20. Juni 2016

PrimeSign

Certificate Policy 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	Siegfried 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 die Anwendungsvorgabe (Certificate Policy, CP) 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.

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 Certificate Policy für qualifizierte Zertifikate zur Nutzung mit qualifizierten Signaturen und qualifizierten Siegeln.
Version:	1.0.0
Datum:	20.06.2016
Object Identifier:	1.2.40.0.39.1.1.1.1.0.0 1.2.40.0.39(primesign).1(Dokumentation).1(CP für qualifizierte Zertifikate).1(CA spezifisch).1.0.0(vorliegende Version)

Die OID 1.2.40.0.39 sowie der symbolische Bezeichner „primesign“ sind auf die Firma PrimeSign GmbH registriert.

[1] Qualifizierte Zertifikate für juristische Personen und qualifizierte Siegel (entsprechend der eIDAS Verordnung) werden seitens des VDA erst ausgegeben, wenn die entsprechenden rechtlichen Rahmenbedingungen vorhanden sind (siehe [SVG] bzw. [SVV]).

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.

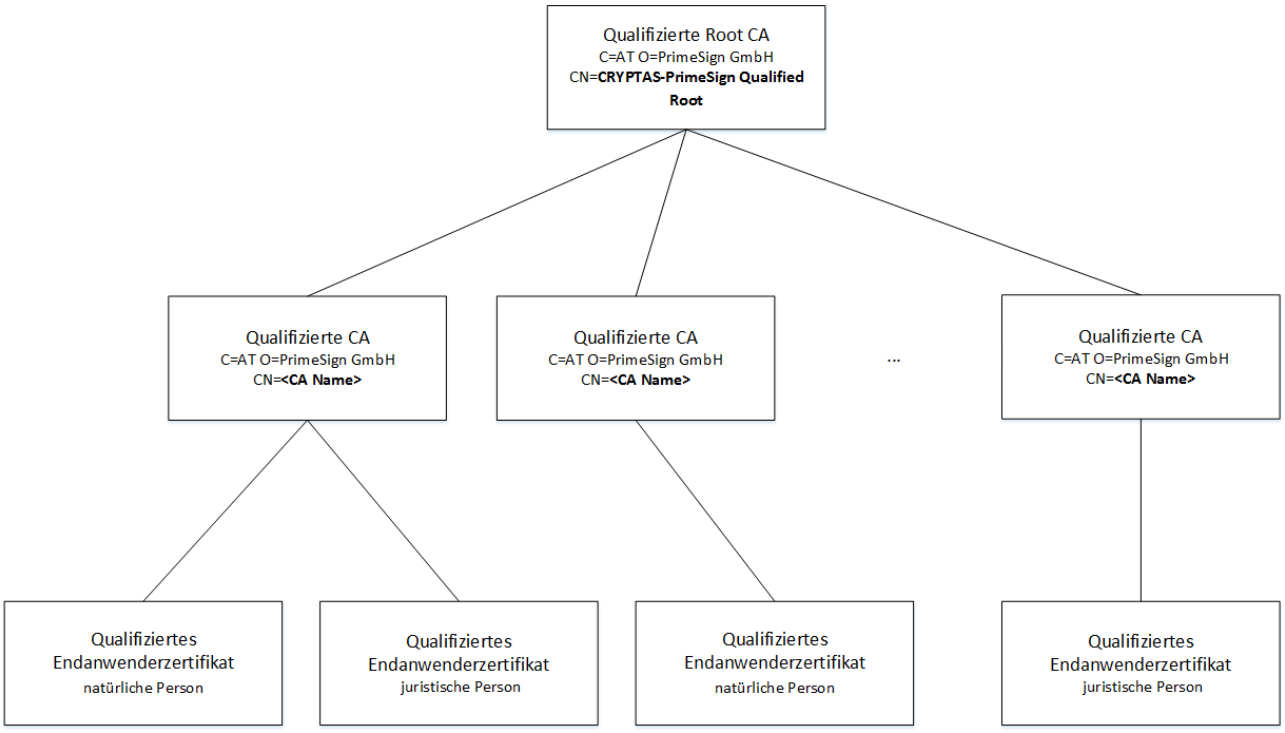

ABBILDUNG 1: ZERTIFIKATSHIERARCHIE

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 qualifzierter 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 Registierungsmöglichkeiten 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 – beispielsweise bei der Überprüfung der Gültigkeit einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels.

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 der CP

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

Der VDA 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) Nr. 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.

2.1.2 Auskunftsdienst über den Zertifikatsstatus

Statusinformationen zu den herausgegebenen Zertifikaten können via CRL oder OCSP abgefragt werden.

2.2 Veröffentlichung von Informationen

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

- https://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 der CP 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 eine Reihe von Attributen dargestellt. Optional kann auch die Zugehörigkeit zu einer Organisation in das Zertifikat mit aufgenommen werden. Details hierzu sind dem entsprechenden Certification Practice Statement [CPS] zu entnehmen.

Für die Ausstellung von Zertifikaten an juristische Personen wird der Name des Zertifikatsinhabers ebenfalls durch eine Reihe von Attribute dargestellt. Details hierzu sind dem entsprechenden Certification Practice Statement [CPS] zu entnehmen.

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 steht dem Zertifikatserwerber weiters die Möglichkeit zur Verfügung die Identität mittels sicherer Identifikationsverfahren (z.B. via Zustellung zu eigenen Handen) nachzuweisen.

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 geeignete Nachweise, die über eine dem Stand der Technik gemäße 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

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. Weiters werden alle im Zertifikat anzugebenden Daten der juristischen Person überprüft.

3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung

Die Schlüsselerneuerung bezeichnet die erneute Generierung von Zertifikaten und Schlüsseln für dasselbe 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 und unterzeichnen.

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.

Weitere Details zum Ablauf einer Sperre bzw. eines Widerrufs sind dem entsprechendem Certification Practice Statement [CPS] zu entnehmen.

4 Betriebsanforderungen

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 (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 Information über Rechte und Pflichten gemäß Signaturvertrag, die Allgemeinen Geschäftsbedingungen und die vorliegenden Dokumente Certificate Policy und Certification Practice Statement [CSP]. 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.

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. Diese kann entweder persönlich mittels Zustellung zu eigenen Handen 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)
- Im Falle der Verwendung einer Smartcard: sichere Verwahrung der Smartcard
- 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
  - Abhandenkommen 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 CP 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 CP und der im Zertifikat ausgewiesenen 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)
- Karte 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 in offener Frist 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 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.

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.

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.

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 VDA 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

Sämtliche baulichen Sicherheitsmaßnahmen sind im entsprechenden Certification Practice Statement [CPS] und im Dokument „Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung“ [TP] beschrieben.

5.2 Verfahrensvorschriften

Sämtliche Verfahrensvorschriften sind im entsprechenden Certification Practice Statement [CPS] und im Dokument „Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung“ [TP] beschrieben.

5.3 Personelle Sicherheitsvorkehrungen

Der VDA, und die mit diesem verbundene Unternehmen, sofern Personal der verbundenen Unternehmen zur Rollen- und Leistungserfüllung herangezogen werden, verfügt über folgende personellen Sicherheitsvorkehrungen:

- Der VDA zieht zur Rollen- und Leistungserfüllung ausschließlich Personal heran oder bedient sich externer Dienstleister, das bzw. die über das benötigte Fachwissen, Qualifikation und Eigenschaften für die jeweilige Position bzw. Rolle verfügt.
- Der VDA zieht zur Rollen- und Leistungserfüllung ausschließlich Personal heran oder bedient sich externer Dienstleister, das bzw. die auch auf die erhöhte Sicherheitsrelevanz eines qualifizierten Vertrauensdiensteanbieters sensibilisiert ist.
- Vor der Aufnahme einer bestimmten Tätigkeit wird das Personal bzw. der Dienstleister entsprechend geschult. Dies betrifft insbesondere Personal bzw. Dienstleister, das bzw. die hochsicherheitskritische Tätigkeiten ausübt bzw. ausüben.

Weitere Details zu den personellen Sicherheitsvorkehrungen und Rollenkonzepte sind im entsprechenden Certification Practice Statement [CPS] beschrieben.

5.4 Protokollierung und Überwachungsmaßnahmen

Der VDA führt umfangreiche Ereignisprotokolle deren Vertraulichkeit und Integrität sichergestellt ist. Weitere Details sind im entsprechenden Certification Practice Statement [CPS] beschrieben.

5.5 Archivierung von Aufzeichnungen

Der VDA archiviert alle Ereignisprotokolle und weiteren Aufzeichnungen. Weitere Details sind im entsprechenden Certification Practice Statement [CPS] beschrieben.

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 dies betrifft CA und Root-CA Schlüssel gleichermaßen wie Benutzerzertifikate.

5.7 Kompromittierung und Notfallsplan

Der VDA überwacht sämtliche Systemkomponenten und ergreift entsprechende Maßnahmen beim Erkennen von ungewöhnlichen bzw. verdächtigen Vorgängen. Des Weiteren hat der VDA 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.

5.8 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

Die Erstellung des Wurzelschlüsselpaares (Root-Key) sowie der CA-Schlüsselpaare, bzw. allgemein die Erstellung aller Schlüsselpaare des VDA, die auch zur Ausstellung von Subordinate-CA sowie auch zur Erstellung von Endbenutzerzertifikaten herangezogen werden, erfolgt innerhalb des Hochsicherheitsbereichs des Rechenzentrums im HSM durch autorisiertes Personal anhand des Vieraugenprinzips (Schlüsselerstellungszeremonie).

Für Endbenutzerzertifikate erfolgt die Schlüsselgenerierung im QSCD (auf Basis eines Signaturtokens wie einer Smartcard bzw. in einer HSM im Falle von Remote Signing). Die eingesetzten QSCDs erfüllen die Sicherheitsanforderungen und Zertifizierungen QSCD gemäß Verordnung (EU) 910/2014 [EIDAS] (Anhang II) bzw. Durchführungsbeschluss 2016/650 [EIDAS DB].

Weitere Details sind im entsprechenden Certification Practice Statement [CPS] sowie im Dokument Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung [TP] beschrieben.

6.2 Schutz der privaten Schlüssel

Wurzel- und CA-Schlüssel werden nur innerhalb der HSM verwendet. Das Schlüsselmaterial auf den QSCDs für Endbenutzer ist durch entsprechenden Maßnahmen geschützt. So ist insbesondere die Verwendung des privaten Schlüsselmaterials nur mit dem Zertifikatsinhaber möglich.

Weitere Details sind im entsprechenden Certification Practice Statement [CPS] sowie im Dokument Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung [TP] beschrieben.

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. Schlüssel für Endbenutzerzertifikate dienen lediglich zur Signaturerstellung.

Weitere Details sind im entsprechenden Certification Practice Statement [CPS] sowie im Dokument Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung [TP] beschrieben.

6.4 Aktivierungsdaten

Die Generierung von Schlüsselmaterial für Wurzel-/CA-Zertifikate erfolgt anhand eines Vieraugenprinzips durch mindestens zwei autorisierte Mitarbeiter des VDA entsprechend des umgesetzten Rollenkonzepts. Die Verwendung des privaten Schlüssels einer Subordinate-CA erfolgt im Zuge der Ausstellung von Endbenutzerzertifikaten.

Der Einsatz des privaten Schlüssels für Endbenutzer ist durch einen Authentifizierungsvorgange (zum Beispiel PIN) geschützt.

Weitere Details sind im entsprechenden Certification Practice Statement [CPS] sowie im Dokument Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung [TP] beschrieben.

6.5 Sicherheitsvorkehrungen in den Computersystemen

Siehe Certification Practice Statement [CPS] sowie Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung [TP].

6.6 Sicherheitsvorkehrungen während der Lebensdauer

Siehe Certification Practice Statement [CPS] sowie Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung [TP].

6.7 Maßnahmen für die Netzwerksicherheit

Siehe Certification Practice Statement [CPS] sowie Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung [TP].

6.8 Zeitstempel

Zeitstempel werden im Rahmen dieser Certificate Policy 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 3: 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 4: 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[2])			
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[3])			
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.			

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

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.

TABELLE 5: 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 6: 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		x	

	nicht kritische CRL Extension *CRLNumber* gibt die Reihenfolge der ausgebenen CRLs in aufsteigender Form an.			

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
- PrimeSign Certification Practice Statement für qualifizierte Zertifikate [CPS]
- 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

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 und Certification Practice Statement [CPS], sowie den (daraus sich ergebenden Anforderungen) der Aufsichtsbehörde.

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.

Weitere Details sind im entsprechenden Certification Practice Statement [CPS] beschrieben.

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 auch 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, Certification Practice Statement [CPS], 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 der CP und Gültigkeitsende

Die Dokumente Certificate Policy und Certification Practice Statement [CPS] 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 und des Certification Practice Statements [CPS], die zum Zeitpunkt der Zertifikatsantragstellung veröffentlicht ist.

9.13 Bestimmungen zur Schlichtung und Konfliktlösung

Sämtliche Beschwerden bezüglich der Einhaltung und Umsetzung der Certificate Policy und des Certification Practice Statements [CPS] sind schriftlich an die 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 Verordnung (EU) 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 dieser Certificate Policy unwirksam sein oder sich gesetzliche Regelungen ändern, die die Bestandteile dieser Certificate Policy betreffen, bleiben die anderen Teile dieser Certificate Policy 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
[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)
[TP]	PrimeSign Technisches Sicherheitskonzept, Systembeschreibung und Risikobewertung