugenprinzip)
Austausch von Hardware- (ausgenommen HSM) und Softwarekomponenten	SO, SA (Vieraugenprinzip mit mind. 1 SO)

Es können verschlüsselte Sicherungen der privaten Schlüssel des HSM (Wurzelschlüsselpaar, CA-Schlüsselpaar) in einer eigens dafür ausgelegten und vom Hersteller dafür konzipierten Backup-HSM angelegt werden. Diese Backup-HSM wird nach Bespielen mit dem verschlüsselten privaten Schlüsselmaterial des HSMs in einem weiteren Standort (off-site) in einem Tresor bzw. Bankschließfach verwahrt. Lediglich Mitarbeiter der Rolle CEO verfügen über Zugriff auf diesen Tresor bzw. das Bankschließfach.

TABLE 6: ALLGEMEINE TÄTIGKEITEN

Tätigkeit	**Zugelassene Rollen**
Generierung und Löschung von CA-Schlüsselmaterial	SO
Vergabe von RO und RVO Berechtigungen	PO

Starten und Stoppen von VDA-Diensten (z.B. Verzeichnisdienst und Widerrufsstatusdienst)	SO, SA
Zugriff auf Protokollierungen im laufenden Betrieb	SO, SA
Monitoring von Protokollierungen auf verdächtige Aktivitäten	SO, SA
Zugriff auf Protokollierungen in der Sicherung	SO
Durchführung von Softwareaktualisierungen	SO
Änderung von Konfigurationen im Produktivsystem	SO
Registrierung und Authentifizierung von Zertifikatserwerbern	RO
Ausstellung von Endbenutzerzertifikaten	RO
Sperre und Widerruf von Endanwenderzertifikaten	RO, RVO
Sperraufhebung	RO, RVO
Widerruf ohne Widerrufspasswort	RO
Aufhebung einer Sperre ohne Sperraufhebungspasswort	RO

5.3 Personelle Sicherheitsvorkehrungen

5.3.1 Anforderungen an das Personal

Das Personal des VDA und auch das Personal von verbundenen Unternehmen bzw. qualifizierten externen Dienstleistern, sofern Personal von verbundenen Unternehmen oder externen Dienstleistern zur Rollen- und Leistungserfüllung herangezogen werden, verfügen über folgende Qualifikationen und Eigenschaften (jeweils entsprechend ihrer zugedachten Rolle):

- Vertrauenswürdigkeit und Integrität
- Zuverlässigkeit und Fachwissen insbesondere in den Bereichen
    - Allgemeine EDV-Ausbildung

- Sicherheitstechnologie, Kryptographie, elektronische Signatur und Public Key Infrastructure
- Technische Normen, insbesondere Evaluierungsnormen
- Hard- und Software
- Vorschriften für die Sicherheit und den Schutz personenbezogener Daten
- Anwendung von Verwaltungs- und Managementverfahren

5.3.2 Sicherheitsüberprüfung des Personals

Das Personal des VDA und auch das Personal von verbundenen Unternehmen bzw. qualifizierten externen Dienstleistern, sofern Personal von verbundenen Unternehmen oder externen Dienstleistern zur Rollen- und Leistungserfüllung herangezogen werden, ist zuverlässig. Die Zuverlässigkeit ist jedenfalls nicht gegeben, wenn eine Person:

- wegen einer mit Vorsatz begangenen strafbaren Handlung zu einer Freiheitsstrafe von mehr als einem Jahr, oder
- wegen strafbarer Handlungen gegen das Vermögen, oder
- gegen die Zuverlässigkeit von Urkunden und Beweiszeichen zu einer Freiheitsstrafe von mehr als drei Monaten verurteilt wurde.

Verurteilungen, die nach den Bestimmungen des Tilgungsgesetzes 1972 getilgt sind oder der beschränkten Auskunft unterliegen, bleiben außer Betracht.

Der VDA überprüft die Zuverlässigkeit gegebenenfalls bzw. bei Bedarf mittels eines Strafregisterauszugs oder anderen geeigneten Mitteln bzw. Verfahren.

Die Registrierung also auch Annahme von Anträgen auf Widerruf und Sperre kann bei Bedarf an Erfüllungsgehilfen delegiert werden, Regelungen für die Sicherheitsüberprüfung des Personals gelten auch für die für den VDA eingesetzten Mitarbeiter des Erfüllungsgehilfen.

5.3.3 Anforderungen an die Schulung

Vor der Aufnahme einer Tätigkeit werden die Mitarbeiter ausreichend geschult. Diese Schulung ist auf die zugedachte Rolle des Mitarbeiters zugeschnitten und umfasst neben der Schulung der konkreten Tätigkeit insbesondere die Sensibilisierung für die erhöhte Sicherheitsrelevanz eines qualifizierten Vertrauensdienstes. Erst nach erfolgter Schulung kann der Mitarbeiter die entsprechen Rolle einnehmen und ausüben.

Im laufenden Betrieb werden die Kenntnisse der Mitarbeiter beurteilt und gegebenenfalls entsprechende Nachschulungen veranlasst.

5.3.4 Wiederholung der Schulung

Schulungen werden regelmäßig wiederholt. Zusätzlich kann eine Zusatz-Schulung bei Bedarf angeordnet werden.

Eine Wiederholung von Schulungen findet jedenfalls statt, wenn sich gravierende Änderungen im Bereich der jeweiligen Rolle ergeben (z.B.: Einführung neuer Software, Einrichtung neuer Hardware, etc.).

5.3.5 Job-Rotationen

Aufgrund der in Abschnitt 5.2 definierten Trennung von Rollen und Aufgaben, der Einhaltung des Vier-Augen-Prinzips für sicherheitskritische Tätigkeiten sowie Stellvertreterregelungen ist eine regelmäßige Job-Rotation nicht erforderlich.

5.3.6 Sanktionen bei unzulässigen Handlungen

Für den Fall, dass sich ein Mitarbeiter des VDA Anweisungen oder Vorschriften widersetzt, werden geeignete und angemessene Maßnahmen zur Verhinderung weiterer Vergehen gesetzt. Bei wiederholten oder schweren Vergehen umfassen diese Maßnahmen auch arbeits- und strafrechtliche Konsequenzen.

5.3.7 Vertragsbedingungen mit dem Personal

Der VDA verpflichtet sein Personal auf die Einhaltung der Anweisungen, Vorschriften und gesetzlichen Bestimmungen. Insbesondere sind die Mitarbeiter verpflichtet personenbezogene Daten vertraulich zu behandeln.

Der VDA behält sich vor, stichprobenartige Prüfungen durchzuführen (bspw. eine Prüfung der korrekten Registrierung eines Zertifikatserwerbers, d.h. ob eine korrekte Prüfung der Identitätsunterlagen und anderer Nachweise durch den RO durchgeführt wurde).

5.4 Protokollierung und Überwachungsmaßnahmen

5.4.1 Ereignisprotokolle

Die Vertraulichkeit und Integrität von Ereignisprotokollen wird entsprechend sichergestellt. Sämtliche Aufzeichnungen aus dem laufenden Betrieb werden vollständig archiviert.

Aufzeichnungen zum laufenden Betrieb können im Rahmen von Gerichtsverfahren zu Verfügung gestellt werden, falls dies dem Nachweis des einwandfreien Betriebs des Vertrauensdienstes dient.

Jedes protokollierte Ereignis wird mit Datum und Uhrzeit versehen sowie gegebenenfalls die durchführende Person mit angeführt. Die genaue Uhrzeit wird durch Verwendung einer vertrauenswürdigen Zeitquelle sichergestellt. Die Synchronisation der Zeit erfolgt täglich.

Generell werden folgende Ereignisgruppen protokolliert:

- Sicherheitsrelevante Ereignisse, wie System StartUp und Shutdown, Systemabstürze, Hardware Fehler, Firewall spezifische Ereignisse sowie Zugriffsversuche
- Ereignisse in Bezug auf Registrierung
    - Antrag für Zertifizierungen

  - Dokumente, die vom Antragsteller zu Verfügung gestellt werden
  - Aufzeichnungen zu Dokumenten, die der Antragsteller zwecks eindeutiger Identifizierung vorlegt
  - Unterzeichneter Signaturvertrag
  - Identität der Stelle, die den Zertifizierungsantrag annimmt
  - Name der Registrierungsstelle
- Ereignisse in Bezug auf die Zertifikatserstellung
  - Ereignisse den Lebenszyklus der CA-Schlüssel betreffend
  - Ereignisse den Lebenszyklus der Zertifikate betreffend
  - Ereignisse den Lebenszyklus sämtlicher Schlüssel, die von der CA verwaltet oder erstellt wurden, betreffend
- Ereignisse in Bezug auf das Widerrufsmanagement, d.h. sämtliche Anträge und Berichte die zum Widerruf von Zertifikaten führen
- Sämtliche Ereignisse die Vorbereitung von QSCDs betreffend
- Alle relevanten Informationen über Daten, die erhalten oder veröffentliche werden.

Informationen werden, soweit erforderlich, über die Einstellung der Tätigkeit des Vertrauensdienstes hinaus aufbewahrt. Hierbei handelt es sich um Informationen die zur späteren Überprüfung, z.B. in Gerichtsverfahren, erforderlich sind.

Die Aufzeichnung erfolgt auf eine Art und Weise, sodass sichergestellt ist, dass diese nicht leicht gelöscht oder zerstört (absichtlich oder versehentlich) werden können.

5.5 Archivierung von Aufzeichnungen

Der VDA archiviert:

- Aufzeichnung sämtlicher Ereignisse, die den Lebenszyklus der von der CA verwalteten bzw. ausgestellten Schlüssel betreffen;
- Aufzeichnungen von Informationen, die sich aus dem Registrierungsprozess ergeben (siehe Abschnitt 4.3).

Die Aufbewahrungszeit des Archivs beträgt mindestens 30 Jahre nach Ablauf der Gültigkeit der Zertifikate oder mangels eines solchen 30 Jahre ab dem Zeitpunkt des Anfallens von einschlägigen Informationen.

Zugriff auf das Archiv ist entsprechend dem Rollenkonzept (siehe Abschnitt 5.2) geregelt.

5.6 Schlüsselwechsel (CA und Root-Schlüssel)

Der VDA führt einen Schlüsselwechsel stets in Form der Generierung eines neuen Schlüsselpaars in Verbindung mit der Neuausstellung des betroffenen Zertifikats durch (siehe auch Abschnitt 4.5 ff), dies betrifft CA und Root-CA Schlüssel gleichermaßen wie Benutzerzertifikate.

Ein Schlüsselwechsel ist erforderlich falls das betroffene Zertifikat widerrufen wurde, dessen Gültigkeit abgelaufen, der Schlüssel kompromittiert oder zugrundeliegende Algorithmen und Parameter nicht mehr den technischen Anforderungen genügen.

Nach dem Schlüsselwechsel eines CA oder Root-CA werden keine weiteren Zertifizierungen mehr mit dem alten Schlüsselpaar durchgeführt.

5.7 Kompromittierung und Notfallsplan

5.7.1 Monitoring

Zugriffe auf bzw. Benutzung von System-Komponenten sowie Service Anfragen werden überwacht, wobei sensible Informationen berücksichtigt werden. Audit-Logs werden überwacht um verdächtige oder bösartige Vorgänge zu erkennen.

Ungewöhnliche Aktivitäten, die auf eine potentielle Sicherheitsverletzung hindeuten, werden erkannt und als Alarme gemeldet.

Der VDA überwacht das Starten und Stoppen der Monitoringfunktion sowie die Verfügbarkeit und Benutzung erforderlicher Netzwerkdienste.

5.7.2 Benachrichtigungen

Der VDA reagiert zeitnah auf erkannte Vorfälle, um deren Auswirkungen zu minimieren. Entsprechend geeignetes Personal, um auf sicherheitsrelevante Alarme zu reagieren, steht zu Verfügung (siehe Rollenkonzept in Abschnitt 5.2).

Der VDA wird einschlägige Stellen (z.B. die Aufsichtsbehörde) im Falle einer Sicherheitsverletzung oder eines Integritätsverlusts, die eine signifikante Auswirkung auf den VDA oder den darin vorhandenen personenbezogenen Daten darstellen, innerhalb von 24 Stunden nach Kenntnisnahme darüber informieren.

Sollte eine Sicherheitsverletzung nachteilige Auswirkung auf natürliche oder juristische Personen als Nutzer des VDA haben, werden diese umgehend über den Vorfall informiert.

5.7.3 Schwachstellen

Der VDA reagiert auf kritische Schwachstellen innerhalb von 48 Stunden nach deren Feststellung.

Falls es unter Berücksichtigung eventueller Auswirkungen der Schwachstelle kosteneffektiv möglich ist, wird ein Konzept entwickelt und umgesetzt, um die jeweilige Schwachstelle zu minimieren oder

zu beheben. Falls sich das Beseitigen einer Schwachstelle als nicht erforderlich erweist, wird dies entsprechend argumentiert und dokumentiert.

Sämtliche Abläufe werden mit dem Ziel errichtet, Auswirkungen und Schäden aufgrund von Sicherheitsverletzungen und Fehlfunktionen, zu minimieren.

5.7.4 Business Continuity

Der VDA hat einen Notfallsplan, um den Betrieb bei Eintreten eines Störfalls (Kompromittierung privater Schlüssel, Sicherheitsverletzungen, Hardwaredefekt) zeitnah wieder aufnehmen zu können. Ursachen des Störfalls werden mit geeigneten Maßnahmen bereinigt.

5.7.5 Datensicherung

Daten, die zur Wiederherstellung des Betriebs nach einem Störfall erforderlich wären, werden gesichert und sicher derart verwahrt, dass die Wiederaufnahme des Betriebs zeitnah möglich ist.

Die Datensicherung findet in regelmäßigen Abständen statt, wobei sichergestellt wird, dass alle relevanten Daten bzw. Software nach einem Störfall wiederhergestellt werden können. Dieses Szenario wird regelmäßig getestet.

Die Datensicherung bzw. die Wiederherstellung von Daten aus einer Sicherung erfolgt durch Personen mit entsprechender Rolle (siehe Rollenkonzept in Abschnitt 5.2).

5.7.6 Kompromittierung von Schlüsseln

Ein Notfallsplan berücksichtigt Kompromittierung, Verlust oder mögliche Kompromittierung von privaten Schlüsseln des VDA und sieht dazu entsprechende Prozesse vor.

5.7.7 Kompromittierung von Algorithmen

Falls sich einer der verwendeten Algorithmen bzw. ein dazugehöriger Parameter für die angedachte verbleibende Nutzungszeit als unzureichend erweisen sollte, dann wird der VDA sämtliche Betroffenen informieren und entsprechende Widerrufe sämtlicher betroffenen Zertifikate planen.

5.8 Einstellung der Tätigkeit

Stellt der VDA seine Tätigkeit ein, so wird sichergestellt, dass die Beeinträchtigung betroffener Dienste bzw. vertrauender Dritte minimiert wird. Der VDA entwickelt einen geeigneten Beendigungsplan, der regelmäßig aktualisiert wird.

Weitere Details sind im Dokument Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung [TP] beschrieben.

6 Technische Sicherheitsmaßnahmen

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 CA-Schlüssel

Die Erstellung des Wurzelschlüsselpaares (Root-Key) sowie der CA-Schlüsselpaare, bzw. allgemein die Erstellung aller Schlüsselpaare des VDA, die auch zur Ausstellung von Subordinate-CAs sowie auch zur Erstellung von Endbenutzerzertifikaten herangezogen werden, erfolgt innerhalb des Hochsicherheitsbereichs des Rechenzentrums im HSM durch autorisiertes Personal anhand des Vieraugenprinzips (Schlüsselerstellungszeremonie; siehe [TP]). Siehe Abschnitt 5.1 und 5.3 für nähere Infos bezüglich baulichen und personellen Sicherheitsanforderungen.

Abschnitt 6.5.1 beschreibt den Prozess und die Sicherheitsanforderungen für die Ausstellung von CA-Zertifikaten. Sämtliche Anforderungen gelten auch für die erstmalige Erstellung des Root-CA Schlüsselmaterials.

Die HSMs zur Generierung und Speicherung von Root- und CA-Schlüsseln, sowie die zur Ausstellung von Endbenutzerzertifikaten eingesetzten HSMs, sind nach Common Criteria (oder auf Grundlage eines gleichwertigen Standards; die Gleichwertigkeit wird ggf. durch eine entsprechende Bestätigung nachgewiesen) vor dem Hintergrund der jeweils geltenden rechtlichen und technischen Bestimmungen sicherheitszertifiziert und erfüllen die darin geforderten Sicherheitskriterien (Sicherheitskriterien formuliert bspw. durch standardisierte Schutzprofile, wie etwa dem Common Criteria Schutzprofil PP/0308 Cryptographic Module for CSP Signing Operations with Backup Protection Profile, Version 0.28 (27. Oktober 2003) [CC], oder dessen Nachfolger).

Die verwendeten HSMs (Hersteller, Typ, Version, Firmware, etc.) sowie deren Zertifizierungen und die diesen Zertifizierungen zu Grunde gelegten Schutzprofilen bzw. Sicherheitszielen werden ist im nicht öffentlich zugänglichen Dokument Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung [TP] des VDA ausgewiesen.

Die eingesetzten Algorithmen und Schlüssellängen entsprechen den zum Zeitpunkt der Erstellung geltenden Anforderungen der Aufsichtsbehörde und beachten nationale als auch internationale Empfehlungen (z.B. [ETSI TS 119 312]).

Der VDA stellt sicher, dass ausreichend vor Ablauf der zeitlichen Gültigkeit von CA-Zertifikaten (sowohl Root als auch Subordinate-CAs) neue CA-Zertifikate mit neuem Schlüsselmaterial ausgestellt werden.

6.1.2 Schlüssel für Endbenutzerzertifikate

QSCD auf Basis eines Signaturtokens (Smartcard)

Die Generierung der Schlüssel erfolgt im Signaturtoken (QSCD, wie bspw. Smartcard) selbst und der private Schlüssel verlässt niemals den Signaturtoken (z.B. Smartcard). Eingesetzte Signaturtoken

erfüllen die Sicherheitsanforderungen und Zertifizierungen für QSCD gemäß Verordnung (EU) 910/2014 [EIDAS] (Anhang II) bzw. Durchführungsbeschluss 2016/650 [EIDAS DB]. Es wird sichergestellt, dass der im Zertifikat hinterlegte öffentliche Schlüssel zum in der Smartcard gespeicherten privaten Schlüssel gehört.

Die eingesetzten Algorithmen und Schlüssellängen entsprechen den zum Zeitpunkt der Erstellung geltenden Anforderungen der Aufsichtsbehörde und beachten nationale als auch internationale Empfehlungen (z.B. [ETSI TS 119 312]). Der VDA überprüft im Zuge des internen Audits, ob sich der Zertifizierungsstatus der als QSCD verwendeten Signaturtokens (Smartcards) geändert hat. Im Falle einer Statusänderung erfolgt ein Austausch der Karten mit der Erzeugung von neuem Schlüsselmaterial.

QSCD bei VDA (Remote Signing)

Im Falle von Remote Signing erfolgt die Generierung von Schlüsselmaterial innerhalb des HSMs des Remote Signing Devices (QSCD). Private Schlüssel werden ausschließlich verschlüsselt aus diesem HSM exportiert und sicher verwahrt. Eine Verwendung des Schlüsselmaterials ist nur innerhalb des HSMs möglich.

Im Falle von Remote Signing erfolgt der Einsatz eines QSCD gemäß Verordnung (EU) 910/2014 [EIDAS].

Die eingesetzten Algorithmen und Schlüssellängen entsprechen den zum Zeitpunkt der Erstellung geltenden Anforderungen der Aufsichtsbehörde und beachten nationale als auch internationale Empfehlungen (z.B. [ETSI TS 119 312]).

6.2 Schutz der privaten Schlüssel

6.2.1 CA-Schlüssel

CA-Schlüssel werden nur innerhalb der HSM verwendet. Es kommen zwei redundante HSMs im Rechenzentrum zum Einsatz. Zusätzlich existiert ein entsprechend kryptographisch gesichertes Backup von CA-Schlüsselmaterial in einem Backup-HSM. Das Backup-HSM wird an einem anderen Standort sicher in einem Tresor verwahrt. Lediglich Personen der Rolle CEO haben Zugriff auf den Tresor (siehe Rollenkonzept Abschnitt 5.2).

Siehe Abschnitt 6.1 für eine Auflistung der erfüllten Zertifizierungen.

Bei Einstellung der Tätigkeit des VDA werden die CA Schlüssel im Rahmen des Beendigungskonzeptes sicher vernichtet.

6.2.2 Schlüssel für Endbenutzerzertifikate

QSCD auf Basis eines Signaturtokens (Smartcard)

Das Schlüsselmaterial wird innerhalb des Signaturtoken (Smartcard) generiert, wobei private Schlüssel nicht exportiert werden können. Es erfolgt kein Schlüssel Backup durch den VDA. Ein Auslesen des privaten Schlüssels aus dem Signaturtoken (Smartcard) ist nicht möglich. Eine Benutzung des privaten Schlüssels kann nur durch die korrekte Eingabe der vom Zertifikatsinhaber gewählten PIN erfolgen. Die PIN ist nur dem Zertifikatsinhaber bekannt.

QSCD bei VDA (Remote Signing)

Das Schlüsselmaterial wird innerhalb des HSMs des Remote-Signing-Device (QSCD) generiert und zur Speicherung verschlüsselt aus dem HSM exportiert. Es ist technisch sichergestellt, dass nur das HSM die exportierten Schlüssel entschlüsseln kann. Damit kann eine Verwendung des privaten Schlüsselmaterials zur Signaturerstellung nur innerhalb des HSMs erfolgen. Weiters kann die Benutzung des privaten Schlüssels nur durch die korrekte Eingabe der vom Zertifikatsinhaber gewählten PIN erfolgen. Die PIN ist nur dem Zertifikatsinhaber bekannt.

6.3 Andere Aspekte des Schlüsselpaar-Managements

Wurzel-Schlüssel werden nur zum Ausstellen von CA-Zertifikaten, Subordinate-CA-Zertifikaten oder Widerrufsinformationen bezüglich CA-Zertifikaten herangezogen. CA-Schlüssel werden lediglich zum Signieren von Endanwender Zertifikaten, Widerrufslisten und der OCSP Antwort verwendet. Das Attribut keyUsage enthält lediglich die Verwendungszwecke keyCertSign (Signieren von Zertifikaten) und crlSign (Signieren von Widerrufslisten). Es wird derselbe Schlüssel zum Signieren der Widerrufsliste und der Antworten des OCSP Responders verwendet. Die Signaturerstellung erfolgt innerhalb der HSMs im gesicherten Bereich des Rechenzentrums. Eine Verwendung der CA-Schlüssel erfolgt weiters ausschließlich innerhalb der zeitlichen Gültigkeit der damit verbundenen Root bzw. Intermediate Zertifikaten.

Nach Ablauf der zeitlichen Gültigkeit der CA-Schlüssel werden diese in allen verwendeten HSMs sicher vernichtet.

Schlüssel für Endbenutzerzertifikate dienen lediglich zur Signaturerstellung. Das Attribut *keyUsage* enthält die Verwendungszwecke *digitalSignature* und *nonRepudiation*.

Sämtliche eingesetzte Algorithmen und Schlüssellängen entsprechen den zum Zeitpunkt der Erstellung Stand der Technik und den geltenden Anforderungen der Aufsichtsbehörde und beachten sowohl nationale als auch internationale Empfehlungen (z.B. [ETSI TS 119 312]).

6.4 Aktivierungsdaten

6.4.1 CA-Schlüssel

Generierung von Schlüsselmaterial für Wurzel-/CA-Zertifikate erfolgt anhand des Vieraugenprinzips durch mindestens zwei autorisierte Mitarbeiter des VDA (siehe Rollenkonzept Abschnitt 5.2). Abschnitt 6.5.1 beschreibt den Prozess zur Verwendung des privaten Root-CA Schlüssels. Die

Mitarbeiter, die über die Aktivierungsdaten für den Root-CA-Schlüssel der Zertifizierungsstelle verfügen, verpflichten sich diese geheim zu halten (PIN) und sicher aufzubewahren (Hardware-Token).

Die Verwendung des privaten Schlüssels der Subordinate-CA erfolgt im Zuge der Ausstellung von Endbenutzerzertifikaten. Lediglich Mitarbeiter der Rolle RO können eine Zertifikatsausstellung initiieren. Diese müssen sich für die Initiierung dieser mittels Mehrfaktorauthentifizierung am Registrierungssystem des VDA authentifizieren.

6.4.2 Schlüssel für Endbenutzerzertifikate

QSCD auf Basis eines Signaturtokens (Smartcard)

Der Einsatz des privaten Schlüssels wird durch eine persönliche PIN geschützt. Die Zertifikatsinhaber wählen die PIN selbst. Die PIN ist niemand anderem als dem Zertifikatsinhaber bekannt und vom Zertifikatsinhaber unbedingt entsprechend geheim zu halten. Der Signaturtoken (Smartcard) verhindert das Auslesen der PIN.

QSCD bei VDA (Remote Signing)

Der Einsatz des privaten Schlüssels wird über ein Passwort (bzw. ggf. eine PIN) und mindestens einem weiteren Faktor abgesichert. Die Zertifikatsinhaber wählen das Passwort selbst. Das Passwort ist niemand anderem als dem Zertifikatsinhaber bekannt und vom Zertifikatsinhaber unbedingt entsprechend geheim zu halten. Das Passwort ist nicht im System des VDA gespeichert.

6.5 Sicherheitsvorkehrungen in den Computersystemen

Der Betrieb der eingesetzten HSMs, sowie Rechner mit den für den Betrieb der vom VDA angebotenen Dienste notwendigen Softwarekomponenten erfolgt im Hochsicherheitsbereich des Rechenzentrums. Für eine nähere Beschreibung zu den Sicherheitsvorkehrungen des Rechenzentrums siehe Abschnitt 5.1.

Der VDA verfügt über ein Konzept zur Trennung von den zum Einsatz kommenden Hardware- und Softwarekomponenten in unterschiedliche Sicherheitszonen. Dabei erfolgt sowohl eine Trennung auf Netzwerkebene als auch durch Virtualisierung.

Es kommt nur Software zum Einsatz, die für die Verwendung in Rechenzentren vorgesehen ist. Auf den eingesetzten Rechnern laufen lediglich Softwarekomponenten, die für den Betrieb der vom VDA angebotenen Dienste notwendig sind. Sämtliche Systeme sind redundant ausgelegt, um im Falle eines Ausfalls die Verfügbarkeit von Widerrufsstatusinformationen zu gewährleisten und eine zeitnahe Wiederaufnahme der Komponenten zur Ausstellung von Zertifikaten zu ermöglichen.

Die auf den Rechnern eingesetzten Betriebssysteme erfordern eine Authentifizierung des Benutzers. Für die Administration der Softwarekomponenten sowie für den Zugriff auf bestimmte Schnittstellen ist weiters eine VPN Verbindung notwendig. Konten für die VPN Verbindungen sind Mitarbeitern der Rolle SO und SA (siehe Rollenkonzept Abschnitt 5.2) persönlich zugeordnet. Wobei Mitarbeiter der Rolle SA lediglich über eingeschränkten Zugriff aufs System verfügen. Sicherheitskritische Softwarekomponenten z.B. für die Ausstellung oder den Widerruf von Zertifikaten erfordern eine Mehrfaktorauthentifizierung von Benutzern der Rolle RO bzw. RVO. Abschnitt 6.5.1 bis Abschnitt 6.5.3 behandeln die zusätzlichen Sicherheitsvorkehrungen für die sicherheitskritischen Prozesse *Generierung von Zertifikaten*, *Verwaltung von Zertifikaten* und initiieren des *Widerrufs*.

Es erfolgt eine regelmäßige Sicherung der für den Betrieb notwendigen Daten und den Daten der Zertifikatsinhaber. Sämtliche Daten werden verschlüsselt abgelegt. Der zur Entschlüsselung notwendige Schlüssel ist unter alleiniger Kontrolle der Mitarbeiter des VDA mit der Rolle SO. Zur Sicherstellung des Betriebs wird die Verwendbarkeit der gesicherten Daten im Zuge des internen Audits strichprobenartig überprüft.

Im Zuge der internen Audits erfolgt die Überprüfung der eingesetzten technischen Komponenten und deren Konfiguration auf Konformität mit den sich aus diesem Dokument und den gesetzlichen Regelungen ergebenen Anforderungen. Diese inkludiert eine Überprüfung der Hardwarekomponenten auf Defekte.

Eine nähere Beschreibung zur Aufteilung in Sicherheitszonen sowie zur Benutzerauthentifizierung und Zugriffskontrolle ist im nicht öffentlich zugänglichen Dokument Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung [TP] des VDA zu finden. Dieses kann von Aufsichtsbehörden bei allfälligen Prüftätigkeiten sowie bei begründetem Interesse auch durch Dritte in den relevanten Teilen eingesehen werden.

6.5.1 Ausstellung von Zertifikaten

CA-Zertifikate

Die Ausstellung von CA-Zertifikaten, erfordert Zugriff auf den privaten Schlüssel der Root CA im HSM. Die Root CA wird offline gehalten, d.h. eine Ausstellung von CA-Zertifikaten kann nur persönlich im Rechenzentrum erfolgen. Die Verwendung des privaten Schlüssels der Root CA erfordert Mehrfaktorauthentifizierung über Hardware Token. Diese Hardware Token werden persönlich zugeordnet an vier qualifizierte Personen der Rollen CEO und SO (siehe Rollenkonzept Abschnitt 5.2) ausgehändigt. Es müssen sich mindestens zwei dieser Personen (mind. 1 Person der Rolle CEO) anhand ihrer Hardware Token und den Hardware Token zugeordneten PIN Codes authentifizieren, um die Signatur des CA-Zertifikats mit der Root CA durchführen zu können. Die Hardware Token sind von den betroffenen Mitarbeitern sicher zu verwahren und die Weitergabe oder Archivierung der zugeordneten PIN Codes ist untersagt.

Jede Ausstellung von CA-Zertifikaten wird protokolliert. Die Protokollierung enthält sowohl den Zeitpunkt der Ausstellung als auch die an der Ausstellung beteiligten Mitarbeiter des VDA.

Zertifikate für Endbenutzer

Die Zertifikatsausstellung kann nur durch qualifizierte Personen mit der Rolle RO initiiert werden (siehe Rollenkonzept Abschnitt 5.2). Dazu ist der Zugriff auf das Registrierungssystem des VDA über Mehrfaktorauthentifizierung abgesichert.

Jede Ausstellung von Zertifikaten wird protokolliert.

6.5.2 Verwaltung von Zertifikaten

Nur Mitarbeiter mit der Rolle RO (siehe Rollenkonzept Abschnitt 5.2) erlangen Zugriff auf das Verwaltungssystem, dies umfasst das Hinzufügen von Zertifikaten und die Bearbeitung von Daten. Sämtliche damit verbundenen Vorgänge werden protokolliert. Der Zugriff auf das Verwaltungssystem ist über Mehrfaktorauthentifizierung abgesichert.

6.5.3 Widerrufsstatus

Nur der Personen mit der Rolle RO oder RVO (siehe Rollenkonzept Abschnitt 5.2) können Zertifikate sperren, widerrufen oder eine Sperre innerhalb der zehntägigen Frist aufheben.

Wobei Personen mit der Rolle RVO einen Widerruf nur unter Angabe des korrekten Widerrufspasswortes initiieren können. Ohne Angabe des Widerrufspasswortes kann nur eine Sperre initiiert werden. Die technischen Systeme zur Initialisierung eines Widerrufs sind durch technische Sicherheitsmaßnahmen geeignet vor nicht autorisierten Zugriff geschützt. Sämtliche berechtigte Personen müssen sich für die Änderung des Widerrufs- bzw. Sperrstatus unter Verwendung von Mehrfaktorauthentifizierung gegenüber dem System authentifizieren.

Jeder Sperr- bzw. Widerrufsvorgang wird protokolliert.

6.6 Sicherheitsvorkehrungen während der Lebensdauer

Es erfolgt eine ständige Überwachung der Verfügbarkeit der vom VDA angebotenen Dienste, diese umfasst insbesondere die Verfügbarkeit des Verzeichnisdienstes und die Dienste zur Abfrage von Widerrufsstatusinformationen.

Sämtliche Aktivitäten, insbesondere die einzelnen Schritte der Zertifikatsausstellung, Widerruf- und Sperraktivitäten, werden protokolliert. Es erfolgt eine regelmäßige Sicherung dieser Protokolle.

Die Auswahl der verwendeten Hard- und Softwarekomponenten erfolgt unter Beachtung der sich aus den gesetzlichen Regelungen und den Inhalten dieses CPS ergebenen Sicherheitsanforderungen. Ein Einsatz erfolgt nur, sofern die betroffene Komponente ausreichende Sicherheitsfunktionen bietet. Die Auflistung der verwendeten Komponenten erfolgt im nicht öffentlich zugänglichen Dokument Technisches Sicherheitskonzept, Systembeschreibung und

Risikobewertung [TP] des VDA. Dieses enthält auch eine Risikoanalyse. Das Dokument kann von Aufsichtsbehörden bei allfälligen Prüftätigkeiten sowie bei begründetem Interesse auch durch Dritte in den relevanten Teilen eingesehen werden.

Vor Inbetriebnahme von neuen Hardwarekomponenten werden diese gemäß den Herstellerangaben geprüft und erst nach erfolgreicher Prüfung gemäß Herstellerempfehlung betrieben. Eine Versiegelung der Hardware durch den Hersteller ermöglicht beispielsweise die Erkennung von Manipulationsversuchen. Gemäß dem Stand der Technik erfolgen Maßnahmen zur Überprüfung der Authentizität der eingesetzten Softwarekomponenten um eine Kompromittierung der für den Betrieb der vom VDA angebotenen Dienste vorzubeugen.

Im Zuge von Audits und auch nach Aktualisierungen erfolgt die Überprüfung der eingesetzten Hard- und Softwarekomponenten sowie deren Konfiguration.

Im Falle von durch Softwareherstellern herausgegebenen Aktualisierungen erfolgt insbesondere bei Behebung von Sicherheitslücken eine zeitnahe Übernahme in die Systeme des VDA. Dazu werden Softwareaktualisierungen zuerst im Testsystem des VDA eingespielt und anschließend ausführlichen Tests unterzogen. Daraus resultierende Testergebnisse werden dokumentiert. Erst nach erfolgreichen Testdurchläufen erfolgt eine Übernahme ins Produktivsystem des VDA. Sollten Sicherheitslücken in den zur Verfügung gestellten Aktualisierungen bekannt werden, erfolgt keine Übernahme ins Produktivsystem. Im Falle einer bereits erfolgten Übernahme wird eine Risikoanalyse sowie die Ausarbeitung eines Migrationspfades durch qualifiziertes Personal des VDA vorgenommen.

Während des laufenden Betriebs wird die Systemauslastung sowie die sich daraus ergebenden Kapazitätsanforderungen überwacht. Damit wird eine Überlastung des Systems frühzeitig erkannt, um eventuell notwendige Maßnahmen zur Aufstockung der Kapazität, Bandbreite oder den Einsatz zusätzlicher Komponenten zu ergreifen.

Ausgetauschte, defekte oder nicht mehr benötigte Speichermedien werden entsprechend Abschnitt 5.1.7 fachgerecht gelöscht bzw. entsorgt um einen unerlaubten Zugriff auf zuvor darauf gespeicherte Daten zu verhindern.

6.7 Maßnahmen für die Netzwerksicherheit

Die für den Betrieb der CA sowie der damit verbundenen Dienste des VDA notwendigen Netzwerkkomponenten werden im Rechenzentrum betrieben. Für eine nähere Beschreibung zu den Sicherheitsvorkehrungen des Rechenzentrums siehe Abschnitt 5.1.

Der VDA verfügt über ein Konzept zur Trennung von diversen zum Einsatz kommenden Hardware- und Softwarekomponenten in unterschiedliche Sicherheitszonen. Dabei erfolgt sowohl eine Trennung auf Netzwerkebene als auch durch Virtualisierung. Die Trennung auf Netzwerkebene wird durch den Einsatz mehrerer Firewalls realisiert. Die Konfiguration der Firewalls enthält nur die

minimal erforderlichen Regeln für die Kommunikation zwischen den einzelnen Sicherheitszonen. Um das Ausfallsrisiko zu minimieren, erfolgt eine redundante Auslegung der zum Einsatz kommenden Netzwerkkomponenten. Sämtliche Netzwerkkomponenten verfügen über die notwendige Bandbreite, um die geforderte Verfügbarkeit sowie zugesicherte Antwortzeiten für Widerrufsstatusinformationen zu gewährleisten. Das Rechenzentrum verfügt über eine redundante Internetanbindung.

Die Root-CA erfüllt höhere Sicherheitsanforderungen. Aus diesem Grund verfügt die Root-CA über keine Netzwerkanbindung. Die Root-CA wird offline betrieben und sämtliche Softwarekomponenten werden nur bei Bedarf aktiviert und gestartet. Im Falle einer Verwendung des privaten Schlüssels des Root Zertifikats erfolgt diese somit direkt im Rechenzentrum durch autorisierte Personen der Rolle CEO und SO (siehe Rollenkonzept Abschnitt 5.2) im Vieraugenprinzip.

Die für den Betrieb der CA notwendigen Komponenten und Netzwerke sind vollkommen vom internen Netzwerk des VDA getrennt. Der VDA verfügt über ein zusätzliches Test- und Entwicklungssystem, welches vollständig vom produktiven System entkoppelt ist.

Eine nähere Beschreibung des Aufbaus der Netzstruktur und der Aufteilung in Sicherheitszonen ist im nicht öffentlich zugänglichen Dokument Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung [TP] des VDA zu finden. Dieses kann von Aufsichtsbehörden bei allfälligen Prüftätigkeiten sowie bei begründetem Interesse auch durch Dritte in den relevanten Teilen eingesehen werden.

Im Zuge der regelmäßigen internen Audits erfolgt eine Überprüfung der eingesetzten technischen Komponenten sowie deren Konfiguration auf Konformität mit den sich aus diesem Dokument und den gesetzlichen Regelungen ergebenen Anforderungen. Dies schließt die Überprüfung der Netzwerkkomponenten auf Defekte mit ein. Des Weiteren erfolgt ein ständiges Monitoring der Verfügbarkeit der angebotenen Dienste.

Nach dem initialen Setup sowie nach Upgrades von Hardware- und Softwarekomponenten erfolgen Penetrationstests. Diese Tests werden von Mitarbeitern des VDA durchgeführt und die Resultate dokumentiert. In regelmäßigen Abständen erfolgen außerdem sogenannte Vulnerability Scans aller von außen und innen erreichbaren IP-Adressen. Die eingesetzten Firewalls sind mit einer Intrusion Detection Software ausgestattet, um erfolgte Zugriffe zu analysieren und verdächtige Aktivitäten zu erkennen und melden.

6.8 Zeitstempel

Zeitstempel werden im Rahmen dieses CPS nicht angeboten.

7 Profile für Zertifikate, Sperrlisten und Statusabfragedienst

7.1 Zertifikatsprofile

Der Aufbau der ausgegebenen Zertifikate entspricht X.509. Nachfolgend werden die verwendeten Zertifikatsfelder näher erläutert.

TABELLE 7: ZERTIFIKATSPROFIL

Name des Zertifikatsfeldes	**Erklärung**	**Beispiel**
Version	Version der Datenstruktur des Zertifikates. Vom VDA werden lediglich Version 3 Zertifikate (Versionswert: 2) ausgegeben.	2
SerialNumber	Positiver Integerwert. Die Seriennummer wird eindeutig innerhalb der Hierarchie einer CA zugewiesen, d.h. die Kombination aus Issuernamen und Seriennummer ist eindeutig.	z.B. 1234567
Issuer	Informationen des Zertifikatsausstellers. Enthält den vollständig registrierten Namen der Organisation des Zertifikatsausstellers, dessen Niederlassung und den gebräuchlichen Namen des Ausstellers (unterschiedlich für unterschiedliche CAs). Die Darstellung erfolgt als ASN.1-Datentyp *Name* [RFC 5280]. Der Inhalt dieses Zertifikatsfeldes muss ident zum Inhalt des Subject Feldes des CA-Zertifikats sein, von dem das Zertifikat ausgestellt wurde.	<u>Endbenutzerzertifikate:</u> z.B. C=AT, O=PrimeSign GmbH, CN=<CA-Name> <u>CA-Zertifikate:</u> C=AT, O=PrimeSign GmbH, CN=CRYPTAS-PrimeSign Qualified Root
Validity	Beginn- (NotBefore) und Enddatum (NotAfter) der Gültigkeit des Zertifikats. Für Endbenutzerzertifikate ist eine maximale Gültigkeitsdauer von 5 Jahren vorgesehen. Subordinate CA Zertifikate werden mit einer maximalen Gültigkeit von 10 Jahren ausgestellt. Root-	z.B. Not Before: Apr 15 10:15:30 2016 GMT Not After: Apr 15 10:15:30 2021 GMT

	Zertifikate weisen eine maximale Gültigkeit von 20 Jahren auf.	
Subject	Informationen des Zertifikatsinhabers (natürliche oder juristische Person). Siehe Abschnitt 3.1 für nähere Informationen zu den Namensregeln. Die Darstellung erfolgt als ASN.1-Datentyp *Name* [RFC 5280]. Die Kodierung des Attributes organizationIdentifier erfolgt als *Semantics Identifier* gemäß [ETSI 319 412-1].	<u>Natürliche Person:</u> z.B. C=AT, givenName=Max surname=Mustermann, CN=Max Mustermann, serialNumber=1122 Optional: z.B. O=Musterfirma, OU=Buchhaltung, organizationIdentifier=NTRAT-123456p <u>Juristische Person:</u> z.B. C=AT, O=Musterfirma, CN=Musterfirma, serialNumber=2233, organizationIdentifier=NTRAT-123456p
SubjectPublicKeyInfo	Öffentlicher Schlüssel des Zertifikatsinhabers und dazugehöriger Algorithmus. Dieser wird als ASN.1-Datentyp *AlgorithmIdentifier* dargestellt [RFC 5280].	Unterstützte Algorithmen: rsaEncryption (1.2.840.113549.1.1.1) [RFC 3279] id-ecPublicKey (1.2.840.10045.2.1) [RFC 5480]
Signature	Gibt den Algorithmus an, mit dem dieses Zertifikat von der CA signiert wurde. Die Darstellung erfolgt als ASN.1-Datentyp *AlgorithmIdentifier* [RFC 5280]. Je nach Anwendungsfall oder verwendetem QSCD kommt SHA256 mit RSA oder ECDSA zur Anwendung.	Unterstützte Algorithmen: sha256WithRSAEncryption (1.2.840.113549.1.1.11) [RFC 3447] oder ecdsa-with-SHA256 (1.2.840.10045.4.3.3) [RFC 5758]
SignatureAlgorithm	Gibt den Algorithmus an, mit dem dieses Zertifikat von der CA signiert wurde. Die Darstellung erfolgt als ASN.1-Datentyp	Siehe Feld *Signature*.

	AlgorithmIdentifier [RFC 5280]. Dieses Feld muss ident zum Feld *Signature* sein. Je nach Anwendungsfall oder verwendetem QSCD kommt SHA256 mit RSA oder ECDSA zur Anwendung.	
SignatureValue	Digitale Signatur dieses Zertifikats. Mit dieser Signatur bestätigt die ausstellende CA die Gültigkeit der Informationen in diesem Zertifikat. Die Signatur wird als BIT STRING kodiert.	BIT STRING mit Signatur des Zertifikats.

Zertifikatserweiterungen dienen zur Erweiterung der im Zertifikat enthaltenen Daten. Dienste, die eine als kritisch markierte Zertifikatserweiterung nicht auswerten können, müssen das betroffene Zertifikat als ungültig betrachten.

Nachfolgende Auflistung enthält die vom VDA verwendeten Zertifikatserweiterungen. Es erfolgt eine Kennzeichnung der gemäß [ETSI 319 412-2] und [ETSI 319 412-3] verpflichtenden Erweiterungen.

TABELLE 8: VERWENDETE ZERTIFIKATSERWEITERUNGEN

Name der Erweiterung	**Erklärung**	**Belegung**	**Pflicht-feld**	**Kritisch**
AuthorityKeyIdentifier	Identifiziert den öffentlichen Schlüssel des Ausstellerzertifikats. Die Darstellung erfolgt als Datentyp *AuthorityKeyIdentifier*.	Verwendung des Feldes *keyIdentifier*. Die Felder *authorityCertIssuer* und *authorityCertSerialNumber* werden nicht verwendet.	x	
SubjectKeyIdentifier	Identifiziert den öffentlichen Schlüssel des Zertifikatsinhabers. Der Inhalt des SubjectKeyIdentifiers eines CA-Zertifikats ist ident zum Wert der AuthorityKeyIdentifier Erweiterung von mit diesem		x (für CA-Zertifikate)	

	CA-Zertifikat ausgestellten Zertifikaten.			
KeyUsage	Enthält Informationen über den erlaubten Verwendungszweck dieses Zertifikats.	Endbenutzerzertifikate: DigitalSignature + Non Repudiation CA-Zertifikate: keyCertSign + cRLSign	x	x
CertificatePolicy	Enthält die OID zu den für dieses Zertifikat geltenden Certificate Policies.	z.B. 1.2.40.0.39.1.1.1.*1.0.0* URL zur CPS: https://tc.prime-sign.com/cps/ Wobei die letzten drei Stellen der OID die Version der Certificate Policies angibt.	x	
AuthorityInfoAccess	In Endbenutzerzertifikaten wird die AuthorityInfoAccess-Erweiterung verwendet, um mittels URL auf den zuständigen OCSP-Responder (*AccessMethod ocsp*) und das ausstellende CA-Zertifikat (*AccessMethod caIssuers*) zu verweisen. Optional kann auch eine LDAP-URL zum Zertifikat angegeben werden. In Root-CA-Zertifikaten scheint die AuthorityInfoAccess-Erweiterung nicht auf. Da die Root-CA Widerrufsstatusinformationen nur über Widerrufslisten anbietet, verwenden CA-Zertifikate, die von der Root-CA ausgestellt werden, die	z.B. CA Issuers - URI:http://tc.prime-sign.com/certs/<CA-Zertifikatsname>.cer OCSP - URI:http://ocsp.tc.prime-sign.com/ocsp/<CA Name>	x	

	AuthorityInfoAcces-Erweiterung nur, um über den Wert des Attributes *AccessMethod calssuers* das ausstellende Root-Zertifikat zu referenzieren. Das Attribut *AccessMethod ocsp* wird hier nicht benötigt.			
QCStatement	Verwendung nur bei Endbenutzerzertifikaten. Gibt an, dass es sich um ein qualifiziertes Zertifikat handelt und sich der zugehörige private Schlüssel in einem QSCD befindet.	Verwendung des QCStatements gemäß [ETSI 319 412-5].	x (für Endbenutzerzertifikate)	
CRLDistributionPoints	Enthält die URL zur für dieses Zertifikat zuständigen Widerrufsliste. Optional kann zusätzlich auch eine LDAP-URL angegeben werden.	URI: http://tc.prime-sign.com/crls/<CA Name>.crl	x	
BasicConstraints	Verwendung nur bei CA-Zertifikaten.	CA-Zertifikate: CA:TRUE	x (nur für CA-Zertifikate)	x
SubjectAlternativeName	Zusätzlicher Namensbezeichner des Zertifikatsinhabers. Es wird lediglich die E-Mail-Adresse als zusätzlicher Namensbezeichner unterstützt. Die Kodierung erfolgt als *RFC822Name*.	email: max.muster@muster.at		
Verwaltungseigenschaft - OID 1.2.40.0.10.1.1.1	Optional für Endbenutzerzertifikate. Keine Verwendung in CA Zertifikaten.			

	"Die Verwaltungseigenschaft dient der Auszeichnung einer Organisation als dem öffentlichen Bereich zugehörig. Zum Beispiel kann ein Verwaltungseigenschaft-Objekt ein Verwaltungskennzeichen beinhalten, welches ein eindeutiger Ordnungsbegriff für Behörden, Ämter, Landtage, Organisationen und Ressorts ist." (Quelle: BKA[3])			
Dienstleistereigenschaft - OID 1.2.40.0.10.1.1.2	Optional für Endbenutzerzertifikate. Keine Verwendung in CA Zertifikaten. "Die Dienstleistereigenschaft dient der Auszeichnung einer Organisation als im Auftrag der öffentlichen Verwaltung tätig." (Quelle: BKA[4])			
Österreichische Finanzverwaltung Registrierkasseninhaber – OID 1.2.40.0.10.1.11.1	Optional für Endbenutzerzertifikate. Anzugeben für Zertifikate, die für die Verwendung in Registrierkassen gemäß Registrierkassensicherheitsverordnung [RKSV] ausgestellt werden.			

7.2 Sperrlistenprofile (CRL Profile)

Die Widerrufs- bzw. Sperrlisten werden gemäß [RFC 5280] und ITU-T X.509 erstellt. Es werden lediglich Version 2 CRLs unterstützt. Die optionalen Felder "version" und "nextUpdate" werden verwendet.

[3] https://www.bka.gv.at/site/5243/default.aspx
[4] https://www.bka.gv.at/site/5243/default.aspx

TABELLE 9: CRL-PROFIL

Name des Feldes	Erklärung	Belegung
Version	Version der Datenstruktur der Widerrufsliste. Es werden lediglich Version 2 Widerrufslisten unterstützt (Versionsnummer: 1)	1
Signature	Gibt den Algorithmus an, mit dem diese Widerrufsliste von der CA signiert wurde. Die Darstellung erfolgt als ASN.1-Datentyp *AlgorithmIdentifier* [RFC 5280]. Dieses Feld muss ident zum Feld *SignatureAlgorithm* sein.	
Issuer	Informationen des Ausstellers der Widerrufsliste. Der Inhalt dieses Feldes ist ident zum Inhalt des CA-Zertifikats sein, von dem die Widerrufsliste ausgestellt und signiert wurde.	z.B. C=AT O=PrimeSign GmbH CN=<CA-Name>
ThisUpdate	Ausstellungsdatum dieser Widerrufsliste.	z.B. Apr 15 10:15:30 2016 GMT
NextUpdate	Ausstellungsdatum der nächsten Widerrufsliste. Eine frühere Ausstellung kann jedoch stattfinden.	z.B. Apr 15 13:15:30 2016 GMT
RevokedCertificates	Liste der widerrufenen Zertifikate. Aufgeführte Zertifikate werden anhand ihrer Seriennummer identifiziert. Zusätzlich ist das Datum des Widerrufs angegeben. Zusätzlich wird die nicht kritische CRL Entry Extension *Reason Code* verwendet, die den Widerrufsgrund angibt. Ist dieser jedoch nicht spezifiziert, so scheint die CRL Entry Extension *Reason Code* nicht auf. Siehe [RFC 5280] Abschnitt 5.3.1 für eine	

	Auflistung aller unterstützten Reason Codes.	
SignatureAlgorithm	Gibt den Algorithmus an, mit dem diese Widerrufsliste von der CA signiert wurde. Die Darstellung erfolgt als ASN.1-Datentyp *AlgorithmIdentifier* [RFC 5280]. Dieses Feld muss ident zum Feld *Signature* sein. Je nach Anwendungsfall kommt SHA256 mit RSA oder ECDSA zur Anwendung.	Unterstützte Algorithmen: sha256WithRSAEncryption (1.2.840.113549.1.1.11) [RFC 3447] ecdsa-with-SHA256 (1.2.840.10045.4.3.3) [RFC 5758]
SignatureValue	Digitale Signatur dieser Widerrufsliste. Mit dieser Signatur bestätigt die ausstellende CA die Gültigkeit der Informationen in dieser Widerrufsliste. Die Signatur wird als BIT STRING kodiert.	BIT STRING mit Signatur der Widerrufsliste.

TABELLE 10: VERWENDETE CRL-ERWEITERUNGEN

Name der Erweiterung	**Erklärung**	**Belegung**	**Pflicht-feld**	**Kritisch**
AuthorityKeyIdentifier	Die CRL Erweiterung *Authority Key Identifier* gibt den Key Identifier des öffentlichen Schlüssels an, mit dem die Signatur der Widerrufsliste validiert werden kann. Der angegebene Key Identifier soll dem Wert der Erweiterung *SubjectKeyIdentifier* des CRL-Ausstellerzertifikats entsprechen. Die Darstellung erfolgt als Datentyp *AuthorityKeyIdentifier*.		x	
CRLNumber	Monoton ansteigende Nummer für die Widerrufsliste einer CA. Die nicht kritische CRL Extension *CRLNumber* gibt die Reihenfolge der ausgebenen CRLs in aufsteigender Form an.		x	

7.3 Profile für Statusabfragedienst (OCSP Profile)

Es wird eine OCSP Schnittstelle gemäß [RFC 2560] angeboten.

OCSP-Responder werden nur von den CAs angeboten die direkt Endbenutzerzertifikate ausstellen. Alle OCSP-Responder werden als delegierte Responder betrieben, wobei das Zertifikat des Responders unmittelbar von der CA ausgestellt wird, die die OCSP-Information bereitstellt. Das bedeutet, dass das Zertifikat des OCSP-Responders mit demselben Schlüssel unterzeichnet wird, mit dem auch die Endbenutzerzertifikate unterzeichnet werden, für die der OCSP-Responder Widerrufsstatusinformationen zur Verfügung stellt.

OCSP-Responder Zertifikate enthalten folgende Zertifikatserweiterungen: AuthorityKeyIdentifier, SubjectKeyIdentifier, KeyUsage (Belegung: „digitalSignature“), ExtendedKeyUsage (Belegung: „ocspSigning“), CertificatePolicies, NoCheck (d.h. für dieses Zertifikat sind keine Revozierungsinformation über den OCSP-Responder verfügbar) und AuthorityInfoAccess (enthält die Referenz auf das ausstellende CA-Zertifikat).

Der OCSP-Responder wird über das HTTP-Protokoll betrieben (Content-Type: "application/ocsp-response", Content-Length: Länge des DER kodierten OCSPResponses).

Die Versionsnummer des OCSPResponses ist 1, als Response-Status wird einer der folgenden Zustände angegeben [RFC 2560]:

- *successful* (Es können Statusinformationen für die abgefragten Zertifikate bereitgestellt werden.)
- *malformedRequest* (Der erhaltene Request ist ungültig.)
- *internalError* (Es liegt ein interner Fehler am OCSP-Responder vor)
- *tryLater* (Der anfragende Dienst soll die Anfrage zu einem späteren Zeitpunkt erneut stellen.)

Die Zustände *sigRequired* und *unauthorized* werden nicht verwendet

Als Response-Typ wird der einzige definierte Response-Typ, *id-pkix-ocsp-basic* (1.3.6.1.5.5.7.48.1.1) verwendet, als Responder-ID die *byName-Alternative*, d.h. der OCSP-Responder wird über den Namen identifiziert, der dem im Feld *Subject* angegebenen Namen des OCSP-Responder-Zertifikats entspricht [RFC 2560].

Der Responder bezieht die Statusinformationen für die abgefragten Zertifikate direkt aus der Datenbank der ausgestellten Zertifikate. In jedem enthaltenen SingleResponse-Element ist das nextUpdate-Feld nicht gesetzt, d.h. der Responder stellt zu jedem Zeitpunkt aktuelle Statusinformation zur Verfügung.

Als einzige nicht kritische Erweiterung enthält der ASN.1-Datentyp BasicOCSPResponse die Erweiterung *Nonce* [RFC 2560]. Diese wird jedoch nur zurückgeliefert, falls der OCSP-Request diese

enthalten hat. SingleResponse-Erweiterungen werden keine verwendet.

Die OCSP-Antwort wird mit dem Algorithmus *sha256WithRSAEncryption* unter Verwendung des RSASSA-PKCS1-v1_5 Signaturschemas signiert.

8 Überprüfungen und andere Bewertungen

8.1 Konformität

Dienste, Prozesse und Sicherheitsmaßnahmen werden vom VDA gemäß den folgenden Regelwerken umgesetzt:

- PrimeSign Certificate Policy für qualifizierte Zertifikate [CP]
- PrimeSign Certification Practice Statement für qualifizierte Zertifikate
- PrimeSign Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung (nicht öffentlich) [TP]
- Verordnung (EU) 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt [EIDAS]
- Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG) [SigG]
- Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008) [SigG]
- Begutachtungsentwurf: Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG) [SVG]
- Begutachtungsentwurf: Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung – SVV) [SVV]
- ETSI 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [ETSI EN 319 401]
- ETSI 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [ETSI 319 411-1]
- ETSI 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates [ETSI 319 411-2]

8.2 Audits

8.2.1 Generelle Informationen und Aspekte des Audits

Audits dienen zur regelmäßigen Überprüfung der Einhaltung der sich aus den gesetzlichen Bestimmungen, internationalen Standards, dem erstellten Dokument Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung [TP] und den Dokumenten Certificate Policy [CP] und Certification Practice Statement, sowie den (daraus sich ergebenden Anforderungen) der Aufsichtsbehörde (siehe in Abschnitt 8.1 gelistete Dokumente).

Zusätzlich kommen interne, vom VDA veranlasste Audits zur Qualitätssicherung zur Anwendung. Besonderes Augenmerk wird hierbei auf eine stichprobenmäßige Prüfung auf Einhaltung der Anforderungen an den Registrierungsprozess und die Widerrufs- und Sperrprozedur gelegt. Der VDA

geht nach einem internen Auditplan vor und fertigt eine entsprechende Dokumentation des Audits an. Diese beinhaltet die geprüften Komponenten, die Prüfprozedur, den Zeitpunkt der Prüfung sowie das Ergebnis der Prüfung.

8.2.2 Häufigkeit von Audits

Externe Audits werden gemäß eIDAS spätestens alle zwei Jahre im Rahmen der eIDAS Konformitätsbewertung durchgeführt. Es steht den Aufsichtsbehörden offen, vor Ablauf der zwei Jahre ad hoc eine erneute Konformitätsbewertung zu initiieren.

Der VDA führt jedenfalls so häufig wie gesetzlich vorgeschrieben aber mindestens jährlich ein internes Audit zur Qualitätssicherung durch. Zusätzlich liegt es im Ermessen des VDA Audits bei sich ändernden technischen Komponenten, Softwareaktualisierungen oder aufgrund von Personalwechsel zu initiieren.

8.2.3 Identität des Gutachters

Die Aufsichtsbehörde führt das Audit selbst durch oder bestimmt die für die Durchführung des Audits betrauten Gutachter und stellt die geeignete Qualifikation dieser sicher.

Interne Audits werden durch qualifizierter Mitarbeiter des VDA mit der Rolle AO durchgeführt (siehe Rollenkonzept Abschnitt 5.2). Im Zusammenhang mit ihrer Tätigkeit und Funktion als Auditor handeln diese unabhängig und nicht weisungsgebunden.

8.2.4 Handlungen bei negativem Ergebnis

Im Falle eines negativen Audit-Ergebnisses erfolgt die unverzügliche Anpassung der technischen und organisatorischen Abläufe um die identifizierten Schwachstellen zu beseitigen.

Falls eine Beseitigung der Schwachstellen nicht möglich ist, erfolgt ein Widerruf aller betroffenen Zertifikate sowie die Einstellung des Betriebs der betroffenen Infrastruktur.

8.2.5 Bekanntgabe der Ergebnisse

Die Aufsichtsbehörde gibt die Ergebnisse des externen Audits bekannt. Die Bekanntgabe erfolgt in Form des Status des VDA innerhalb der Vertrauensliste europäischer Vertrauensdiensteanbieter[5].

Sollte ein negatives Audit Ergebnis vorliegen sowie eine Beseitigung der Schwachstellen nicht möglich sein, erfolgt die Benachrichtigung aller betroffenen Zertifikatsinhaber sowie die Einstellung des Betriebs der betroffenen Infrastruktur.

[5] https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-certification-service-providers

9 Sonstige finanzielle und rechtliche Regelungen

9.1 Gebühren

Folgende Leistungen sind kostenfrei:

- Sperre oder Widerruf von Zertifikaten
- Abruf von Zertifikaten aus dem Verzeichnisdienst
- Abruf von Widerrufsinformationen via CRL oder OCSP

Für sonstigen Leistungen behält sich der VDA vor ein Entgelt einzuheben.

9.2 Finanzielle Verantwortung

Der VDA verfügt in Bezug auf das Haftungsrisiko für Schäden über ausreichend finanzielle Mittel, gem. den gesetzlichen Vorgaben. Zusätzlich verfügt der VDA gem. den gesetzlichen Vorgaben über eine angemessene Haftpflichtversicherung.

9.3 Vertraulichkeit und Geschäftsdaten

Alle in ausgestellten und veröffentlichten Zertifikaten enthaltenen Daten gelten als öffentlich. Andere Daten des Zertifikatserwerbers werden vertraulich behandelt und nur für die im Signaturvertrag festgelegten Dienste sowie zur Kommunikation mit dem Zertifikatserwerber verwendet.

Der VDA erfüllt die gesetzlichen Auskunftspflichten sofern Behörden, Dritte oder Betroffene ein berechtigtes rechtliches Interesse nachweisen können.

9.4 Datenschutz und Personendaten

Der VDA verpflichtet sich zum Schutz der von ihr verwendeten personenbezogenen Daten des Zertifikatserwerbers zur Einhaltung der jeweils geltenden und anzuwendenden datenschutzrechtlichen Bestimmungen.

Vom Zertifikatserwerber bei der Registrierung bekanntgegebene Daten, allfällige vom Zertifikatserwerber unterschriebene Dokumente, sowie automatisch generierte Systemlog-Dateien werden sicher und vor unerlaubten Zugriffen geschützt verwahrt und ausschließlich für die durch den Signaturvertrag vereinbarten Zwecke verwendet.

Öffentlich einsehbar sind im Zertifikat enthaltenen Daten, sofern der Zertifikatserwerber einer Veröffentlichung des Zertifikats zustimmt.

Weiters, sind folgende Informationen öffentlich zugänglich:

- Prüfinformationen im Zuge einer Widerrufsstatusprüfung

- Zugriff auf öffentliche Zertifikate über den Verzeichnisdienst und
- im Falle einer Verwendung von Pseudonymen kann eine Weitergabe des vollständigen Namens des Zertifikatsinhabers an den Zertifikatsverwender stattfinden.

Eine darüber hinausgehende Weitergabe von Daten an Dritte ist ausgeschlossen.

9.5 Gewerbliche Schutz- und Urheberrechte

Die Dokumente Certificate Policy [CP], Certification Practice Statement, Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung [TP], sowie die auf der Webseite verfügbaren technischen Beschreibungen sind urheberrechtlich geschützt. Eine Verwendung von Textteilen und Grafiken ist nur mit ausdrücklicher schriftlicher Einverständniserklärung des VDA zulässig.

9.6 Gewährleistungsansprüche und Garantien

Der VDA stellt gegenüber dem Zertifikatsinhaber sicher, dass die in diesem Dokument beschriebenen Verfahren und die geltenden gesetzlichen Regelungen eingehalten werden. Zusätzlich gelten die in den Allgemeinen Geschäftsbedingungen festgelegten Vereinbarungen. Für ausgelagerte Tätigkeiten, beispielsweise zur Registrierung stellt, der VDA sicher, dass Verfahrensvorschriften von Erfüllungsgehilfen hinreichend umgesetzt werden und Sicherheitsanforderungen ausreichend erfüllt werden.

Der VDA stellt insbesondere sicher, dass bei der Registrierung eine hinreichende Überprüfung der Identität des Zertifikatserwerbers und die Verifizierung der vom Zertifikatserwerber angegebenen und im Zertifikat enthaltenen Daten erfolgt.

Bei Verfahrensänderung aufgrund technischer, organisatorischer oder rechtlicher Notwendigkeit werden die bereitgestellten Dokumente aktualisiert und sowohl Zertifikatsinhaber als auch Aufsichtsstellen hinreichend informiert.

9.7 Haftungsausschlüsse

Generelle Informationen zu Haftung sowie Haftungsbeschränkungen sind in den Allgemeinen Geschäftsbedingungen geregelt. Diese sind auf der Webseite des VDA verfügbar.

9.8 Haftungsbeschränkungen

Haftungsbeschränkungen können sich aus den Inhalten des Zertifikates ergeben. Insbesondere betrifft dies betragliche Grenzen (finanzieller Transaktionswert), bzw. den Inhalt und Umfang einer Vertretungsvollmacht.

9.9 Schadenersatz

Die Haftung des VDA für Schäden ist in den Allgemeinen Geschäftsbedingungen geregelt. Diese sind

auf der Webseite des VDA verfügbar.

9.10 Gültigkeitsdauer des CPS und Gültigkeitsende

Die Dokumente Certificate Policy [CP] und Certification Practice Statement gelten ab Zeitpunkt der Veröffentlichung. Die Gültigkeit endet bei Ablauf der zeitlichen Gültigkeit des letzten unter diesen Dokumenten ausgestellten Zertifikates. Eine Verpflichtung zur Geheimhaltung der vom Zertifikatsinhaber gespeicherten Daten besteht jedoch auch über die Gültigkeit hinaus.

9.11 Kommunikation

Allfällige Mitteilungen des VDA an den Zertifikatsinhaber werden an die zuletzt vom Zertifikatsinhaber angegebene postalische Adresse oder an die vom Zertifikatsinhaber registrierte E-Mail-Adresse versendet.

Der Zertifikatsinhaber sowie sonstige Dritte können den VDA gemäß der in Abschnitt 1.5.2 angegebenen Kontaktinformation kontaktieren.

9.12 Nachträge

Der VDA behält sich das Recht vor, vorliegende Dokumente gemäß geänderten Sicherheitsanforderungen, Änderungen der technischen Gegebenheiten sowie Änderungen der Gesetzeslage anzupassen bzw. notwendige Ergänzungen durchzuführen. Die jeweils aktuellen Dokumente sind auf der Webseite des VDA unter folgender Adresse verfügbar.

Die veröffentlichten Dokumente enthalten eine fortlaufende Versionsnummer sowie eine Kurzbeschreibung der jeweils durchgeführten Änderung. Es gilt jeweils die Version der Certificate Policy [CP] und des Certification Practice Statements, die zum Zeitpunkt der Zertifikatsantragstellung veröffentlicht ist.

9.13 Bestimmungen zur Schlichtung und Konfliktlösung

Sämtliche Beschwerden bezüglich der Einhaltung und Umsetzung der Certificate Policy [CP] und des Certification Practice Statements sind schriftlich an PrimeSign GmbH zu senden. Sofern nach einer Frist von 6 Wochen nach einreichen der Beschwerde der Gegenstand der Beschwerde nicht aufgelöst wurde, ist der Rechtsweg nicht ausgeschlossen.

9.14 Gerichtsstand

Gerichtsstand ist Graz/Österreich. Es gilt österreichisches Recht.

9.15 Einhaltung geltenden Rechts

Die Ausstellung von qualifizierten Zertifikaten wird in der EU Verordnung 910/2014 [EIDAS] geregelt. Ergänzende Bestimmungen sind in [SVG] und [SVV] enthalten.

9.16 Sonstige Bestimmungen

9.16.1 Vollständigkeitserklärung

Der VDA stellt sicher, dass dem Zertifikatsinhaber alle sich aus diesen Vereinbarungen ergebenen Anforderungen zur Kenntnis gebracht werden, sowie deren Erfüllung vertraglich vereinbart wird.

Der VDA ist für die Einhaltung aller in diesem Dokument beschriebenen Prozesse verantwortlich.

9.16.2 Salvatorische Klausel

Sollten Teile dieses Certification Practice Statements unwirksam sein oder sich gesetzliche Regelungen ändern, die die Bestandteile dieses Certification Practice Statements betreffen, bleiben die anderen Teile dieses Certification Practice Statements in Kraft.

9.16.3 Höhere Gewalt

Der VDA übernimmt keine Haftung im Falle höherer Gewalt.

9.16.4 Rechtsübertragung

Keine Anwendung.

9.17 Andere Bestimmungen

9.17.1 Diskriminierung und Zugänglichkeit

Die vom VDA angebotenen Vertrauensdienste sind allen Interessierten zugänglich, sofern die geltenden Allgemeinen Geschäftsbedingungen, die entsprechenden Entgeltbestimmungen und der ausgestellte Signaturvertrag vom Zertifikatserwerber akzeptiert werden.

Im Rahmen ihrer Möglichkeiten bietet der VDA sowohl Onlinedienste als auch sämtliche Verfahren für Menschen mit Beeinträchtigung nach dem aktuellen Stand der Technik zugänglich an.

9.17.2 Erfüllungsgehilfen

Bei ausgelagerten Tätigkeiten stellt der VDA sicher, dass sämtliche getroffene Vereinbarungen mit Erfüllungsgehilfen schriftlich dokumentiert und vertraglich abgesichert sind.

9.17.3 Rollenteilung

Siehe Abschnitt 5.2.

10 Referenzen

[CC]	Common Criteria Schutzprofil: PP/0308 Cryptographic Module for CSP Signing Operations with Backup Protection Profile, Version 0.28 (27. Oktober 2003), https://www.commoncriteriaportal.org/files/ppfiles/pp0308.pdf
[CP]	PrimeSign Certificate Policy (CP) für qualifizierte Zertifikate
[CPS]	PrimeSign Certification Practice Statement (CPS) für qualifizierte Zertifikate
[EIDAS]	Verordnung (EU) 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
[EIDAS DB]	Durchführungsbeschluss (EU) 2016/650 der Kommision vom 25. April 2016 zur Festlegung von Normen für die Sicherheitsbewertung qualifizierter Signatur- und Siegelerstellungseinheiten gemäß Artikel 30 Absatz 3 und Artikel 39 Absatz 2 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
[EN 50600]	ÖVE/ÖNORM EN 50600: Informationstechnik - Einrichtungen und Infrastrukturen von Rechenzentren
[ETSI TS 119 312]	ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites; V1.1.1 (2014-11)
[ETSI EN 319 401]	ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI EN 319 411-1]	ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements; V1.1.1 (2016-02)
[ETSI EN 319 411-2]	ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates; V2.1.1 (2016-02)
[ETSI 319 412-1]	ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[ETSI 319 412-2]	ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[ETSI 319 412-3]	ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[ETSI 319 412-5]	ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[FIPS PUB 140-2]	FIPS PUB 140-2: Security Requirements for Cryptographic Modules
[RFC 2560]	RFC 2560: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, https://www.ietf.org/rfc/rfc2560.txt
[RFC 3279]	RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://www.ietf.org/rfc/rfc3279.txt
[RFC 3447]	RFC 3447: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, https://www.ietf.org/rfc/rfc3447.txt
[RFC 3647]	RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, https://www.ietf.org/rfc/rfc3647.txt
[RFC 5280]	RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://www.ietf.org/rfc/rfc5280.txt
[RFC 5480]	RFC 5480: Elliptic Curve Cryptography Subject Public Key Information, https://www.ietf.org/rfc/rfc5480.txt
[RFC 5758]	RFC 5758: Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA, https://www.ietf.org/rfc/rfc5758.txt
[ISO 3166]	ISO 3166: Codes for the representation of names of countries and their subdivisions
[ISO 15408]	ISO 15408: Information technology -- Security techniques -- Evaluation criteria for IT security
[ISO 19790]	ISO 19790: Information technology -- Security techniques -- Security requirements for cryptographic modules
[ISO 20000]	ISO 20000: Information technology -- Service management
[ISO 27001]	ISO 27001: Information technology -- Security techniques -- Information security management systems -- Requirements
[RKSV]	Verordnung des Bundesministers für Finanzen über die technischen Einzelheiten für Sicherheitseinrichtungen in den Registrierkassen und andere,

	der Datensicherheit dienende Maßnahmen (Registrierkassensicherheitsverordnung, RKSV), StF: BGBl. II Nr. 410/2015
[SigG]	Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), StF: BGBl. I Nr. 190/1999 idF BGBl. I Nr. 59/2008; Letzte Änderung: BGBl. I Nr. 75/2010 (NR: GP XXIV RV 750 AB 832 S. 73. BR: AB 8370 S. 787.)
[SigV]	Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008), StF: BGBl. II Nr. 3/2008; Letzte Änderung: BGBl. II Nr. 401/2010
[TP]	PrimeSign Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung
[SVG]	Begutachtungsentwurf: Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG)
[SVV]	Begutachtungsentwurf: Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung – SVV)