Certification Practice Statement of the D-TRUST CSM PKI

ENGLISH

DEUTSCH
Certification Practice Statement of the D-TRUST CSM PKI

Version 3.0
COPYRIGHT NOTICE AND LICENSE

Certification Practice Statement of the D-TRUST CSM PKI
©2020 D-Trust GmbH

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

Please direct any inquiries regarding any other form of use of this CPS of D-Trust GmbH not covered by the above-mentioned license to:

D-Trust GmbH
Kommandantenstr. 15
10969 Berlin, Germany
Phone: +49 (0)30 259391 0
E-mail: info@d-trust.net
## Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>2015-02-09</td>
<td>Initial version</td>
</tr>
<tr>
<td>1.1</td>
<td>2015-02-23</td>
<td>- Editorial changes during first-time certification according to ETSI 102 042 LCP. Several contents of the CP of D-Trust GmbH were incorporated in the CPS.</td>
</tr>
</tbody>
</table>
| 1.2     | 2015-10-05 | - Editorial changes  
  - More detailed information regarding the option to have the key material generated and delivered by the TSP  
  - Revocation now only via the online interface and by phone when a revocation password was agreed to  
  - All new certificates are always published in the D-TRUST LDAP. |
| 1.3     | 2016-10-03 | - Change to EN 319 411-1                                                                                                                   |
| 2.0     | 2017-01-01 | - Introduction of qualified TLS certificates (QWACs) according to EN 319 411-2 and eIDAS                                                 |
| 2.1     | 2017-10-01 | - Editorial changes along with more specific details in section 6.5                                                                          |
| 2.2     | 2018-03-28 | - Editorial changes and a revision of compatibility with RFC 3647  
  - Adaptation of the use license to "Creative Commons Attribution"  
  - Adapted to Mozilla Root Store Policy 2.5 |
| 2.3     | 2018-07-05 | - Change in domain validation methods in 4.2.1  
  - OrgID field in section 3.1.4 was amended according to variant 3 in section 5.1.4 of EN 319 412-1.  
  - Editorial changes |
| 2.4     | 2018-10-11 | - Table listing CA certificates in section 1.1.3  
  - Amendments in section 7.3  
  - Adaptation of sections 1.5.2 and 4.9 according to SC6v3 Ballot from the CAB Forum |
| 2.5     | 2018-11-30 | - This CPS complies with the requirements of Mozilla Policy 2.6.1  
  - The hotline service is discontinued (section 4.9.3)  
  - Full annual review of the CPS  
  - Editorial changes |
| 2.6     | 2019-05-15 | - Addition of Qualified Website Authentication Certificates (QWACs) with PSD2 extension  
  - Full annual review of the CPS  
  - Editorial changes |
| 2.7     | 2019-05-22 | - Addition of qualified seal certificates with PSD2 extension without QSCD  
  - In section 4.2.1, methods 3.2.2.4.7, 3.2.2.4.13 and 3.2.2.4.14 added to the domain validation methods according to [BRG] |
### Certification Practice Statement of the D-TRUST CSM PKI

#### 2.8 2019-10-09
- Update according to observation report
- Clarification of section 5.5.2
- Editorial changes

#### 2.9 2020-03-19
- Introduction of domain-validated TLS certificates (DVCP) according to EN 319 411-1 and BRG
- This CPS complies with the requirements of Mozilla Policy 2.7
- Full annual review of the CPS
- Adjustment of the archiving period for LCP in section 5.5.2
- SHA-256 fingerprints added in section 1.1.3
- Domain validation methods added in section 4.2.1

#### 2.10 2020-04-27
- Activation of the sub-CA for issuing DV certificates, see section 1.1.3.
- Integration of new sub-CAs for issuing EV and OV certificates, see section 1.1.3.
- Amendments to certificate chain verification in section 4.5.2.
- Amendments in sections 5.3.7 and 5.5.2
- Reduction of the validity period of TLS certificates, see section 6.3.2.

#### 2.11 2020-06-17
- Introduction of administration-PKI (V-PKI) certificates according to BSI TR-03145-1

#### 2.12 2020-09-28
- Assignment of a D TRUST OID for the V-PKI
- Publication and commissioning of the V-PKI sub CA
- Link added in section 4.2.1 for publication of registration or incorporating agency information in the repository

#### 3.0 2020-11-10
- From version 3 or higher, the CSM CPS is subordinate to the TSPS
- Update according to observation report
- Amendment in section 3.3.1
Contents

1. Introduction ...................................................................................................................... 7
1.1 Overview ......................................................................................................................... 7
1.2 Document name and identification ............................................................................... 13
1.3 PKI participants ............................................................................................................ 13
1.4 Certificate usage .......................................................................................................... 13
1.5 Policy administration .................................................................................................. 14
1.6 Definitions and acronyms ............................................................................................. 14
2. Publication and Repository Responsibility ...................................................................... 15
2.1 Repositories .................................................................................................................. 15
2.2 Publication of certificate information ........................................................................... 15
2.3 Publication frequency ................................................................................................... 15
2.4 Repository access control ............................................................................................. 16
2.5 Access to and use of services ....................................................................................... 16
3. Identification and Authentication .................................................................................... 16
3.1 Naming .......................................................................................................................... 16
3.2 Initial identity verification .............................................................................................. 21
3.3 Identification and authentication for re-keying requests ............................................ 24
3.4 Identification and authentication of revocation requests ............................................ 24
4. Operational Requirements .............................................................................................. 25
4.1 Certificate request and registration .............................................................................. 25
4.2 Processing the certificate request ................................................................................ 25
4.3 Certificate issuance ....................................................................................................... 26
4.4 Certificate handover ...................................................................................................... 26
4.5 Key Pair and Certificate Usage ..................................................................................... 27
4.6 Certificate renewal ......................................................................................................... 27
4.7 Certificate renewal with re-keying ................................................................................ 27
4.8 Certificate modification ............................................................................................... 28
4.9 Certificate revocation and suspension ......................................................................... 28
4.10 Certificate status services ............................................................................................ 30
4.11 Withdrawal from the certification service .................................................................... 31
4.12 Key escrow and recovery ............................................................................................. 31
5. Facility, Management and Operational Controls .............................................................. 31
5.1 Physical controls .......................................................................................................... 31
5.2 Procedural controls ...................................................................................................... 31
5.3 Personnel controls ....................................................................................................... 31
5.4 Audit logging procedures ............................................................................................. 32
5.5 Records archival .......................................................................................................... 32
5.6 Key change at the TSP ............................................................................................... 33
5.7 Compromise and disaster recovery at the TSP ............................................................ 33
5.8 Closure of the TSP or termination of services .............................................................. 33
6. Technical Security Controls ............................................................................................ 33
6.1 Key pair generation and installation ............................................................................. 33
6.2 Private key protection and cryptographic module engineering controls .................... 34
6.3 Other aspects of key pair management ........................................................................ 36
6.4 Activation data ............................................................................................................ 36
6.5 Computer security controls ........................................................................................ 37
6.6 Life cycle technical controls ....................................................................................... 37
6.7 Network security controls ........................................................................................... 37
6.8 Time stamps ................................................................................................................ 37
7. Profiles of Certificates, Certificate Revocation Lists and OCSP .................................... 37

Date of release 2020-11-10
Effective date 2020-11-12
Page 5/39
7.1 Certificate profiles .................................................................................................................. 37
7.2 CRL Profiles ........................................................................................................................ 38
7.3 OCSP profiles ....................................................................................................................... 38
8. Compliance Audit and Other Assessments .............................................................................. 39
9. Other Business and Legal Matters ......................................................................................... 39
1. Introduction

1.1 Overview

This document is the Certification Practice Statement (CPS) of the trust services operated by D-Trust GmbH that are provided via the Certificate Service Manager (CSM). The document name is abbreviated CSM CPS and is subject to the Trust Service Practice Statement of D-TRUST (abbreviated as TSPS) and the Certificate Policy (referred to here as CP).

1.1.1 Trust service provider (TSP)

These rules are documented in the CP.

1.1.2 About this document

The following diagram shows the document hierarchy used by D-Trust GmbH. The green marking highlights the document, which you are currently reading.

References are shown as follows:

- **These rules are documented in the CP.**
  
  Rules that refer to certificate policies are documented in the CP.

- **The general rules are documented in the TSPS.**
  
  The general rules are documented in the TSPS and the specific rules remain in the CPS.

- **Other rules are documented in the TSPS.**
  
  In addition to the specific rules in the CPS, there are also other rules that are documented in the TPS.

- **These rules are documented in the TSPS.**
  
  Rules are described in the TSPS only.
This CPS refers to the CP (Certificate Policy) of D-Trust GmbH with OID 1.3.6.1.4.1.4788.2.200.1, the TSPS (D-TRUST Trust Service Practice Statement) and to [EN 319 411-1] or EN 319 411-2, respectively, and describes the implementation of the resultant requirements.

Unless this document distinguishes between the certification requirements or policy levels according to section 1.1.3 or unless certain policy levels are expressly ruled out, the requirements or provisions of the respective sections are applicable to all certificates pursuant to the classification of the Certificate Policy of D-Trust GmbH.

The structure of this document is based on the RFC 3647 Internet standard: "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework".

Other rules are documented in the TSPS.

1.1.3 Properties of the PKI

The trust services provided via the CSM are based on a multi-level PKI. Figs. 1 and 2 show PKI set-ups for qualified and non-qualified trust services. It always consists of a chain which begins with a root CA (root authority or trust anchor) which is optionally followed by further sub-CAs (intermediate CAs). The last sub-CA of this chain is the issuing CA which issues EE certificates.

**Fig. 1 PKI hierarchy for qualified trust services**

Depending on their features, EE certificates can be assigned to the requirements of the different policies (policy level) within EN 319 411-2:

- **QCP-w** – Qualified Website Authentication Certificates (QWACs)
- **QCP-I** – Qualified Seal Certificates (QSealCs)

The policy levels are explained in the TSPS.
Certification Practice Statement of the D-TRUST CSM PKI

PKI for non-qualified trust services

\[
\begin{array}{c}
D-\text{TRUST Root Class 3 CA 2 EV 2009} \\
D-\text{TRUST Root Class 3 CA 2 2009} \\
D-\text{TRUST Root CA 3 2013} \\
D-\text{TRUST SSL Class 3 CA 1 EV 2009} \\
(DVCP) \\
D-\text{TRUST SSL Class 3 CA 1 2009} \\
(DVCP) \\
D-\text{TRUST Application CAs 3-1 2013 (LCP)} \\
VR IDENT EV SSL CA 2020 \\
(EVCP) \\
VR IDENT SSL CA 2020 \\
(OVCP)
\end{array}
\]

PKI für Nicht-qualifizierte Vertrauensdienste (publicly trusted)

\[
\begin{array}{c}
\text{Root-CA-Ebene} \\
\text{Sub-CA-Ebene}
\end{array}
\]

Fig. 2 PKI hierarchy for non-qualified trust services

Depending on their features, EE certificates can be assigned to the requirements of the different policies (policy level) within EN 319 411-1:

- LCP – Lightweight Certificate Policy
- DVCP – Domain Validation Certificate Policy
- OVCP – Organizational Validation Certificate Policy
- EVCP – Extended Validation Certificate Policy

The policy levels are explained in the TSPS.

Trust service of the administration PKI (V-PKI) with a trust anchor at BSI

\[
\begin{array}{c}
\text{PCA-1-Verwaltung-nm} \\
\text{Root-CA-Ebene vom BSI} \\
\text{Sub-CA-Ebene der D-TRUST}
\end{array}
\]

Fig. 3 PKI hierarchy for the trust service of the administration PKI (V-PKI)

---

\footnote{In future, the “D-TRUST EV Root CA 1 2020” root CA is to replace the existing “D-TRUST Root Class 3 CA 2 EV 2009” root CA and is listed here for information purposes. In future, the “D-TRUST BR Root CA 1 2020” root CA is to replace the existing “D-TRUST Root Class 3 CA 2 2009” root CA and is listed here for information purposes.

The “D-TRUST SSL CA 2 2020” SubCA was created on 21 April 2020 and is integrated into the CCADB.}
The root authority PCA-1-Administration is operated by the Federal Office for Information Security in accordance with the "Security guidelines of the administration root certification authority", version 3.2 dated 9 January 2003 and the related amendments, version 1.1, dated 29 January 2013 (abbreviated as: CP V-PKI BSI).

The “D-TRUST V-PKI CA 1 2020” sub-CA is registered with the Federal Office for Information Security (BSI) and issues V-PKI certificates only.

A regular key exchange is carried out each year in the root authority. When the key of the certification authority is exchanged, the root authority issues a new certification authority certificate. This means that, pursuant to CP V-PKI BSI, section 6.6, several valid certification authority certificates may exist. “nm” in the name of the RootCA is incremented accordingly.

As part of the V-PKI, the CMS CPS refers to the CP V-PKI BSI from the Federal Office for Information Security.

Certificates from the V-PKI as well as their sub-CAs are issued according to the requirements of BSI [TR-03145-1]. Depending on their features, EE certificates can be assigned to the requirements of the different policies within BSI [TR-03145-1].

It is not foreseen for the “D-TRUST V-PKI CA 1 2020” sub-CA to issue further sub-CAs or issuing CAs. The sub-CA may only issue certificates for the customer's own employees and not for external employees.

Policy OID 0.4.0.127.0.7.3.6.1.1.4.4 (BSI) and policy OID 1.3.6.1.4.1.4788.2.201.2 (D-TRUST) assigned for certificates from the V-PKI (administration PKI).

### CA certificates

The complete overview of all root CAs and sub-CAs with policy levels QCP-w, EVCP, OVCP, DVCP and LCP, showing which CPS applies to the respective CA application, can be found in the repository:


The following table provides an overview of all root CAs and the associated sub-CAs to which this CPS applies.

<table>
<thead>
<tr>
<th>D-TRUST Root Class 3 CA 2 EV 2009</th>
<th><a href="http://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_EV_2009.crt">http://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_EV_2009.crt</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint:</td>
<td></td>
</tr>
<tr>
<td>SHA1: 96C91B0B95B4109842FA0D82279FE60FAB91683</td>
<td></td>
</tr>
<tr>
<td>SHA256: EEC5496B988CE98625B934092EE2908BED0B0F316C2D4730C84EAF1F3D34881</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D-TRUST CA 2-2 EV 2016</th>
<th><a href="http://www.d-trust.net/cgi-bin/D-TRUST_CA_2-2_EV_2016.crt">http://www.d-trust.net/cgi-bin/D-TRUST_CA_2-2_EV_2016.crt</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Level: QCP-w</td>
<td></td>
</tr>
<tr>
<td>Fingerprint:</td>
<td></td>
</tr>
<tr>
<td>SHA1: 8423CDA13FF6025BCD3188DD37F8618C31D85D9</td>
<td></td>
</tr>
<tr>
<td>SHA256: 2316D05A2E2D347FA141135B98ED0F56E81F1CF5679793D3B39DD6D8E461A48</td>
<td></td>
</tr>
<tr>
<td>OID: 1.3.6.1.4.1.4788.2.150.4</td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td></td>
</tr>
<tr>
<td>D-TRUST SSL Class 3 CA 1 EV 2009</td>
<td></td>
</tr>
<tr>
<td><a href="https://www.d-trust.net/cgi-bin/D-TRUST_SSL_Class_3_CA_1_EV_2009.crt">https://www.d-trust.net/cgi-bin/D-TRUST_SSL_Class_3_CA_1_EV_2009.crt</a></td>
<td></td>
</tr>
<tr>
<td>Policy Level: EVCP</td>
<td></td>
</tr>
<tr>
<td>Fingerprint:</td>
<td></td>
</tr>
<tr>
<td>SHA1: 1069423D308D0FC54575059638560FC7556E32B3</td>
<td></td>
</tr>
<tr>
<td>SHA256: B0935DC04B4E60C0C42DEF7EC57A1B1D8F958D17988E71CC80A8CF5E635BA5B4</td>
<td></td>
</tr>
<tr>
<td>OID: 1.3.6.1.4.1.4788.2.202.1</td>
<td></td>
</tr>
<tr>
<td>VR IDENT EV SSL CA 2020</td>
<td></td>
</tr>
<tr>
<td><a href="https://www.d-trust.net/cgi-bin/VR_IDENT_EV_SSL_CA_2020.crt">https://www.d-trust.net/cgi-bin/VR_IDENT_EV_SSL_CA_2020.crt</a></td>
<td></td>
</tr>
<tr>
<td>Policy Level: EVCP</td>
<td></td>
</tr>
<tr>
<td>Fingerprint:</td>
<td></td>
</tr>
<tr>
<td>SHA1: AC4126DEB7907EE11BB06504BD2AB224237915</td>
<td></td>
</tr>
<tr>
<td>SHA256: 9E6C8035C0F1C8A945310E72D83E531947B571F9292E42A4248A3708F7B305BE</td>
<td></td>
</tr>
<tr>
<td>D-TRUST Root Class 3 CA 2 2009</td>
<td></td>
</tr>
<tr>
<td><a href="https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt">https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt</a></td>
<td></td>
</tr>
<tr>
<td>Policy Level: OVCP</td>
<td></td>
</tr>
<tr>
<td>Fingerprint:</td>
<td></td>
</tr>
<tr>
<td>SHA1: 58E8ABB0361533FB80F79B1B6D29D3FF8D5F00F0</td>
<td></td>
</tr>
<tr>
<td>SHA256: 49E7A442ACF0EA62B7050054B52564B650E4F49E42E348D6AA38E039E957B1C1</td>
<td></td>
</tr>
<tr>
<td>D-TRUST SSL Class 3 CA 1 2009</td>
<td></td>
</tr>
<tr>
<td><a href="https://www.d-trust.net/cgi-bin/D-TRUST_SSL_Class_3_CA_1_2009.crt">https://www.d-trust.net/cgi-bin/D-TRUST_SSL_Class_3_CA_1_2009.crt</a></td>
<td></td>
</tr>
<tr>
<td>Policy Level: OVCP</td>
<td></td>
</tr>
<tr>
<td>Fingerprint:</td>
<td></td>
</tr>
<tr>
<td>SHA1: 2FC5DE6528CDBE50A14C382FC1DE524FAABF95FC</td>
<td></td>
</tr>
<tr>
<td>SHA256: 6AC159B4C2BC8E729F3B84642EF1286BCC80D775FE278C740ADA468D59439025</td>
<td></td>
</tr>
<tr>
<td>OID: 1.3.6.1.4.1.4788.2.230.1</td>
<td></td>
</tr>
<tr>
<td>D-TRUST SSL CA 2 2020</td>
<td></td>
</tr>
<tr>
<td><a href="https://www.d-trust.net/cgi-bin/D-TRUST_SSL_CA_2_2020.crt">https://www.d-trust.net/cgi-bin/D-TRUST_SSL_CA_2_2020.crt</a></td>
<td></td>
</tr>
<tr>
<td>Policy Level: DVCP</td>
<td></td>
</tr>
<tr>
<td>Fingerprint:</td>
<td></td>
</tr>
<tr>
<td>SHA1: AEB9682B91D20B50384A2C6B6DACBB851F629962</td>
<td></td>
</tr>
<tr>
<td>SHA256: 972A181B60294EBA07333B9C19B82440D43395ABA91D450EC0EFB485AED49D5A7</td>
<td></td>
</tr>
<tr>
<td>OID: 1.3.6.1.4.1.4788.2.202.3</td>
<td></td>
</tr>
</tbody>
</table>
Certification Practice Statement of the D-TRUST CSM PKI

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Date</th>
<th>Policy Level</th>
<th>Fingerprints</th>
<th>Fingerprint Hashes</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>VR IDENT SSL CA 2020</td>
<td>2020-11-10</td>
<td>OVCP</td>
<td>SHA1: C3A6BC49BC9936E9450A97775465B7235E78EE705</td>
<td>SHA256: 007108194115F3C899F54EE67CB4DA87275EDC1D6798DA787E0758CFA6AE96B1</td>
<td>1.3.6.1.4.1.4788.2.230.2</td>
</tr>
<tr>
<td>D-TRUST Root CA 2 2018</td>
<td>2020-11-12</td>
<td></td>
<td>SHA1: 4B467FB8D2051D7BC4CDB733777FA7077034BCCE1</td>
<td>SHA256: 113BBD9EFFFAC743D6D09038DC0AAB1A5F1FAD7492868193917C63D82D74FA1</td>
<td></td>
</tr>
<tr>
<td>D-TRUST CA 2-1 2018</td>
<td>2020-11-12</td>
<td>QCP-w</td>
<td>SHA1: 5982BDD5E228E48694E1713710CC5C3DDE006C43</td>
<td>SHA256: 5F28B88456D21158C5E3E8A31719CF3B305300BC5B436B696BE22F6973F1DF1</td>
<td></td>
</tr>
<tr>
<td>D-TRUST CA 2-2 2019</td>
<td>2020-11-12</td>
<td>QCP-l</td>
<td>SHA1: 455FD6F160938C1FCCE1EF8D4F33700F2148FF87</td>
<td>SHA256: E85F41CE30CF9910CBBD12470F9E312E8F862FFE0D581F5995772D8B46CB7E99</td>
<td></td>
</tr>
<tr>
<td>D-TRUST Root CA 3 2013</td>
<td>2020-11-12</td>
<td></td>
<td>SHA1: 6C7CCCE7D4AE51F9908CD3FF6E8C378DF6FeF97</td>
<td>SHA256: A1A86D04121EB87F027C66F53303C28E5739F943FC84B38AD6AF009035DD9457</td>
<td></td>
</tr>
<tr>
<td>D-TRUST Application Certificates CA 3-1 2013</td>
<td>2020-11-12</td>
<td>LCP</td>
<td>SHA1: 1785B07501F0FCEFFC97C6B070C255A8A9B99F12</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Date of release: 2020-11-10
Effective date: 2020-11-12
Page: 12/39
1.2 Document name and identification

Document name: Certification Practice Statement of the D-TRUST CSM PKI
Version: 3.0

1.3 PKI participants

1.3.1 Certification authorities (CAs)
These rules are documented in the TSPS.

1.3.2 Registration authorities (RAs)
These rules are documented in the TSPS.

1.3.3 Subscribers and end-entities (EEs)
These rules are documented in the TSPS.

1.3.4 Relying parties (RPs)
These rules are documented in the TSPS.

1.4 Certificate usage

1.4.1 Permitted certificate usage
These rules are documented in the TSPS.
1.4.2 Forbidden certificate usage
   These rules are documented in the TSPS.

1.4.3 Service certificate usage
   These rules are documented in the TSPS.

1.5 Policy administration

1.5.1 Responsibility for the document and contact data
   These rules are documented in the TSPS.

1.5.2 Reporting security incidents with certificates
   These rules are documented in the CP.

1.5.3 Compatibility of CPs of external CAs with this CPS
   The general rules are documented in the TSPS.

QCP-w, EVCP
   TLS certificates or their sub-CAs and root CAs comply with the requirements of the CA/Browser Forum’s Guidelines for Extended Validation Certificates [EVGL] as well as with [EN 319 411-1] and [EN 319 411-2]. In the event of inconsistencies between this document and the guidelines referred to, [EVGL] and [EN 319 411-1] as well as [EN 319 411-2] have priority.

QCP-w with PSD2 extension
   TLS certificates or their sub-CAs and root CAs comply with the requirements of [EN 319 411-1], [EN 319 411-2] as well as [TS 119 495]. In the event of inconsistencies between this document and the guidelines referred to, [EN 319 411-1], [EN 319 411-2] as well as [TS 119 495] have priority.

QCP-I
   Seal certificates or their sub-CAs and root CAs comply with the requirements of [EN 319 411-1], [EN 319 411-2] and [eIDAS]. In the event of inconsistencies between this document and the regulations referred to, [eIDAS] and [EN 319 411-2] have priority.

1.6 Definitions and acronyms

1.6.1 Definitions and names
   These rules are documented in the CP.

1.6.2 Acronyms
   Other rules are documented in the CP.

1.6.3 References
   These rules are documented in the CP.
2. Publication and Repository Responsibility

2.1 Repositories

The status of certificates can be requested via OCSP from the repository service where they remain for up to at least one year after the certificates have expired.

**QCP-n-qscd, QCP-l-qscd, QCP-l**

The status of certificates can be permanently requested via OCSP.

Other rules are documented in the CP.

2.2 Publication of certificate information

The TSP publishes the following information:

- EE certificates
- Certificate status of TLS demo websites
- This CPS
- The Subscriber Agreement
- Cross certificates
- PKI user information for qualified trust services.

Other rules are documented in the TSPS.

2.3 Publication frequency

**QCP-w, EVCP, OVCP, DVCP, LCP**

One precondition when applying for EE certificates is consent for their publication. Published EE certificates can be retrieved until the end of their validity term and at least up to the end of the following year.

**QCP-l**

Prior consent to publication is a precondition for the request. Published EE certificates can be retrieved until the end of their validity term plus at least ten years and until the end of the year.

**V-PKI**

V-PKI certificates are for a closed user group; they are governed by BSI and are not published in a public LDAP.

Publication takes place immediately after the certificate is issued.

CA certificates are published after their creation and maintained after the validity of the CA has expired:

- at least 10 years (QCP-l, QCP-w, EVCP) and until the end of the year or
- at least 1 year and until the end of the year (OVCP, DVCP, LCP).

Certificate revocation lists are issued regularly and until the end of validity of the issuing CA certificate. Certificate revocation lists are issued and published immediately following certificate revocation. Even if no certificates were revoked, the TSP ensures that a new certificate revocation list is created every 12
Certification Practice Statement of the D-TRUST CSM PKI

hours. The certificate revocation lists are retained and kept for a minimum period of one year following expiration of the validity of the CA.

CA revocation lists that are issued by root CAs are issued and published at least every 12 months even if no certificates were revoked.

This CPS is published and remains available for retrieval as long as the certificates that were issued on the basis of this CPS remain valid.

The websites of the TSP can be accessed publicly and free of charge 24/7.

2.4 Repository access control

These rules are documented in the TSPS.

2.5 Access to and use of services

These rules are documented in the CP.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of names

CA and EE certificates generally contain information regarding the issuer and the subscriber and/or the end-entity (subject). In line with the [X.509] standard, these names are given as DistinguishedName.

Alternative names can be registered and included in the subjectAltName extension of the certificates.

3.1.2 Need for telling names

The DistinguishedName used is unambiguous within this PKI if it is not an TLS certificate.

Unambiguous assignment of the certificate to the subscriber (and to the end-entity in the case of certificates for natural persons) is ensured.

In the case of alternative names (subjectAltName), there is no need for telling names with the exception of TLS certificates (including EV certificates).

This information may not include any references to the certificate itself. IP addresses are not permitted.

3.1.3 Anonymity or pseudonyms of subscribers

Pseudonyms are used exclusively for natural persons. Pseudonyms are generally assigned by the TSP.

In the case of certificates that were created with pseudonyms, the TSP or the RA also documents the subject’s (and, if applicable, the subscriber’s) real identity.

3.1.4 Rules for the interpretation of different name forms

The attributes of the DistinguishedName (DN components) of EE certificates are interpreted as follows:
<table>
<thead>
<tr>
<th>DN component (GivenName)</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>G</strong></td>
<td>Given name(s) of the natural person</td>
</tr>
<tr>
<td></td>
<td>QCP-I, QCP-w, EVCP, OVCP, DVCP: This field is not used.</td>
</tr>
<tr>
<td></td>
<td>LCP: According to the proof used for identification</td>
</tr>
<tr>
<td><strong>SN</strong> (Surname)</td>
<td>Surname of the natural person</td>
</tr>
<tr>
<td></td>
<td>QCP-I, QCP-w, EVCP, OVCP, DVCP: This field is not used.</td>
</tr>
<tr>
<td></td>
<td>LCP: According to the proof used for identification</td>
</tr>
<tr>
<td></td>
<td>If pseudonyms are used, SN corresponds to CN.</td>
</tr>
</tbody>
</table>

**CN (commonName) (2.5.4.3)**

- **Common name:** The following variants are used:
  - Natural persons without a pseudonym: "Surname, name used".
  - Natural persons with a pseudonym: "Pseudonym:PN".
  - Legal entities: Official name of the organization (company, public authority, association, etc.), if necessary, reduced to a meaningful name if the maximum number of 64 characters is exceeded.
  - Special case: It is also possible to include one or more domain names in the CN.
  - QCP-w, EVCP: Wildcards are not permitted for TLS certificates.
  - Function or group of persons: Name of the function or group of persons preceded by the abbreviation "GRP:" in order to indicate that this is a group certificate.
  - V-PKI: In the V-PKI, certificates that are issued for a group of people are referred to as function certificates. If the CN does not indicate the function, "FKT" is used in the CN. The subscriber is responsible for ensuring that the private key of a function certificate from the V-PKI is not used by more than 30 people at the same time.
  - Technical components: Name of the server, service or application using the certificate

**Alternative applicant (SAN)**

The following variants are used:
- E-mail address of the subscriber
- Technical components: Name of the server, service or application using the certificate

Special case: It is also possible to include one or more domain names in the SAN.
QCP-w, EVCP: Wildcards are not permitted for TLS certificates.

**PN (Pseudonym)**

- **Pseudonym:** Identical to CN.
- V-PKI: No pseudonyms are assigned.
<table>
<thead>
<tr>
<th>DN component</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number (serialNumber)</td>
<td><em>Serial number</em>: Name suffix number to ensure unambiguity of the name (typically the application number). Special case for EV certificates according to [EVGL]: Register number if assigned, date of registration or establishment. Other product-specific uses of the field are possible.</td>
</tr>
<tr>
<td>O (organizationName)</td>
<td>Official name of the subscriber or name of the organization to which the end-entity belongs or to which he or she is affiliated (company, public authority, association, etc.) according to the proof of existence; if necessary, abbreviated to a meaningful name if the maximum number of 64 characters is exceeded. DVCP: This field is not used.</td>
</tr>
<tr>
<td>OU (organizationalUnit Name)</td>
<td><em>Organization unit</em> (department, division or other unit) of the organization DVCP: This field is not used.</td>
</tr>
</tbody>
</table>
### Certification Practice Statement of the D-TRUST CSM PKI

<table>
<thead>
<tr>
<th>DN component</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>OrgID</td>
<td><strong>LCP (Seal ID):</strong></td>
</tr>
<tr>
<td>(organizationIdentifier)</td>
<td>Unambiguous organization number of the organization.</td>
</tr>
<tr>
<td>(2.5.4.97)</td>
<td>The number of the commercial register as well as the VAT ID number or a number assigned by D-TRUST can be entered.</td>
</tr>
<tr>
<td></td>
<td>The number assigned by D-TRUST is based on the format according to variant 3 in section 5.1.4 of EN 319 412-1 and is made up as follows:</td>
</tr>
<tr>
<td></td>
<td>DT:DE-1234567890 (DT: D-TRUST; DE: Germany; random number that is unambiguously assigned to the organization).</td>
</tr>
<tr>
<td>QCP-l and QCP-w with PSD2 extension:</td>
<td><strong>PSD2 Authorisation Number</strong></td>
</tr>
<tr>
<td></td>
<td>In the case of certificates that are used in PSD2 according to [TS 119 495], the organization identifier (2.5.4.97) must be used.</td>
</tr>
<tr>
<td></td>
<td>The “Authorisation Number” ensures unambiguity.</td>
</tr>
<tr>
<td></td>
<td>The “Authorisation Number” comprises the following characters:</td>
</tr>
<tr>
<td></td>
<td><strong>PSD&lt;cc&gt;-&lt;x..x&gt;-&lt;y..y&gt;</strong></td>
</tr>
<tr>
<td></td>
<td>where</td>
</tr>
<tr>
<td></td>
<td>&quot;PSD“ – &quot;legal person identity type&quot;, contains three characters;</td>
</tr>
<tr>
<td></td>
<td>&lt;cc&gt; ISO 3166 country code of the national competent authority (NCA) – precisely two characters</td>
</tr>
<tr>
<td></td>
<td>minus hyphen &quot;-&quot;</td>
</tr>
<tr>
<td></td>
<td>&lt;x..x&gt; Identifier of the NCA – 2 – 8 capital letters A – Z,</td>
</tr>
<tr>
<td></td>
<td>no blanks</td>
</tr>
<tr>
<td></td>
<td>minus hyphen &quot;-&quot;</td>
</tr>
<tr>
<td></td>
<td>&lt;y..y&gt; Identifier of the payment service provider, as defined by the NCA</td>
</tr>
<tr>
<td></td>
<td>- any sequence of characters</td>
</tr>
<tr>
<td></td>
<td>Example: PSDDE-BAFIN-1234Ab</td>
</tr>
<tr>
<td>C</td>
<td>The notation of the country to be stated corresponds to [ISO 3166] and is set up as follows: If an organization O is listed in the DistinguishedName, the organization’s place of business in the register determines the entry in the certificate. If no organization O is entered, the country is listed which issued the document that was used to identify the subscriber.</td>
</tr>
<tr>
<td>(countryName)</td>
<td>(2.5.4.6)</td>
</tr>
<tr>
<td>Street</td>
<td>Postal address Street</td>
</tr>
<tr>
<td>(streetAddress)</td>
<td>(2.5.4.9)</td>
</tr>
</tbody>
</table>
Certification Practice Statement of the D-TRUST CSM PKI

<table>
<thead>
<tr>
<th>DN component</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locality</td>
<td>Postal address <em>City</em></td>
</tr>
<tr>
<td>(localityName)</td>
<td></td>
</tr>
<tr>
<td>(2.5.4.7)</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Postal address <em>(Federal) state</em></td>
</tr>
<tr>
<td>(stateOrProvinceName)</td>
<td></td>
</tr>
<tr>
<td>(2.5.4.8)</td>
<td></td>
</tr>
<tr>
<td>PostalCode</td>
<td>Postal address <em>Postal code</em></td>
</tr>
<tr>
<td>(postalCode)</td>
<td></td>
</tr>
<tr>
<td>(2.5.4.17)</td>
<td></td>
</tr>
<tr>
<td>BusinessCategory</td>
<td>Business Category</td>
</tr>
<tr>
<td>(businessCategory)</td>
<td></td>
</tr>
<tr>
<td>(2.5.4.15)</td>
<td></td>
</tr>
<tr>
<td>Jurisdiction Of Incorporation Locality</td>
<td>Jurisdiction of the organization according to [EVGL]: <em>City</em></td>
</tr>
<tr>
<td>(jurisdictionLocalityName)</td>
<td>(1.3.6.1.4.1.311.60.2.1.1)</td>
</tr>
<tr>
<td>Jurisdiction Of Incorporation State Or Province Name</td>
<td>Jurisdiction of the organization: <em>(Federal) state</em></td>
</tr>
<tr>
<td>(jurisdictionStateOrProvinceName)</td>
<td>(1.3.6.1.4.1.311.60.2.1.2)</td>
</tr>
<tr>
<td>Jurisdiction Of Incorporation CountryName</td>
<td>Jurisdiction of the organization according to [EVGL]: <em>Country</em></td>
</tr>
<tr>
<td>(jurisdictionCountryName)</td>
<td>(1.3.6.1.4.1.311.60.2.1.3)</td>
</tr>
</tbody>
</table>

**QCP-w², EVCP**

TLS certificates contain at least the subject-DN components: “organizationName”, “commonName”, “serialNumber”, “jurisdictionCountryName”, “localityName”, “streetAddress”, “countryName”, “postalCode”, “businessCategory” as well as “subjectAltName”.

² In the case of QCP-w certificates with PSD2 extension, the “organizationIdentifier” is additionally used and checked.
Certification Practice Statement of the D-TRUST CSM PKI

QCP-l
Qualified certificates for legal entities include, as a minimum, the subject DN components: "commonName", "countryName", "serialNumber" and "organizationName" as well as "organizationIdentifier".

It is not necessary to use all the DN components mentioned here. Further components can be added. Additional DN components must comply with [RFC 5280], [RFC 6818] and [ETSI EN 319 412].

3.1.5 Unambiguity of names
The TSP ensures that the subscriber’s and/or subject’s ("Subject" field) name (DistinguishedName) used in EE certificates is always assigned to the same subscriber or subject, respectively, within the PKI provided via the CSM. The serial number ensures the unambiguity of the certificate.

The TSP ensures the unambiguity of DistinguishedNames in CA certificates.

3.1.6 Recognition, authentication and the role of brand names
The subscriber is liable for compliance with intellectual property rights in the application and certificate data (see Certificate Policy of D-Trust GmbH, section 9.5).

QCP-w, EVCP
The TSP takes any steps which are necessary to ensure that, at the time the certificate is issued, the party named in the "Subject" field of the certificate has proven control of the domain or domain components contained in the SAN field.

3.2 Initial identity verification

3.2.1 Proof of ownership of the private key
Two cases are distinguished:

a) Key pairs of subscribers are produced in the TSP's sphere of responsibility. The TSP forwards the tokens or soft PSE (LCP) and, if applicable, the PIN letters according to section 4.4.1 to the subscribers and thereby ensures that the subscribers receive the private keys.

b) Key pairs are produced in the subscriber's sphere of responsibility. Ownership of the private keys must be either technically proven or plausibly confirmed by the subscriber. By sending a PKCS#10 request to the TSP, the subscriber issues binding confirmation of private key ownership.

3.2.2 Identification and authentication of organizations and domains
Organizations that are either named in the certificate or in whose names certificates are issued must provide unambiguous proof of their identity.

Subscriber identification and application validation are subject to the requirements of [EN 319 411-1] and depending on the application, LCP, EVCP EVCP or OVCP, or the requirements of [EN 319 411-1] and [EN 319 411-2] for QCP-w or QCP-l. This validation covers all DN components.

On the different policy levels, the DN components are subjected to the validation procedures above according to section 3.1.4 plus further attributes, if necessary. The procedures shown in the table below are described in section 4.2.1.
If the application is submitted on behalf of a legal entity, the representative must (in analogy to the procedure for proving affiliation with an organization according to section 3.2.3) prove his or her authorization to this effect and authenticate or, if applicable, identify themselves for qualified seal certificates according to QCP-I and for qualified website certificates according to QCP-w.

**Documents in non-Latin characters are not accepted.**

### 3.2.3 Identification and authentication of natural persons

Natural persons applying for certificates must provide unambiguous proof of their identity and, when necessary, also that their organization has authorized them to submit the application.

**LCP, V-PKI**

Natural persons or legal entities who request certificates for other subscribers must prove that they are authorized to apply for certificates.

The verification methods described are applied as follows to the DN components according to section 3.1.4 plus further attributes, if necessary and applicable. The procedures mentioned are described in section 4.2.1.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>QCP-w, EVCP</th>
<th>OVCP</th>
<th>DVCP</th>
<th>QCP-I</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN</td>
<td>Register/Non-Register/Domain/CAA</td>
<td>Register/Non-Register/Domain/CAA</td>
<td>Domain</td>
<td>Register/Non-Register</td>
</tr>
<tr>
<td>C</td>
<td>Register/Non-Register/Domain</td>
<td>Register/Non-Register/Domain</td>
<td>n.a.</td>
<td>n.a.</td>
</tr>
<tr>
<td>O</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
</tr>
<tr>
<td>OrgID</td>
<td>Register:</td>
<td>n.a.</td>
<td>n.a.</td>
<td>Register</td>
</tr>
<tr>
<td>OU</td>
<td>C confirmation/A confirmation</td>
<td>C confirmation/A confirmation</td>
<td>n.a.</td>
<td>C confirmation/A confirmation</td>
</tr>
<tr>
<td>STREET</td>
<td>Register/Non-Register</td>
<td>Register/Non-Register</td>
<td>n.a.</td>
<td>Register/Non-Register</td>
</tr>
<tr>
<td>L</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
</tr>
<tr>
<td>State</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
</tr>
<tr>
<td>PostalCode</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
</tr>
<tr>
<td>Alternative applicant (SAN)</td>
<td>Domain/CAA</td>
<td>Domain/CAA</td>
<td>Domain/CAA</td>
<td>n.a.</td>
</tr>
<tr>
<td>All other attributes</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
<td>n.a.</td>
</tr>
</tbody>
</table>

G                  | Pers-Ident                                       | HR-DB/Dok-Ident/Pers-Ident                |

SN
In the case of applications for certificates for groups, functions or IT processes, all attributes shown in the table for the end-entity (except for OU, e-mail address, all other attributes unless relevant for the certificate) are verified. The inclusion of names for groups, functions or IT processes in the CN is subject to the procedures analogous to the "All other attributes" line.

**Documents in non-Latin characters are not accepted.**

3.2.4 Non-verified subscriber information

Verification of the subscriber's information is carried out or skipped according to sections 3.2.2, 3.2.3 and 4.2.1. In the case of alternative names, only the e-mail addresses or their domain components are generally verified. Other certificate contents, e.g. LDAP directories, etc. as well as certificate extensions (AdditionalInformation, monetaryLimit, etc.), if any, are not checked for correctness.

TLS certificates according to QCP-w and EVCP are an exception because the alternative name is used here to include further URLs. In these cases, domains in dNSNames are also verified.

3.2.5 Verification of request authorization

In the case of natural persons, the identity and, if necessary or applicable, affiliation with the organization concerned will be determined and verified and/or confirmed using the specific procedures according to section 3.2.3.

In the case of organizations, proof of their existence and the right of an authorized signatory to represent the organization in question is verified and/or confirmed according to section 3.2.2. Furthermore, at least one technical representative is identified in person or using an appropriate identification method.

3.2.6 Criteria for interoperation

See section 1.5.3.
3.3 Identification and authentication for re-keying requests

Re-keying is equivalent to the production of new certificates and, if applicable, tokens and keys for the same end-entity. Re-keying is offered for OVCP, DVCP, V-PKI and LCP certificates only, but not for TLS certificates according to EVCP or QCP-w. In the case of these certificates, the complete identification and registration process which also applies to first-time applications must be carried out. It is, however, possible to re-use existing proof and verification documents in as far as they are still valid as such according to [EVGL].

3.3.1 Routine re-keying applications

Identification does not have to be repeated in the case of re-keying applications as long as the proof deposited at the TSP can still be used. Re-keying applications must be submitted electronically via the agreed interface.

**EVCP, QCP-w**

According to EVGL 11.14.3, already validated data may only be used for a maximum period of 13 months. After that, this data must be validated once again. Exceptions are the reissuance of an EV certificate according to EVGL 11.14.2 and any other matter that may be permitted in EVGL 11.14.1. In addition, different terms and conditions may be agreed to between the CA and the requester regarding names, titles, agencies and authorities in accordance with EVGL 11.14.3 (G).

Procedures other than the above can be agreed to on a case-to-case basis. The conditions of section 4.7 must be fulfilled.

3.3.2 Re-keying following certificate revocation

Re-keying on the basis of a certificate that has been revoked is not offered.

3.4 Identification and authentication of revocation requests

Revocation authorization is verified as follows:

- If a revocation request is received in a signed e-mail, revocation must be requested by the subscriber himself or herself, or the party requesting revocation must have been named as a third party authorized to revoke and whose certificate must be available to the TSP. (LCP only)
- In the case of revocation requests submitted by telephone or in the case of a request by e-mail without a signature, the party authorized to revoke must state the correct password.
- Revocation requests can only be submitted via the online interface if the party requesting revocation can unambiguously authenticate itself to the interface.

Other procedures for authenticating revocation requests can be agreed to with the subscriber.

**LCP, V-PKI**

Revocation requests by end-entities can generally be addressed to the technical contact of the RA who then triggers a revocation order at the TSP via the agreed online interface. Unambiguous authentication of the technical contact to the online interface of the TSP is mandatory. In the event that the technical contact has communicated the revocation password to the end-entity, the end-entity can then also use other revocation methods.

Revocation procedures are defined in section 4.9.
4. Operational Requirements

4.1 Certificate request and registration

4.1.1 Request authorization

Requests can only be submitted by natural persons and legal entities (or their authorized representatives).

Group or team certificates are issued for legal entities and individual companies only.

**QCP-w, EVCP**

Subscribers must fulfil the requirements of [EVGL].

The TSP is entitled to reject requests (see section 4.2.2).

4.1.2 Registration process and responsibilities

The general rules are documented in the TSPS.

The QCP-I, QCP-w, EVCP, OVCP, DVCP, and LCP policy levels referred to in section 1.1.3 are applicable in this CPS. The registration process and responsibilities for the respective policy level are described in the TSPS.

In addition to the TSPS, the following rule is also applicable to OVCP level:

In the CSM, the customer can choose an OVCP product with or without CT logging.

4.2 Processing the certificate request

4.2.1 Performing identification and authentication processes

The general rules are documented in the TSPS.

As part of the CSM CPS, different methods of identification are permitted depending on the policy level. The tables in sections 3.2.2 and 3.2.3 show which method of identification and authentication are permitted depending on the policy level. These are listed below and will be explained in the TSPS:

**Pers-Ident**

**Dok-Ident**

**Register**

**Non-Register**

**HR-DB**

**C confirmation**

**A confirmation**

**Out-of-band mechanisms**

**Domain**

**E-mail address**

**CAA**

Identification and authentication are carried out according to sections 3.2.2 and 3.2.3.

4.2.2 Acceptance or rejection of certificate requests

These rules are documented in the TSPS.
4.2.3 Deadlines for processing certificate requests
These rules are documented in the TSPS.

4.3 Certificate issuance

4.3.1 Procedure of the TSP for issuing certificates
The general rules are documented in the TSPS.
As part of the CSM CPS, the following specific rules are also applicable:

**EVCP, QCP-w\(^3\), OVCP\(^4\), DVCP**

When issuing TLS certificates, D-Trust GmbH uses Certificate Transparency (CT) according to RFC 6962. Some browsers require publication of all TLS certificates issued by the CA in at least three auditable logs of external providers.

4.3.2 Notification of the subscriber that the certificate has been issued.
These rules are documented in the TSPS.

4.4 Certificate handover

4.4.1 Certificate handover procedure

**LCP, V-PKI**

Certificates whose private key was produced in the area of the TSP are made available for access-protected and TLS-encrypted download and/or via an TLS-protected interface (CSM) or sent by e-mail (the PKCS#12 file is protected with a PIN).

**QCP-1, QCP-w, EVCP, OVCP, DVCP, LCP**

If a certificate is issued for a key pair that the subscriber already has, the certificate is either made available for download (for instance, published in the repository service) or sent electronically.

Other methods can be agreed to on a customer-specific basis.

The general rules are documented in the TSPS.

4.4.2 Publication of the certificate by the TSP

The certificates produced will be generally published in the public repository service.

The status can be retrieved via OCSP after production.

**V-PKI**

V-PKI certificates are for a closed user group; they are governed by BSI and are not published in a public LDAP. A revocation list is generated. No OCSP status query service is provided in the V-PKI.

---

\(^3\) Not applicable to QCP-w with PSD2 extension.

\(^4\) Only applicable when the product was selected with CT logging when ordered.
4.4.3 Notification of other PKI entities concerning issuance of the certificate

Third parties authorized to request revocation according to section 4.9.2 are notified in writing and receive the revocation password unless anything to the contrary was agreed to with the organization or the party authorized to request revocation.

4.5 Key pair and certificate usage

4.5.1 Use of the private key and of the certificate by the subscriber

Subscribers and end-entities are entitled to use their private keys exclusively for those applications which are in conformity with the types of use stated in the certificate.

QCP-I, QCP-w

Once the validity period has expired or the certificate has been revoked, the pertinent private keys may no longer be used.

The provisions in section 1.4 apply to subscribers.

4.5.2 Public key and certificate usage by relying parties

These rules are documented in the TSPS.

4.6 Certificate renewal

The rules laid down in sections 4.7 and 3.3 apply.

4.7 Certificate renewal with re-keying

Certificate renewal is the re-issuance of a certificate that is based on the content data of the original certificate. The CP and CPS in effect at the time of renewal apply to the renewed certificates.

Certificate renewal is not performed for CA keys.

Different procedures can be agreed to on a case-to-case basis and the TSP decides on their implementation if such procedures are not subject to certification according to EN 319 411-1. The conditions of section 3.3 must be fulfilled.

4.7.1 Conditions for certificate renewal

In the event that any material changes in the terms of use have come into effect, the subscriber will be informed thereof. The subscriber confirms the new terms.

In contrast to a new application for a certificate, the initial identification process can be omitted for certificate renewal requests.

This is, however, conditional upon the certificate being issued for the same end-entity. The certificate to be renewed must still be valid at the time the electronic application for certificate renewal is submitted or validated data and documents for the renewal are available and can be used.

LCP

A reloading procedure can be implemented on the basis of an agreement to this effect. The application is then submitted by authorized representatives, and the subscriber in person agrees to the new certificate to be reloaded onto his or her card as well as new terms of use, if any, by entering the PIN as part of the reloading process.
V-PKI

Certificate renewal is understood to be the issuance of a follow-up certificate with the same content data as the old certificate but with a new key. Requests to renew certificates must be submitted at least six weeks before the certificate expires. Requests are submitted, as described in 3.2.3, by the certificate holder or by an authorized representative via the agreed online interface. If necessary, the applicant must accept the new terms of use.

4.7.2 Authorization for certificate renewal

Each subscriber who is authorized (pursuant to section 4.1.1) to submit a certificate application can apply for certificate renewal if the conditions pursuant to section 4.6 are fulfilled and if the TSP offers a corresponding procedure for the chosen product.

4.7.3 Processing an application for certificate renewal

Subscribers who are authorized to apply for certificate renewal use an online interface of the TSP which is made available on a product-specific basis for submitting applications.

Applications submitted via the corresponding interfaces are automatically checked for authorization and contents.

4.7.4 Notification of the subscriber concerning issuance of a new certificate

The rules laid down in section 4.3.2 apply.

4.7.5 Procedure in conjunction with the issuance of a certificate renewal

The certificate generated is made available via the provided online interface. The rules laid down in section 4.4.1 are also applicable.

4.7.6 Publication of certificate renewal by the TSP

The rules laid down in section 0 apply.

4.7.7 Notification of other PKI entities concerning certificate renewal

The rules laid down in section 0 apply.

4.8 Certificate modification

These rules are documented in the TSPS.

4.9 Certificate revocation and suspension

4.9.1 Conditions for certificate revocation

These rules are documented in the TSPS.

Parties authorized to request revocation must identify themselves according to section 0.

4.9.2 Authorization to revoke

These rules are documented in the TSPS.
4.9.3 Revocation request procedure

Certificates can be generally revoked 24/7 by subscribers and/or their authorized representatives using the agreed online interface. Revocation at a future point in time is not offered. Revocation via the online interface becomes effective immediately.

Revocation requests by end-entities can generally be addressed to the technical contact of the RA who then triggers a revocation order at the TSP via the agreed online interface. The technical contact of the RA must unambiguously identify himself or herself to the online interface of the TSP.

Certificate revocation by phone is not possible.

Other revocation methods can be agreed to.

The TSP is responsible for revoking a certificate. Notwithstanding this, the TSP can subcontract part of its tasks. The certificate revocation service can be performed by third parties acting on the basis of the requirements of the TSP.

The operating instructions and procedures set forth strict rules for performing the revocation service and include a detailed description of processes, workflows and rules for problem handling.

The reasons for revocation given by the party requesting revocation are documented. Following revocation, the subscriber and/or end-entity will be informed about revocation. The subscriber can inform the end-entity if this was agreed to.

Authentication of persons authorized to revoke certificates is carried out according to section 3.4.

PSD2-specific revocation procedure

Public authorities only, as the issuers of PSD2-specific attributes, can submit their revocation requests to the following e-mail address:

E-mail address: sperren@d-trust.net

This revocation procedure is only provided for NCA authorities using the PSD2 method.

4.9.4 Revocation request deadlines

These rules are documented in the TSP's.

4.9.5 Time span for processing a revocation request by the TSP

Revocation requests can be submitted 24/7 via the online interface. Revocation takes place according to section 4.9 [BRG] within 24 hours after successful authorization of the party requesting revocation.

4.9.6 Methods available for validating revocation information

Up-to-date revocation information is maintained in certificate revocation lists which can be retrieved via the LDAP protocol or the link shown in section 2.1. An OCSP service is additionally available. The availability of these services is indicated in the certificates in the form of URLs. Furthermore, revocation information is also available from the TSP's website (see section 2.1). Delta CRLs are not used.

The integrity and authenticity of the revocation information are ensured by a signature of the CRL and/or the OCSP response.

Information on status and revocation (OCSP and CRL) is consistent.
Status changes in the OCSP are available for query immediately after revocation. Status changes in a CRL contain the same revocation information. However, distribution of a new CRL takes place with a time delay after revocation.

Revocation entries in certificate revocation lists remain there at least until the certificate’s term of validity has expired.

**QCP-I**

Revocation entries remain in the associated certificate revocation lists after the respective certificate validity has expired.

4.9.7 Publication frequency of certificate revocation lists
See section 2.3.

4.9.8 Maximum latency time for certificate revocation lists
Certificate revocation lists are created immediately and published after 60 minutes at the latest.

4.9.9 Online availability of revocation information
An OCSP service is available for online verification. The availability of this service is indicated in the certificates in the form of a URL.

**V-PKI**

As part of the V-PKI, a certificate revocation list is issued. The CRL is stated in the certificates in the form of a URL. No OCSP status query service is provided.

4.9.10 Need for online verification of revocation information
These rules are documented in the TSPS.

4.9.11 Other forms for notification of revocation information
These rules are documented in the TSPS.

4.9.12 Special requirements if the private key is compromised
These rules are documented in the TSPS.

4.9.13 Conditions for suspension
These rules are documented in the TSPS.

4.10 Certificate status services

4.10.1 Operation of the certificate status service
These rules are documented in the TSPS.

4.10.2 Availability of the certificate status service
These rules are documented in the TSPS.

4.10.3 Optional services
These rules are documented in the TSPS.
4.11 Withdrawal from the certification service

These rules are documented in the TSPS.

4.12 Key escrow and recovery

The TSP does not offer key escrow. The subscriber is free to deposit keys in his or her own sphere of responsibility.

4.12.1 Escrow and recovery procedures for private keys
The TSP does not offer key escrow.

4.12.2 Conditions and procedures for escrow and recovery of session keys
The TSP does not offer key escrow.

5. Facility, Management and Operational Controls

The descriptions in this section refer to the CAs operated by D-Trust GmbH in accordance with [EN 319 411-1] and [EN 319 411-2].

Other rules are documented in the TSPS.

5.1 Physical controls

These rules are documented in the TSPS.

5.2 Procedural controls

5.2.1 Role and authorization concept
These rules are documented in the TSPS.

5.2.2 Four-eyes principle
These rules are documented in the TSPS.

5.2.3 Identification and authentication for individual roles
These rules are documented in the TSPS.

5.2.4 Role exclusions
These rules are documented in the TSPS.

5.3 Personnel controls

The TSP meets the requirements concerning personnel as laid down in [EN 319 411-1] and [EN 319 411-2].

5.3.1 Qualifications, experience and clearance requirements
These rules are documented in the TSPS.
5.3.2 Background checks
These rules are documented in the TSPS.

5.3.3 Training
These rules are documented in the TSPS.

5.3.4 Frequency of training and information
These rules are documented in the TSPS.

5.3.5 Job rotation frequency and sequence
These rules are documented in the TSPS.

5.3.6 Sanctions for unauthorized actions
These rules are documented in the TSPS.

5.3.7 Independent contractor requirements
These rules are documented in the TSPS.

5.3.8 Documentation supplied to personnel
These rules are documented in the TSPS.

5.4 Audit logging procedures

5.4.1 Monitoring access
These rules are documented in the TSPS.

5.4.2 Risk monitoring
These rules are documented in the TSPS.

5.5 Records archival

5.5.1 Types of records archived
These rules are documented in the TSPS.

5.5.2 Retention period for archive
These rules are documented in the TSPS.

5.5.3 Archive protection
These rules are documented in the TSPS.

5.5.4 Archive data backup
These rules are documented in the TSPS.

5.5.5 Requirements for time stamping of records
These rules are documented in the TSPS.
5.5.6 Archiving (internally/externally)
These rules are documented in the TSPS.

5.5.7 Procedure for obtaining and verifying archive information
These rules are documented in the TSPS.

5.6 Key change at the TSP
These rules are documented in the TSPS.

5.7 Compromise and disaster recovery at the TSP

5.7.1 Incident and compromise handling procedures
These rules are documented in the TSPS.

5.7.2 Recovery after resources have been compromised
These rules are documented in the TSPS.

5.7.3 Compromising of the private CA key
These rules are documented in the TSPS.

5.7.4 Disaster recovery options
These rules are documented in the TSPS.

5.8 Closure of the TSP or termination of services
These rules are documented in the TSPS.

6. Technical Security Controls
The descriptions contained in this section refer to the PKI services that are referred to in this CPS and which are operated at D-Trust GmbH.

6.1 Key pair generation and installation

6.1.1 Generation of key pairs
The general rules are documented in the TSPS.

During generation of EE keys, the subscriber is required to generate these in a cryptographically secure manner in accordance with the requirements of [EN 319 411-1] and [EN 319 411-2].
V-PKI
In the case of federal government projects, when EE keys are generated, the subscriber is required to generate these in a cryptographically secure manner in accordance with the requirements of BSI [TR-02102-1].

If EE keys are generated by the TSP, these keys are generated with the help of an HSM in the secure environment of the trust service provider and in accordance with the requirements of [EN 319 411-1] and [EN 319 411-2].

6.1.2 Private key delivery to the subscriber
If the private keys are generated at the TSP, they are delivered according to section 4.4.1. The private keys are in this case stored at the TSP in a safe environment until they are delivered.

Since the key escrow option is not offered, the private key is deleted at the TSP after delivery to the subscriber.

6.1.3 Public key delivery to the TSP
QCP-w, EVCP, OVC, DVCP, LCP, V-PKI
Certificate requests can be submitted by subscribers for an existing key pair in the form of a PKCS#10 request which must be signed with the corresponding private key. The PKCS#10 request contains the public key. The corresponding response returns the complete certificate.

6.1.4 CA public key delivery to relying parties
The CA public key is contained in certificate. This certificate is normally contained in the token which is delivered to the subscriber. Furthermore, CA certificates can be obtained from the public repository where they are published after their generation.

6.1.5 Key lengths
These rules are documented in the TSPS.

6.1.6 Determining the key parameters and quality control
These rules are documented in the TSPS.

The signature and encryption algorithms are mentioned in section 0.

6.1.7 Key usage purposes
These rules are documented in the TSPS.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls
The general rules are documented in the TSPS.

If the private EE keys are generated in the subscriber's sphere of responsibility, the subscriber must also ensure sufficient quality during key generation.

V-PKI
The "CryptoServer CP 5 VS-NfD Version 5.1.0.0" HSM approved by BSI (BSI-VSA-10370) is used for key generation and storage.
LCP
The TSP operates suitable hardware-based and software-based key generators in order to warrant the quality of the EE keys.

6.2.2 Private key (n out of m) multi-person control
The HSM on which the CA keys are stored is located in the secure environment of the trust service provider. A private key must be activated by two authorized persons.
Access to private EE keys is only possible in the case of keys in escrow according to section 6.2.3.

6.2.3 Private key escrow
The TSP does not offer escrow of private EE keys.

6.2.4 Private key backup
The general rules are documented in the TSPS.
No backup is offered for private EE keys; backups are only available in the form of the key escrow option if this is available for the specific product or has been agreed to.

6.2.5 Private key archival
These rules are documented in the TSPS.

6.2.6 Transfer of private keys to or from cryptographic modules
These rules are documented in the TSPS.

6.2.7 Storage of private keys in cryptographic modules
The general rules are documented in the TSPS.
Before being delivered, EE keys are contained in encrypted form in a database of the TSP.

6.2.8 Activation of private keys
The general rules are documented in the TSPS.
Private EE keys are activated by entering the secret.

6.2.9 Deactivation of private keys
The general rules are documented in the TSPS.
The respective application deactivates the private EE key, at the latest when the soft PSE is deactivated or deleted.

6.2.10 Destruction of private keys
The general rules are documented in the TSPS.
Keys that were generated within the TSP’s area are automatically deleted after delivery.

6.2.11 Assessment of cryptographic modules
These rules are documented in the TSPS.
6.3 Other aspects of key pair management

6.3.1 Archiving of public keys
These rules are documented in the TSPS.

6.3.2 Validity periods of certificates and key pairs
The general rules are documented in the TSPS.

The term of validity of the EE keys and certificates is variable and shown in the certificate. The maximum possible validity period totals:

**QCP-w, EVCP, OVCP, DVCP**
Up until 31 August 2020, TLS certificates will be issued with the following validity period:
825 days max.

Beginning 1 September 2020, TLS certificates will be issued with the following validity period:
398 days max.

**QCP-w with PSD2 extension**
Qualified website certificates with PSD2 extension are issued with the following validity period:
825 days max.

**V-PKI**
27 months max.

**LCP**
63 months

**QCP-I**
EE certificates are issued with a maximum period of validity of 39 months.

If a certificate is issued for a period of more than 24 months, after this period, the customer bears both the risk and costs of replacement which may become necessary for security reasons.

6.4 Activation data

6.4.1 Activation data generation and installation
The general rules are documented in the TSPS.

If the key pair is generated by the subscriber, the activation secret is also produced during this process and is immediately made available to the subscriber.

**LCP, V-PKI**
If EE keys are generated by the TSP, the PIN is either sent or handed over to the subscriber in a PIN letter or made available to the subscriber via a secured TLS connection or online interface. If the subscriber is not the end-entity, then the subscriber is responsible for the secure delivery of the PIN to the end-entity.

6.4.2 Protection of activation data
The general rules are documented in the TSPS.
Subscriber: The PINs are delivered using a transport PIN method or are printed once as a specially protected PIN letter or sent or handed over to the subscriber via a TLS-secured website.

6.4.3 Other aspects of activation data
Not specified.

6.5 Computer security controls

6.5.1 Specific technical security requirements in the computer systems
These rules are documented in the TSPS.

6.5.2 Assessment of computer security
These rules are documented in the TSPS.

6.5.3 Monitoring
These rules are documented in the TSPS.

6.6 Life cycle technical controls
These rules are documented in the TSPS.

6.6.1 Security controls during development
These rules are documented in the TSPS.

6.6.2 Security controls in conjunction with computer management
These rules are documented in the TSPS.

6.6.3 Life cycle security controls
These rules are documented in the TSPS.

6.7 Network security controls
These rules are documented in the TSPS.

6.8 Time stamps
These rules are documented in the TSPS.

7. Profiles of Certificates, Certificate Revocation Lists and OCSP

7.1 Certificate profiles

7.1.1 Version numbers
These rules are documented in the TSPS.

7.1.2 Certificate extensions
These rules are documented in the TSPS.
7.1.3 Algorithm OIDs

The following encryption algorithm is currently used in CA and EE certificates:
- RSA with OID 1.2.840.113549.1.1.1
- RSA-PSS with OID 1.2.840.113549.1.1.10
- ECDSA (secp384r1) with OID 1.3.132.0.34

The following signature algorithms are currently used in CA and EE certificates:
- SHA512 RSA with OID 1.2.840.113549.1.1.13
- SHA256 RSA with OID 1.2.840.113549.1.1.11
- SHA384 ECDSA with OID 1.2.840.10045.4.3.3

SHA1 is not used.

7.1.4 Name formats

These rules are documented in the TSPS.

7.1.5 Name constraints

These rules are documented in the TSPS.

7.1.6 Certificate Policy Object Identifier

These rules are documented in the TSPS.

7.1.7 Use of the "PolicyConstraints" extension

These rules are documented in the TSPS.

7.1.8 Syntax and semantics of "PolicyQualifiers"

These rules are documented in the TSPS.

7.1.9 Processing the semantics of the critical "CertificatePolicies" extension

These rules are documented in the TSPS.

7.2 CRL profiles

7.2.1 Version number(s)

These rules are documented in the TSPS.

7.2.2 Extensions of certificate revocation lists and certificate revocation list entries

These rules are documented in the TSPS.

7.3 OCSP profiles

These rules are documented in the TSPS.

7.3.1 Version number(s)

These rules are documented in the TSPS.
7.3.2 OCSP extensions

These rules are documented in the TSPS.

8. **Compliance Audit and Other Assessments**

These rules are documented in the TSPS.

9. **Other Business and Legal Matters**

With regard to the corresponding provisions, see section 9 in the CP.
Certification Practice Statement der D-TRUST CSM PKI

Version 3.0
COPYRIGHT UND NUTZUNGS-LIZENZ

Certification Practice Statement der D-TRUST CSM PKI
©2020 D-Trust GmbH

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

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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Datum</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>09.02.2015</td>
<td>Initialversion</td>
</tr>
<tr>
<td>1.1</td>
<td>23.02.2015</td>
<td>Editorische Änderungen im Rahmen der Erstzertifizierung gemäß ETSI 102 042 LCP. Es wurden diverse Inhalte aus der CP der D-Trust GmbH in das CPS überführt.</td>
</tr>
<tr>
<td>1.2</td>
<td>05.10.2015</td>
<td>Editorische Änderungen&lt;br&gt;Konkretisierung der Möglichkeit das Schlüsselmaterial durch den TSP erzeugen und ausliefern zu lassen&lt;br&gt;Sperrung nur noch über Online-Schnittstelle und wenn ein Sperrpasswort vereinbart wurde telefonisch&lt;br&gt;Alle neuen Zertifikate werden immer im LDAP der D-TRUST veröffentlicht</td>
</tr>
<tr>
<td>1.3</td>
<td>03.10.2016</td>
<td>Umstellung auf EN 319 411-1</td>
</tr>
<tr>
<td>2.0</td>
<td>01.01.2017</td>
<td>Einführung von qualifizierten TLS-Zertifikaten (QWACs) gemäß EN 319 411-2 und eIDAS</td>
</tr>
<tr>
<td>2.1</td>
<td>01.10.2017</td>
<td>Editorische Änderungen und Konkretisierung des Kapitels 6.5</td>
</tr>
<tr>
<td>2.2</td>
<td>28.03.2018</td>
<td>Editorische Änderungen und eine Überarbeitung der Kompatibilität mit RFC 3647&lt;br&gt;Anpassung Nutzungslicenz an „Creative Commons Attribution“&lt;br&gt;Angleichung an die Mozilla Root Store Policy 2.5</td>
</tr>
<tr>
<td>2.3</td>
<td>05.07.2018</td>
<td>Änderung der Domain-Validierungsmethoden in 4.2.1&lt;br&gt;Feld OrgID in Abschnitt 3.1.4 wurde gemäß Variante 3 aus Kapitel 5.1.4 der EN 319 412-1 ergänzt.&lt;br&gt;Redaktionelle Anpassungen</td>
</tr>
<tr>
<td>2.4</td>
<td>11.10.2018</td>
<td>Tabellarische Darstellung der CA Zertifikate in Abschnitt 1.1.3&lt;br&gt;Ergänzungen in Kapitel 7.3&lt;br&gt;Anpassungen der Abschnitte 1.5.2 und 4.9 gemäß Ballot SC6v3 aus dem CAB-Forum</td>
</tr>
<tr>
<td>2.5</td>
<td>30.11.2018</td>
<td>Dieses CPS entspricht den Anforderungen der Mozilla Policy 2.6.1&lt;br&gt;Der Hotline Dienst wird eingestellt (Abschnitt 4.9.3)&lt;br&gt;Jährliches Review des gesamten CPS&lt;br&gt;Redaktionelle Anpassungen</td>
</tr>
<tr>
<td>2.6</td>
<td>15.05.2019</td>
<td>Ergänzung der qualifizierten Website Authentication Zertifikate (QWACs) mit der Ausprägung PSD2&lt;br&gt;Jährliches Review des gesamten CPS&lt;br&gt;Redaktionelle Anpassungen</td>
</tr>
<tr>
<td>2.7</td>
<td>22.05.2019</td>
<td>Ergänzung der qualifizierten Siegelzertifikate mit der Ausprägung PSD2 ohne QSCD&lt;br&gt;Im Abschnitt 4.2.1 werden die Domainvalidierungsmethoden gemäß [BRG] um die Methoden 3.2.2.4.7, 3.2.2.4.13 und 3.2.2.4.14 ergänzt.</td>
</tr>
<tr>
<td>Vermerk</td>
<td>Datum</td>
<td>Inhalt</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2.8</td>
<td>09.10.2019</td>
<td>▪ Update nach observation report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Präzisierung des Abschnitts 5.5.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Editorische Änderungen</td>
</tr>
<tr>
<td>2.9</td>
<td>19.03.2020</td>
<td>▪ Einführung von Domain validierten TLS-Zertifikaten (DVCP) gemäß EN 319 411-1 und BRG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Dieses CPS entspricht den Anforderungen der Mozilla Policy 2.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Jährliches Review des gesamten CPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Anpassung der Aufbewahrungsfrist für LCP in Abschnitt 5.5.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Ergänzung des SHA-256 Fingerprints in Abschnitt 1.1.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Ergänzung der Domainvalidierungsmethoden in Abschnitt 4.2.1</td>
</tr>
<tr>
<td>2.10</td>
<td>27.04.2020</td>
<td>▪ Aktivierung der SubCA zur Ausstellung von DV-Zertifikaten, siehe Abschnitt 1.1.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Einbindung neuer SubCAs zur Ausstellung von EV- und OV-Zertifikaten, siehe Abschnitt 1.1.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Ergänzungen zur Verifikation der Zertifikatskette in Abschnitt 4.5.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Ergänzungen in den Abschnitten 5.3.7 und 5.5.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Reduzierung der Gültigkeitsdauer von TLS-Zertifikaten, siehe 6.3.2</td>
</tr>
<tr>
<td>2.11</td>
<td>17.06.2020</td>
<td>▪ Einführung von Verwaltungs-PKI (V-PKI) Zertifikaten gemäß BSI TR-03145-1</td>
</tr>
<tr>
<td>2.12</td>
<td>28.09.2020</td>
<td>▪ Vergabe einer D-TRUST OID für V-PKI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Veröffentlichung und Inbetriebnahme der V-PKI SubCA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Ergänzung eines Links in Abschnitt 4.2.1 zur Veröffentlichung von Registerführenden Stellen im Repository</td>
</tr>
<tr>
<td>3.0</td>
<td>10.11.2020</td>
<td>▪ Einführung eines übergeordneten Practice Statements (TSPS, V1.0) für das CSM CPS ab Version 3.0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Update nach observation report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Ergänzung in Abschnitt 3.3.1</td>
</tr>
</tbody>
</table>
Inhaltsverzeichnis

1. Einleitung .......................................................................................................................... 7
1.1 Überblick ......................................................................................................................... 7
1.2 Name und Kennzeichnung des Dokuments ................................................................. 14
1.3 PKI-Teilnehmer ............................................................................................................. 14
1.4 Verwendung von Zertifikaten ..................................................................................... 14
1.5 Administration der Policy ............................................................................................. 14
1.6 Begriffe und Abkürzungen .......................................................................................... 15

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen ........................................... 15
2.1 Verzeichnisse .................................................................................................................. 15
2.2 Veröffentlichung von Informationen zu Zertifikaten .................................................. 15
2.3 Häufigkeit von Veröffentlichungen .............................................................................. 16
2.4 Zugriffskontrollen auf Verzeichnisse .......................................................................... 16
2.5 Zugang und Nutzung von Diensten ............................................................................. 16

3. Identifizierung und Authentifizierung .............................................................................. 16
3.1 Namensregeln ................................................................................................................. 16
3.2 Initiale Überprüfung der Identität ............................................................................... 21
3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselneuerung (re-keying).................................................................................................................. 24
3.4 Identifizierung und Authentifizierung von Sperranträgen ......................................... 25

4. Betriebsanforderungen ...................................................................................................... 25
4.1 Zertifikatsantrag und Registrierung ............................................................................ 25
4.2 Verarbeitung des Zertifikatsantrags ........................................................................... 26
4.3 Ausstellung von Zertifikaten ...................................................................................... 26
4.4 Zertifikatsübergabe ....................................................................................................... 26
4.5 Verwendung des Schlüsselpaars und des Zertifikats .................................................. 27
4.6 Zertifikatserneuerung (certificate renewal) ................................................................. 28
4.7 Zertifikatserneuerung mit Schlüsselneuerung .............................................................. 28
4.8 Zertifikatsänderung ...................................................................................................... 29
4.9 Widerruf und Suspendierung von Zertifikaten ............................................................ 29
4.10 Statusabfragedienst für Zertifikate ............................................................................ 31
4.11 Austritt aus dem Zertifizierungsdienst ...................................................................... 31
4.12 Schlüsselhinterlegung und -wiederherstellung ................................................................ 31

5. Nicht-technische Sicherheitsmaßnahmen ........................................................................... 32
5.1 Bauliche Sicherheitsmaßnahmen ................................................................................. 32
5.2 Verfahrensvorschriften ............................................................................................... 32
5.3 Eingesetztes Personal ................................................................................................... 32
5.4 Überwachungsmaßnahmen .......................................................................................... 33
5.5 Archivierung von Aufzeichnungen ............................................................................. 33
5.6 Schlüsselwechsel beim TSP ....................................................................................... 33
5.7 Kompromittierung und Geschäftsweiterführung beim TSP ....................................... 33
5.8 Schließung des TSP bzw. die Beendigung der Dienste ................................................ 34

6. Technische Sicherheitsmaßnahmen .................................................................................. 34
6.1 Erzeugung und Installation von Schlüsselpaaren ........................................................ 34
6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module .......................................................................................................................... 35
6.3 Andere Aspekte des Managements von Schlüsselpaaren ......................................... 36
6.4 Aktivierungsdaten ........................................................................................................ 37
6.5 Sicherheitsmaßnahmen in den Rechneranlagen ............................................................ 37
6.6 Technische Maßnahmen während des Life Cycles ......................................................... 38
6.7 Sicherheitsmaßnahmen für Netze ................................................................................ 38
6.8 Zeitstempel .................................................................................................................. 38

7. Profile von Zertifikaten, Sperrlisten und OCSP ................................................................. 38
7.1 Zertifikatsprofile ................................................................. 38
7.2 Sperrlistenprofile ............................................................... 39
7.3 Profile des Statusabfragdienstes (OCSP) .................................. 39
8. Auditierungen und andere Prüfungen ........................................ 39
9. Sonstige finanzielle und rechtliche Regelungen .............................. 39
1. **Einleitung**

1.1 Überblick


1.1.1 Vertrauensdienstanbieter*innen

Diese Regelungen sind in der CP dokumentiert.

1.1.2 Über dieses Dokument

Die folgende Grafik skizziert die Dokumentenhierarchie der D-TRUST GmbH. Die grüne Markierung hebt das Dokument, indem Sie sich befinden, hervor.

![Diagramm der Dokumentenhierarchie](image)

Verweise werden wie folgt angezeigt:

- **Diese Regelungen sind in der CP dokumentiert.**
  Regelungen, die die Zertifikatsrichtlinien betreffen sind in der CP dokumentiert.

- **Die allgemeinen Regelungen sind im TSPS dokumentiert.**
  Die allgemeinen Regelungen sind im TPS dokumentiert und die spezifischen Regelungen verbleiben im dem CPS.

- **Die weiteren Regelungen sind im TSPS dokumentiert.**
  Über die spezifischen Regelungen im CPS gibt es noch weitere Regelungen, die im TSPS dokumentiert werden.
**Diese Regelungen sind im TSPS dokumentiert.**

Regelungen sind nur im TSPS beschrieben.

Dieses CPS nimmt Bezug auf die CP (Zertifikatsrichtlinie) der D-Trust GmbH mit der OID 1.3.6.1.4.1.4788.2.200.1, die TSPS (D-TRUST Trust Service Practice Statement) und die [EN 319 411-1] bzw. [EN 319 411-2]. Es beschreibt die Umsetzung der daraus resultierenden Anforderungen.

Soweit in diesem Dokument nicht zwischen den Zertifizierungsanforderungen bzw. Policy Levels Policy Level gemäß Abschnitt 1.1.3 unterschieden wird oder bestimmte Policy Level explizit ausgeschlossen werden, sind die Anforderungen oder Bestimmungen der jeweiligen Abschnitte auf alle Zertifikate gemäß der Klassifizierung der Zertifikatsrichtlinie der D-Trust GmbH anwendbar.


Die weiteren Regelungen sind im TSPS dokumentiert.

1.1.3 Eigenschaften der PKI


**PKI für qualifizierte Vertrauensdienste**

Abbildung 1 PKI-Hierarchie für qualifizierte Vertrauensdienste

Die EE-Zertifikate lassen sich in ihrer Ausprägung den Anforderungen der einzelnen Richtlinien (Policy Level) innerhalb der EN 319 411-2 zuordnen:

- QCP-w – Qualifizierte Webseitenzertifikate (QWAC)
- QCP-I – Qualifizierte Siegelzertifikate (QSealC)
Die Policy Level werden im TSPS erläutert.

PKI für nicht-qualifizierte Vertrauensdienste

<table>
<thead>
<tr>
<th>PKI für Nicht-qualifizierte Vertrauensdienste (publicly trusted)</th>
</tr>
</thead>
<tbody>
<tr>
<td>D-TRUST Root Class 3 CA 2 EV 2009</td>
</tr>
<tr>
<td>D-TRUST Root Class 3 CA 2 2009</td>
</tr>
<tr>
<td>D-TRUST SSL Class 3 CA 1 EV 2009</td>
</tr>
<tr>
<td>VR IDENT SSL CA 2020 (DVCP)</td>
</tr>
<tr>
<td>VR IDENT SSL CA 2020 (OVCP)</td>
</tr>
<tr>
<td>D-TRUST SSL CA 2 2009 (DVCP)</td>
</tr>
<tr>
<td>VR IDENT SSL CA 2020 (OVCP)</td>
</tr>
<tr>
<td>D-TRUST Application Certificates CA 3-1 2013 (LCP)</td>
</tr>
</tbody>
</table>

Abbildung 2 PKI-Hierarchie für nicht-qualifizierte Vertrauensdienste

Die EE-Zertifikate lassen sich in ihrer Ausprägung den Anforderungen der einzelnen Richtlinien (Policy Level) innerhalb der EN 319 411-1 zuordnen:

- LCP – Lightweight Certificate Policy
- DVCP – Domain Validation Certificate Policy
- OVCP – Organizational Validation Certificate Policy
- EVCP – Extended Validation Certificate Policy

Die Policy Level werden im TSPS erläutert.

1 Die RootCA „D-TRUST EV Root CA 1 2020“ soll zukünftig die bestehende RootCA „D-TRUST Root Class 3 CA 2 EV 2009“ ersetzen und wird hier informativ aufgeführt. Die RootCA „D-TRUST BR Root CA 1 2020“ soll zukünftig die bestehende RootCA „D-TRUST Root Class 3 CA 2 2009“ ersetzen und wird hier informativ aufgeführt.

**Vertrauensdienst der Verwaltungs-PKI (V-PKI) mit Vertrauensanker beim BSI**

![Diagram](https://example.com/diagram.png)

**Abbildung 3 PKI-Hierarchie für den Vertrauensdienst Verwaltungs-PKI (V-PKI)**


Im Rahmen der V-PKI nimmt das CSM CPS Bezug auf die CP V-PKI BSI vom Bundesamt für Sicherheit in der Informationstechnik.


Aus der Sub-CA „D-TRUST V-PKI CA 1 2020“ ist die Ausstellung von weiteren Sub-CAs bzw. Issuing-CAs nicht vorgesehen. Aus der Sub-CA dürfen Zertifikate ausschließlich für eigene Mitarbeiter des Auftraggebers ausgestellt werden, nicht für externe Mitarbeiter.

Für Zertifikate aus der V-PKI (Verwaltungs-PKI) wurde die Policy-OID 0.4.0.127.0.7.3.6.1.1.4.4 vom BSI und die Policy OID 1.3.6.1.4.1.4788.2.201.2 von D-TRUST vergeben.

**CA-Zertifikate**

Die Gesamtübersicht aller RootCAs und SubCAs mit den Policy Level QCP-w, EVCP, OVCP, DVCP und LCP aus der hervorgeht welches CPS auf die jeweilige CA Anwendung findet, ist im Repository zu finden:


Die folgende Tabelle liefert eine Übersicht über alle RootCAs und der dazugehörigen SubCAs, für die dieses CPS Anwendung findet.
**D-TRUST Root Class 3 CA 2 EV 2009**

http://www.d-trust.net/cgi-bin/D-TRUST_Root-Class_3_CA_2_EV_2009.crt

Fingerprint:
SHA1: 96C91B0B95B4109842FAD0D82279FE60FAB91683
SHA256: EEC5496B988CE98625B934092EEC2908BED0B0F316C2D4730C84EAF1F3D34881

**D-TRUST CA 2-2 EV 2016**

http://www.d-trust.net/cgi-bin/D-TRUST_CA_2-2_EV_2016.crt

Policy Level: QCP-w

Fingerprint:
SHA1: 8423CDA13FF6025B8CD3188DD837F8618C31D85D9
SHA256: 2316D05A2E2D347FA141135B98ED09F56E81F1CF5679793D3B39DD68E461A48
OID: 1.3.6.1.4.1.4788.2.150.4

**D-TRUST SSL Class 3 CA 1 EV 2009**

https://www.d-trust.net/cgi-bin/D-TRUST_SSL-Class_3_CA_1_EV_2009.crt

Policy Level: EVCP

Fingerprint:
SHA1: 1069423D308D0FC54575059638560FC7556E32B3
SHA256: B0935DC04B4E60C0C42DEF7EC57A1B1D8F958D17988E71CC80A8CF5635BA5B4
OID: 1.3.6.1.4.1.4788.2.202.1

**VR IDENT EV SSL CA 2020**

https://www.d-trust.net/cgi-bin/VR_IDENT_EV_SSL_CA_2020.crt

Policy Level: EVCP

Fingerprint:
SHA1: AC4126DEB7907EE1BBC00A6504BD2AB224237915
SHA256: 9E6C8035C0F1C8A945310E72D83E531947B571F9292E42A4248A370BF7B305BE
OID: 1.3.6.1.4.1.4788.2.230.1

**D-TRUST Root Class 3 CA 2 2009**

https://www.d-trust.net/cgi-bin/D-TRUST_Root-Class_3_CA_2_2009.crt

Fingerprint:
SHA1: 58E8AB0361533FB80F79B1B6D29D3FF8D5F00F0
SHA256: 49E7A442ACF0EA6287050054B52564B650E4F49E42E348D6AA38E039E957B1C1
<table>
<thead>
<tr>
<th>Certification Practice Statement der D-TRUST CSM PKI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>D-TRUST SSL Class 3 CA 1 2009</strong></td>
</tr>
<tr>
<td><a href="https://www.d-trust.net/cgi-bin/D-TRUST_SSL_Class_3_CA_1_2009.crt">https://www.d-trust.net/cgi-bin/D-TRUST_SSL_Class_3_CA_1_2009.crt</a></td>
</tr>
<tr>
<td>Policy Level: OVCP</td>
</tr>
<tr>
<td>Fingerprint:</td>
</tr>
<tr>
<td>SHA1: 2FC5DE6528CDBE50A14C382FC1DE524FAABF95FC</td>
</tr>
<tr>
<td>SHA256: 6AC159B4C2BC8E729F3B84642EF1286BCC80D775FE278C740ADA468D59439025</td>
</tr>
<tr>
<td>OID: 1.3.6.1.4.1.4788.2.200.1</td>
</tr>
<tr>
<td><strong>D-TRUST SSL CA 2 2020</strong></td>
</tr>
<tr>
<td><a href="https://www.d-trust.net/cgi-bin/D-TRUST_SSL_CA_2_2020.crt">https://www.d-trust.net/cgi-bin/D-TRUST_SSL_CA_2_2020.crt</a></td>
</tr>
<tr>
<td>Policy Level: DVCP</td>
</tr>
<tr>
<td>Fingerprint:</td>
</tr>
<tr>
<td>SHA1: AEB9682B91D20B50384A2C6B6DACBB851F629962</td>
</tr>
<tr>
<td>SHA256: 972A181B60294EBA07333B9C1982440D43395ABA91D450EC0EFB485AED49D5A7</td>
</tr>
<tr>
<td>OID: 1.3.6.1.4.1.4788.2.202.3</td>
</tr>
<tr>
<td><strong>VR IDENT SSL CA 2020</strong></td>
</tr>
<tr>
<td><a href="https://www.d-trust.net/cgi-bin/VR_IDENT_SSL_CA_2020.crt">https://www.d-trust.net/cgi-bin/VR_IDENT_SSL_CA_2020.crt</a></td>
</tr>
<tr>
<td>Policy Level: OVCP</td>
</tr>
<tr>
<td>Fingerprint:</td>
</tr>
<tr>
<td>SHA1: C3A6BC49BC9936E9450A9775465B7235E78EE705</td>
</tr>
<tr>
<td>SHA256: 007108194115F3C899F54EE67CB4DA87275EDC16798DA787E0758CFA6AE96B1</td>
</tr>
<tr>
<td>OID: 1.3.6.1.4.1.4788.2.230.2</td>
</tr>
<tr>
<td><strong>D-TRUST Root CA 2 2018</strong></td>
</tr>
<tr>
<td><a href="http://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_2_2018.crt">http://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_2_2018.crt</a></td>
</tr>
<tr>
<td>Fingerprint:</td>
</tr>
<tr>
<td>SHA1: 4B467FB8D2051D7BC4CDB73377FA7077034BCCE1</td>
</tr>
<tr>
<td>SHA256: 113BBD9EFFFFA4C743D6D09038DC0AAB1A5F1FAD7492868193917C63D82D74FA1</td>
</tr>
<tr>
<td><strong>D-TRUST CA 2-1 2018</strong></td>
</tr>
<tr>
<td><a href="http://www.d-trust.net/cgi-bin/D-TRUST_CA_2-1_2018.crt">http://www.d-trust.net/cgi-bin/D-TRUST_CA_2-1_2018.crt</a></td>
</tr>
<tr>
<td>Policy Level: QCP-w</td>
</tr>
<tr>
<td>Fingerprint:</td>
</tr>
<tr>
<td>SHA1: 5982BDD5E228E4869461713710CC5C3DDE06C43</td>
</tr>
<tr>
<td>SHA256: 5F28BB88456D21158C5E3E8A31719CF3B305300BC5B4366B696BE22F6973F1DF1</td>
</tr>
<tr>
<td>OID: 1.3.6.1.4.1.4788.2.150.4</td>
</tr>
</tbody>
</table>
D-TRUST CA 2-2 2019
http://www.d-trust.net/cgi-bin/D-TRUST_CA_2-2_2019.crt
Policy Level: QCP-I
Fingerprint:
SHA1: 455FD6F160938C1FCCE1EF8D4F33700F2148FF87
SHA256: E85F41CE30CF9910CB8D12470F9E312E8F862FFeD0581F5995772D8B46CB7E99
OID: 1.3.6.1.4.1.4788.2.150.5

D-TRUST Root CA 3 2013
http://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_3_2013.crt
Fingerprint:
SHA1: 6C7CCCE7D4AE515F9908CD3FF6E8C378DF6FeF97
SHA256: A1A86D04121EB87F027C66F5330C28E5739F943FC84B38AD6AF009035DD9457

D-TRUST Application Certificates CA 3-1 2013
http://www.d-trust.net/cgi-bin/D-TRUST_Application_Certificates_CA_3-1_2013.crt
Policy Level: LCP
Fingerprint:
SHA1: 1785B07501F0FCEFFC97C6B070C255A8A9B99F12
SHA256: C80F7B7670EA2B818ABE80587902434B30EF7A8C0273B84884243F89593EA630
OID: 1.3.6.1.4.1.4788.2.200.1

PCA-1-Verwaltung
Siehe Webseite des BSI:

D-TRUST V-PKI CA 1 2020
http://x500.bund.de/
Policy Level: V-PKI
OID: 0.4.0.127.0.7.3.6.1.1.4.4
OID: 1.3.6.1.4.1.4788.2.201.2

Sowohl in CA- als auch in EE-Zertifikaten können CPs oder OIDs referenziert werden, die detailliert Anforderungen und Beschränkungen definieren.
1.2 Name und Kennzeichnung des Dokuments

Dokumentname: Certification Practice Statement der D-TRUST CSM PKI
Version: 3.0

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (CA)
Diese Regelungen sind im TSPS dokumentiert.

1.3.2 Registrierungsstellen (RA)
Diese Regelungen sind im TSPS dokumentiert.

1.3.3 Zertifikatsnehmer (ZNE) und Endanwender (EE)
Diese Regelungen sind im TSPS dokumentiert.

1.3.4 Zertifikatsnutzer (ZNU)
Diese Regelungen sind im TSPS dokumentiert.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten
Diese Regelungen sind im TSPS dokumentiert.

1.4.2 Verbotene Verwendungen von Zertifikaten
Diese Regelungen sind im TSPS dokumentiert.

1.4.3 Verwendung von Dienstezertifikaten
Diese Regelungen sind im TSPS dokumentiert.

1.5 Administration der Policy

1.5.1 Zuständigkeit für das Dokument und Kontaktdaten
Diese Regelungen sind im TSPS dokumentiert.

1.5.2 Meldung von Sicherheitsvorfällen mit Zertifikaten
Diese Regelungen sind in der CP dokumentiert.

1.5.3 Verträglichkeit von CPs fremder CAs mit diesem CPS
Die allgemeinen Regelungen sind im TSPS dokumentiert.

**QCP-w, EVCP**

QCP-w mit der Ausprägung PSD2

QCP-I

1.6 Begriffe und Abkürzungen

1.6.1 Begriffe und Namen
Diese Regelungen sind in der CP dokumentiert.

1.6.2 Abkürzungen
Die weiteren Regelungen sind in der CP dokumentiert.

1.6.3 Referenzen
Diese Regelungen sind in der CP dokumentiert.

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Der Status von Zertifikaten kann mittels OCSP-Abfrage im Verzeichnisdienst mindestens ein Jahr nach Ablauf der Gültigkeit der Zertifikate abgerufen werden.

QCP-n-qscd, QCP-I-qscd, QCP-I
Der Status der Zertifikate kann mittels OCSP-Abfrage dauerhaft abgerufen werden.
Die weiteren Regelungen sind in der CP dokumentiert.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Der TSP veröffentlicht folgende Informationen:
- EE-Zertifikate,
- Zertifikatsstatus von TLS Demo-Webseiten
- dieses CPS,
- die Verpflichtungserklärung,
- Cross-Zertifikate,
- die PKI-Nutzerinformation für qualifizierte Vertrauensdienste.
Die weiteren Regelungen sind im TSPS dokumentiert.
2.3 Häufigkeit von Veröffentlichungen

QCP-w, EVCP, OVC P, DVCP, LCP


QCP-I

Die Zustimmung zur Veröffentlichung ist Voraussetzung für die Beantragung. Veröffentlichte EE-Zertifikate bleiben bis zum Ende ihrer Gültigkeit sowie mindestens für zehn Jahre und bis zum Jahresende abrufbar.

V-PKI

Die Zertifikate der V-PKI sind für einen geschlossenen Anwenderkreis und obliegen der Hoheit des BSI und werden nicht in einem öffentlichen LDAP veröffentlicht.

Die Veröffentlichung findet sofort nach Ausstellung eines Zertifikats statt.

CA-Zertifikate werden nach ihrer Erstellung veröffentlicht und:

- mindestens 10 Jahre (QCP-I, QCP-w, EVCP) und bis zum Jahresende bzw.
- mindestens 1 Jahr und bis zum Jahresende (OVCP, DVCP, LCP)

nach Ablauf der Gültigkeit der CA vorgehalten.


CA-Sperrlisten, die von Root-CAs ausgestellt werden, werden mindestens alle 12 Monate erstellt und veröffentlicht, auch wenn kein Widerruf von Zertifikaten vorgenommen wurde.

Dieses CPS wird veröffentlicht und bleibt mindestens so lange abrufbar, wie Zertifikate, die auf Basis dieses CPS ausgestellt wurden, gültig sind.

Die Webseiten des TSP können öffentlich und unentgeltlich 24x7 abgerufen werden.

2.4 Zugriffskontrollen auf Verzeichnisse

Diese Regelungen sind im TSPS dokumentiert.

2.5 Zugang und Nutzung von Diensten

Diese Regelungen sind in der CP dokumentiert.

3. Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

Alternative Namen können registriert und in die subjectAltName-Erweiterung der Zertifikate aufgenommen werden.

3.1.2 Notwendigkeit für aussagefähige Namen

Der verwendete DistinguishedName ist eindeutig innerhalb dieser PKI, wenn es sich nicht um TLS-Zertifikate handelt.

Eine eindeutige Zuordnung des Zertifikats zum*r Zertifikatsnehmer*in (bei Zertifikaten für natürliche Personen auch zum*r Endanwender*in) ist gegeben.

Bei alternativen Namen (subjectAltName) gibt es, mit Ausnahmen von TLS-Zertifikaten (einschließlich EV-Zertifikate), keine Notwendigkeit für aussagefähige Namen.

Diese Angaben dürfen keine Referenzen auf das Zertifikat selbst enthalten. IP-Adressen sind nicht zugelassen.

3.1.3 Anonymität oder Pseudonyme von Zertifikatsnehmern

Pseudonyme werden ausschließlich für natürliche Personen benutzt. Generell werden Pseudonyme vom TSP vergeben.

Auch bei Zertifikaten, die mit Pseudonymen erstellt werden, wird durch den TSP oder die RA die reale Identität des*der Endanwenders*in (und ggf. des*der Zertifikatsnehmers*in) in der Dokumentation dokumentiert.

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Die Attribute des DistinguishedName (DN-Bestandteile) von EE-Zertifikaten werden wie folgt interpretiert:

<table>
<thead>
<tr>
<th>DN-Bestandteil</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>G (GivenName)</td>
<td>Vorname(n) der natürlichen Person</td>
</tr>
<tr>
<td></td>
<td>QCP-I, QCP-w, EVCP, OVCP, DVCP: Feld wird nicht verwendet</td>
</tr>
<tr>
<td></td>
<td>LCP: gemäß dem zur Identifizierung verwendeten Nachweis</td>
</tr>
<tr>
<td>SN (Surname)</td>
<td>Familienname der natürlichen Person</td>
</tr>
<tr>
<td></td>
<td>QCP-I, QCP-w, EVCP, OVCP, DVCP: Feld wird nicht verwendet</td>
</tr>
<tr>
<td></td>
<td>LCP: gemäß dem zur Identifizierung verwendeten Nachweis</td>
</tr>
<tr>
<td></td>
<td>Bei der Verwendung von Pseudonymen entspricht der SN dem CN.</td>
</tr>
<tr>
<td>DN-Bestandteil</td>
<td>Interpretation</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CN</td>
<td><strong>Gebräuchlicher Name:</strong> Folgende Varianten werden verwendet:</td>
</tr>
<tr>
<td></td>
<td>Natürlichen Personen ohne Pseudonym: „Familienname, Rufname“</td>
</tr>
<tr>
<td></td>
<td>Natürliche Personen mit Pseudonym: „Pseudonym:PN“</td>
</tr>
<tr>
<td></td>
<td>Juristische Personen: offizielle Bezeichnung der Organisation (Firma, Behörde, Verein etc.), ggf. sinnvolle Abkürzung bei Überschreiten der Zeichenbegrenzung von 64 Zeichen.</td>
</tr>
<tr>
<td></td>
<td>Sonderfall: ein oder mehrere Domainnamen können ebenfalls in den CN aufgenommen werden.</td>
</tr>
<tr>
<td></td>
<td>QCP-w, EVCP: Wildcards sind nicht zulässig bei TLS-Zertifikaten.</td>
</tr>
<tr>
<td></td>
<td>Funktion oder Personengruppe: Name der Funktion oder Personengruppe mit der vorangestellten Abkürzung „GRP:“ als Hinweis, dass es sich um ein Gruppenzertifikat handelt.</td>
</tr>
<tr>
<td></td>
<td>V-PKI: In der V-PKI werden Zertifikate, die für eine Personengruppe ausgestellt werden, Funktionszertifikate genannt. Wenn die Funktion aus dem CN nicht erkennbar ist, wird im CN der Hinweis „FKT:“ verwendet. Der Zertifikatsnehmer ist dafür verantwortlich, dass der private Schlüssel eines Funktionszertifikats aus der V-PKI von maximal 30 Personen gleichzeitig genutzt wird.</td>
</tr>
<tr>
<td></td>
<td>Technische Komponenten: Name des Servers, des Dienstes oder der Applikation, der/die das Zertifikat benutzt.</td>
</tr>
<tr>
<td>Alternativer Antragsteller (SAN)</td>
<td>Folgende Varianten werden verwendet:</td>
</tr>
<tr>
<td></td>
<td>- E-Mail-Adresse des Zertifikatsnehmers</td>
</tr>
<tr>
<td></td>
<td>- Technische Komponenten: Name des Servers, des Dienstes oder der Applikation, der/die das Zertifikat benutzt.</td>
</tr>
<tr>
<td></td>
<td>Sonderfall: ein oder mehrere Domainnamen können ebenfalls in den SAN aufgenommen werden.</td>
</tr>
<tr>
<td></td>
<td>QCP-w, EVCP: Wildcards sind nicht zulässig bei TLS-Zertifikaten.</td>
</tr>
<tr>
<td>PN</td>
<td><strong>Pseudonym:</strong> ist identisch zu CN.</td>
</tr>
<tr>
<td></td>
<td>V-PKI: Es werden keine Pseudonyme vergeben.</td>
</tr>
<tr>
<td>Serial Number</td>
<td><strong>Serienummer:</strong> Namenszusatznummer, welche die Eindeutigkeit des Namens sicherstellt (i.d.R. die Antragsnummer).</td>
</tr>
<tr>
<td>(serialNumber)</td>
<td>Sonderfall bei EV-Zertifikaten gemäß [EVGL]: Registernummer falls vergeben, Datum der Registrierung oder Gründung.</td>
</tr>
<tr>
<td></td>
<td>Produktspezifisch kann das Feld anderweitig verwendet werden.</td>
</tr>
</tbody>
</table>
### DN-Bestandteil | Interpretation
--- | ---
O (organizationName) (2.5.4.10) | Offizielle Bezeichnung des Zertifikatsnehmers oder Bezeichnung der Organisation, der der Endanwender angehört oder damit verbunden ist (Firma, Behörde, Verein etc.) entsprechend Existenznachweis, ggf. sinnvolle Abkürzung bei Überschreiten der Zeichenbegrenzung von 64 Zeichen. DVCP: Feld wird nicht verwendet
OU (organizationalUnitName) (2.5.4.11) | Organisationseinheit (Abteilung, Bereich oder andere Unterteilung) der Organisation. DVCP: Feld wird nicht verwendet
OrgID (organizationIdentifier) (2.5.4.97) | **LCP (Seal ID):**

_Eindeutige Organisationsnummer der Organisation._

Es kann die Nummer des Handelsregistereintrags sowie die Umsatzsteueridentnummer oder eine von D-TRUST vergebene Nummer eingetragen werden.

Die von D-TRUST vergebene Nummer ist an das Format gemäß Variante 3 aus Kapitel 5.1.4 der EN 319 412-1 angelehnt und setzt sich wie folgt zusammen:

DT:DE-1234567890 (DT: D-TRUST; DE: Deutschland; zufällige Nummer, die der Organisation eindeutig zugeordnet wird).

**QCP-I und QCP-w mit der Ausprägung PSD2:**

_PSD2 Authorisation Number_

Bei Zertifikaten, die im Rahmen des PSD2-Verfahrens gemäß [TS 119 495] eingesetzt werden, ist das Setzen des organization identifiers (2.5.4.97) verpflichtend. Die Eindeutigkeit wird über die „Authorisation Number“ gewährleistet.

Die „Authorisation Number“ besteht aus den Zeichen:

\[
\text{PSD}<\text{cc}>-<\text{x..x}>-<\text{y..y}>
\]

Wobei

"PSD" - "legal person identity type", enthält 3 Zeichen;

<cc> ISO 3166 Ländercode der nationalen zuständigen Behörde (NCA) - genau 2 Zeichen

Hyphen-minus „-“

<x..x> Identifikator der NCA - 2 - 8 Großbuchstaben A – Z, keine Leerzeichen

Hyphen-minus „-“

<y..y> Identifikator des Zahlungsdienstleisters, wie von der NCA festgelegt - Beliebige Zeichenfolge

Beispiel: PSDDE-BAFIN-1234Ab
<table>
<thead>
<tr>
<th>DN-Bestandteil</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>C (countryName) (2.5.4.6)</td>
<td>Das aufzuführende Land wird gemäß [ISO 3166] notiert und ergibt sich wie folgt: Ist eine Organisation O im DistinguishedName aufgeführt, so bestimmt der im Register benannte Sitz der Organisation den Eintrag im Zertifikat. Ist keine Organisation O eingetragen, so wird das Land aufgenommen, dass das Dokument ausgestellt hat, mit dem der* die Zertifikatsnehmer* in identifiziert wurde.</td>
</tr>
<tr>
<td>Street (streetAddress) (2.5.4.9)</td>
<td>Postalische Adresse Straße</td>
</tr>
<tr>
<td>Locality (localityName) (2.5.4.7)</td>
<td>Postalische Adresse Ort</td>
</tr>
<tr>
<td>State (stateOrProvinceName) (2.5.4.8)</td>
<td>Postalische Adresse (Bundes-)Land</td>
</tr>
<tr>
<td>PostalCode (postalCode) (2.5.4.17)</td>
<td>Postalische Adresse Postleitzahl</td>
</tr>
<tr>
<td>BusinessCategory (businessCategory)</td>
<td>Business Category</td>
</tr>
<tr>
<td>Jurisdiction Of Incorporation Locality (jurisdictionLocality Name)</td>
<td>Gerichtsstand der Organisation gemäß [EVGL]: Ort (1.3.6.1.4.1.311.60.2.1.1)</td>
</tr>
<tr>
<td>Jurisdiction Of Incorporation State Or Province Name (jurisdictionStateOrProvinceName)</td>
<td>Gerichtsstand der Organisation: (Bundes-)Land (1.3.6.1.4.1.311.60.2.1.2)</td>
</tr>
</tbody>
</table>
DN-Bestandteil | Interpretation
---|---
Jurisdiction Of Incorporation CountryName (jurisdictionCountryName) | Gerichtsstand der Organisation gemäß [EVGL]: Land (1.3.6.1.4.1.311.60.2.1.3)

**QCP-w**², **EVCP**
TLS-Zertifikate enthalten mindestens die subject-DN-Bestandteile „organizationName“, „commonName“, „serialNumber“, "jurisdictionCountryName" „localityName“, “streetAddress”, „countryName“, „postalCode", "businessCategory" sowie „subjectAltName".

**QCP-I**
Qualifizierte Zertifikate für juristische Personen enthalten mindestens die subject-DN-Bestandteile „commonName", „countryName", „serialNumber" und „organizationName“ sowie „organizationIdentifier".


### 3.1.5 Eindeutigkeit von Namen
Der TSP stellt sicher, dass ein in EE-Zertifikaten verwendeter Name (DistinguishedName) des*der Zertifikatsnehmers*in bzw. des*der Endanwenders*in (Feld subject) innerhalb der über den CSM bereitgestellten PKI stets dem*der gleichen Zertifikatsnehmer*in bzw. Endanwender*in zugeordnet ist. Die Eindeutigkeit des Zertifikats wird mittels der Seriennummer erzielt.

Der TSP stellt die Eindeutigkeit von DistinguishedNames in CA-Zertifikaten sicher.

### 3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen
Der*Die Zertifikatsnehmer*in haftet für die Einhaltung geistiger Eigentumsrechte in den Antrags- und Zertifikatsdaten (siehe Zertifikatsrichtlinie der D-Trust GmbH, Abschnitt 9.5).

**QCP-w**, **EVCP**
Der TSP unternimmt notwendige Schritte um sicherzustellen, dass zum Zeitpunkt der Ausstellung des Zertifikates, derjenige, der im Feld „Subject“ des Zertifikates benannt ist, die nachweisliche Kontrolle über die im SAN-Feld enthaltene Domain bzw. Domainbestandteile besitzt.

### 3.2 Initiale Überprüfung der Identität

#### 3.2.1 Nachweis für den Besitz des privaten Schlüssels
Es werden zwei Fälle unterschieden:

---
² Bei QCP-w Zertifikaten mit der Ausprägung PSD2 wird der "organizationIdentifier" zusätzlich gesetzt und geprüft.
a) Schlüsselpaare von Zertifikatsnehmern*innen werden im Verantwortungsbereich des TSP produziert. Mit der Übergabe der Token oder Soft-PSE (LCP) und ggf. PIN-Briefe gemäß Abschnitt 4.4.1 an die Zertifikatsnehmer*innen durch den TSP wird sichergestellt, dass die privaten Schlüssel in den Besitz der Zertifikatsnehmer*innen gelangen.

b) Schlüsselpaare werden im Verantwortungsbereich des*der Zertifikatsnehmers*in produziert. Der Besitz des privaten Schlüssels muss entweder technisch nachgewiesen werden oder von dem*der Zertifikatsnehmer*in nachvollziehbar bestätigt werden. Mit der Übersendung eines PKCS#10-Requests an den TSP bestätigt der*die Zertifikatsnehmer*in verbindlich im Besitz des privaten Schlüssels zu sein.

3.2.2 Identifizierung und Authentifizierung von Organisationen und Domains

Organisationen, die entweder im Zertifikat genannt werden oder in deren Namen Zertifikate ausgestellt werden, müssen sich eindeutig authentisieren.


In den verschiedenen Policy Leveln werden die vorgestellten Prüfverfahren wie folgt auf die DN-Bestandteile nach Abschnitt 3.1.4 und ggf. weitere Attribute angewendet. Die in der folgenden Tabelle angegebenen Verfahren sind in Abschnitt 4.2.1 beschrieben.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>QCP-w, EVCP</th>
<th>OVCP</th>
<th>DVCP</th>
<th>QCP-l</th>
</tr>
</thead>
</table>
| CN                         | Register/  | Register/  | Domain | Register/ 
|                            | Non-Register/| Non-Register/ |     | Non-Register |
|                            | Domain/    | Domain/  |       |       |
|                            | CAA        | CAA     |       |       |
| C                          | Register/  | Register/  | n.a. |       |
|                            | Non-Register/| Non-Register/ |     |       |
|                            | Domain     | Domain   |       |       |
|                            |            |          | n.a. |       |
| OrgID                      | Register   | n.a.     | n.a. | Register |
| OU                         | Z-Bestätigung/ | Z-Bestätigung/ | n.a. | Z-Bestätigung/ |
|                            | A-Bestätigung| A-Bestätigung|     | A-Bestätigung |
| STREET                     | Register/  | Register/  | n.a. | Register/ 
|                            | Non-Register| Non-Register |     | Non-Register |
|                            |            |          | n.a. |       |
| L                          |            |          | n.a. |       |
| State                      |            | n.a.     | n.a. |       |
| PostalCode                 |            | n.a.     | n.a. |       |
| (SAN)                      | CAA        | CAA     | CAA   |       |
| Alle weiteren Attribute    | n.a.       | n.a.     | n.a.  | n.a.  |
Wird der Antrag im Auftrag einer juristischen Person gestellt, muss der*die Vertreter*in (analog zu dem Verfahren für die Organisationszugehörigkeit aus Abschnitt 3.2.3) seine diesbezügliche Berechtigung nachweisen und sich authentifizieren und ggf. identifizieren für qualifizierte Siegelzertifikate gemäß QCP-I und für qualifizierte Webseitenzertifikate gemäß QCP-w.

Nachweise in nicht lateinischer Schrift werden nicht akzeptiert.

3.2.3 Identifizierung und Authentifizierung natürlicher Personen

Natürliche Personen, die Zertifikate beantragen, müssen sich eindeutig authentifizieren und ggf. ihre Berechtigung zur Antragstellung durch die Organisation nachweisen.

LCP, V-PKI

Natürliche oder juristische Personen, die für andere Zertifikatsnehmer*innen Zertifikate beantragen, müssen ihre Berechtigung zur Antragstellung nachweisen.

Die vorgestellten Prüfverfahren werden wie folgt auf die DN-Bestandteile nach Abschnitt 3.1.4 und ggf. weitere Attribute angewendet. Die angegebenen Verfahren sind in Abschnitt 4.2.1 beschrieben.

<table>
<thead>
<tr>
<th>V-PKI</th>
<th>LCP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>G</strong></td>
<td>Pers-Ident</td>
</tr>
<tr>
<td><strong>SN</strong></td>
<td>HR-DB / Dok-Ident / Pers-Ident</td>
</tr>
<tr>
<td><strong>CN</strong></td>
<td>Register / Non-Register</td>
</tr>
<tr>
<td><strong>C</strong></td>
<td>HR-DB / Register / Non-Register</td>
</tr>
<tr>
<td><strong>O</strong></td>
<td>Register / Non-Register</td>
</tr>
<tr>
<td><strong>OU</strong></td>
<td>Z-Bestätigung / A-Bestätigung</td>
</tr>
<tr>
<td><strong>STREET</strong></td>
<td>n.a.</td>
</tr>
<tr>
<td><strong>L</strong></td>
<td>n.a.</td>
</tr>
<tr>
<td>State</td>
<td></td>
</tr>
<tr>
<td>PostalCode</td>
<td></td>
</tr>
<tr>
<td>Alternativer Antragsteller (SAN)</td>
<td>E-Mail-Adresse</td>
</tr>
<tr>
<td>Alle weiteren Attribute</td>
<td>n.a.</td>
</tr>
<tr>
<td></td>
<td>A-Bestätigung / Dok-Ident / out-of-band mechanisms</td>
</tr>
</tbody>
</table>

Bei Antrag auf Zertifikate für Gruppen, Funktionen oder IT-Prozesse, werden alle in der Tabelle aufgeführten Attribute zum* zur Endanwender*in (bis auf OU, E-Mail-Adresse, alle weiteren Attribute, wenn nicht zertifikatsrelevant) geprüft. Für die Aufnahme von Namen für Gruppen, Funktionen oder IT-Prozesse im CN gelten die Verfahren analog zu Zeile „Alle weiteren Attribute“.

Nachweise in nicht lateinischer Schrift werden nicht akzeptiert.
3.2.4 Ungeprüfte Angaben zum* zur Zertifikatsnehmer*in

Die Angaben des* der Zertifikatsnehmers* in werden entsprechend den Abschnitten 3.2.2, 3.2.3 und 4.2.1 geprüft bzw. nicht geprüft. Bei alternativen Namen werden generell nur die E-Mail-Adressen bzw. deren Domainbestandteile geprüft. Andere Zertifikatsinhalte wie z.B. LDAP-Verzeichnisse etc. sowie eventuelle Zertifikats-Extensions (AdditionalInformation, monetaryLimit, etc.) werden nicht auf Korrektheit geprüft.

Eine Ausnahme bilden hierbei TLS-Zertifikate nach QCP-w und EVCP, bei denen der Alternative Name für die Aufnahme weiterer URLs genutzt wird. In diesen Fällen werden auch Domains in dNSNames geprüft.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Bei natürlichen Personen werden Identitätsnachweis und ggf. die Organisationszugehörigkeit mittels der spezifischen Verfahren gemäß Abschnitt 3.2.3 ermittelt und geprüft bzw. bestätigt.

Bei Organisationen wird der Existenznachweis sowie die Vertretungsberechtigung eines Zeichnungsberechtigten nach Abschnitt 3.2.2 geprüft bzw. bestätigt. Weiterhin wird mindestens ein*e technischer*e Vertreter*in persönlich bzw. über ein entsprechendes Ident-Verfahren identifiziert.

3.2.6 Kriterien für die Interoperabilität

Siehe Abschnitt 1.5.3.

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


3.3.1 Routinemäßige Anträge zur Schlüsselerneuerung

Bei Anträgen zur Schlüsselerneuerung ist keine erneute Identifizierung erforderlich, so lange die beim TSP hinterlegten Nachweise noch verwertbar sind. Der Auftrag zur Schlüsselerneuerung muss elektronisch über die vereinbarte Schnittstelle übertragen werden.

EVCP, QCP-w


Abweichende Verfahren können kundenindividuell vereinbart werden. Die Bedingungen des Abschnitts 4.7 müssen erfüllt werden.

3.3.2 Schlüsselerneuerung nach Widerruf eines Zertifikats

Schlüsselerneuerung auf Basis eines widerrufenen Zertifikats wird nicht angeboten.
3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Sperrberechtigung wird wie folgt geprüft:

- Bei einem Sperrantrag, der in einer signierten E-Mail eingeht, muss der*die Sperrantragsteller*in entweder der*die Zertifikatsnehmer*in selbst sein oder als Sperrberechtigter Dritter benannt worden sein, dessen Zertifikat dem TSP vorliegen muss. (nur LCP)
- Bei telefonischem Sperrantrag oder einem Antrag per E-Mail ohne Signatur muss der*die Sperrberechtigte das entsprechende Sperrpasswort korrekt nennen.
- Sperranträge können nur dann über die Online-Schnittstelle eingereicht werden, wenn sich der*die Sperrantragsteller*in gegenüber der Schnittstelle eindeutig authentifizieren kann.

Andere Verfahren zur Authentifizierung von Sperranträgen können mit dem*der Zertifikatsnehmer*in vereinbart werden.

LCP, V-PKI

Sperranträge eines*einer Endanwenders*in sind grundsätzlich an den*die technischen*e Ansprechpartner*in der RA zu richten. Dieser*e löst dann einen Sperrauftrag beim TSP über die vereinbarte Online-Schnittstelle aus. Der*Die technische Ansprechpartner*in muss sich zwingend gegenüber der Online-Schnittstelle des TSPs eindeutig authentifizieren. Für den Fall, dass der*die technische Ansprechpartner*in, dem*der Endanwender*in das Sperrpasswort mitgeteilt hat, kann der*die Endanwender*in auch andere Sperrverfahren nutzen.

Sperrverfahren werden in Abschnitt 4.9 definiert.

4. Betriebsanforderungen

4.1 Zertifikatsantrag und Registrierung

4.1.1 Berechtigung zur Antragstellung

Anträge dürfen von natürlichen Personen und juristischen Personen (bzw. deren autorisierten Vertretern) gestellt werden.

Gruppen- oder Teamzertifikate werden ausschließlich für juristische Personen und Einzelunternehmen ausgestellt.

**QCP-w, EVCP**

Zertifikatsnehmer*innen müssen den Anforderungen aus [EVGL] entsprechen.

Der TSP ist berechtigt, Anträge abzulehnen (siehe Abschnitt 4.2.2).

4.1.2 Registrierungsprozess und Zuständigkeiten

Die allgemeinen Regelungen sind in dem TSPS dokumentiert.

In diesem CPS finden die in Abschnitt 1.1.3 genannten Policy Level QCP-I, QCP-w, EVCP, OVCP, DVCP, LCP Anwendung. Der Registrierungsprozess und die Zuständigkeiten für die jeweiligen Policy Level werden in der TSPS beschrieben.

**Für das Policy Level OVCP gilt zusätzlich zur TSPS folgende Regelung:**

Der*Die Kunde*in hat in CSM die Option ein OVCP Produkt mit oder ohne CT-Logging auszuwählen.
4.2 Verarbeitung des Zertifikatantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Die allgemeinen Regelungen sind im TSPS dokumentiert.

Im Rahmen des CSM CPS sind je nach Policy Level bestimmte Identifizierungsverfahren zugelassen. Welche Identifizierung und Authentifizierung je nach Policy Level zugelassen ist, ist den Tabellen in den Abschnitten 3.2.2 und 3.2.3 zu entnehmen. Diese sind im Folgenden aufgelistet und werden im TSPS erläutert:

- Pers-Ident
- Dok-Ident
- Register
- Non-Register
- HR-DB
- Z-Bestätigung
- A-Bestätigung
- out-of-band-Mechanismen
- Domain
- E-Mail-Adresse
- CAA

Identifizierung und Authentifizierung finden gemäß den Abschnitten 3.2.2 und 3.2.3 statt.

4.2.2 Annahme oder Ablehnung von Zertifikatanträgen

Diese Regelungen sind im TSPS dokumentiert.

4.2.3 Fristen für die Bearbeitung von Zertifikatanträgen

Diese Regelungen sind im TSPS dokumentiert.

4.3 Ausstellung von Zertifikaten

4.3.1 Vorgehen des TSP bei der Ausstellung von Zertifikaten

Die allgemeinen Regelungen sind im TSPS dokumentiert.

Darüber hinaus gibt es im Rahmen des CSM CPS folgende spezifische Regelungen:

**EVCP, QCP-w\(^3\), OVCP\(^4\), DVCP**


4.3.2 Benachrichtigung des*der Zertifikatsnehmers*in über die Ausstellung des Zertifikats.

Diese Regelungen sind im TSPS dokumentiert.

---

\(^3\) Gilt nicht für QCP-w mit PSD2 Ausprägung.

\(^4\) Gilt nur, wenn das Produkt im Bestellprozess mit CT-Logging ausgewählt wurde.
4.4 Zertifikatsübergabe

4.4.1 Verhalten bei der Zertifikatsübergabe

**LCP, V-PKI**
Zertifikate, deren privater Schlüssel im Bereich des TSP erstellt wurde, werden zum zugriffsgeschützten und TLS-verschlüsselten Download bzw. TLS-geschützter Schnittstelle (CSM) bereitgestellt oder per E-Mail gesendet (die PKCS#12-Datei ist mit einer PIN geschützt).

**QCP-I, QCP-w, EVCP, OVCP, DVCP, LCP**
Wird ein Zertifikat zu einem*einer bei dem*der Zertifikatsnehmer*in vorhandenen Schlüsselpaar ausgestellt, wird das Zertifikat entweder zum Download bereitgestellt (z.B. im Verzeichnisdienst veröffentlicht) oder elektronisch versendet.

Kundenspezifisch können abweichende Verfahren vereinbart werden.

Die allgemeinen Regelungen sind im TSPS dokumentiert.

4.4.2 Veröffentlichung des Zertifikats durch den TSP

Die Zertifikate werden nach der Produktion grundsätzlich in den öffentlichen Verzeichnisdienst eingestellt.

Der Status ist nach Produktion über OCSP abrufbar.

**V-PKI**
Die Zertifikate der V-PKI sind für einen geschlossenen Anwenderkreis und obliegen der Hoheit des BSI und werden nicht in einem öffentlichen LDAP veröffentlicht. Eine Sperrliste wird erstellt.
Der OCSP Dienst zur Statusabfrage wird im Rahmen der V-PKI nicht angeboten.

4.4.3 Benachrichtigung anderer PKI-Teilnehmer*in über die Ausgabe des Zertifikats
Sperrberechtigte Dritte nach Abschnitt 4.9.2 werden schriftlich benachrichtigt und erhalten das Sperrpasswort, sofern nichts anderes mit der Organisation oder dem*der Sperrberechtigten Dritten vereinbart wurde.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den*die Zertifikatsnehmer*in
Zertifikatsnehmer*innen und Endanwender*innen dürfen ihre privaten Schlüssel ausschließlich für die Anwendungen nutzen, die in Übereinstimmung mit den im Zertifikat angegebenen Nutzungsarten stehen.

**QCP-I, QCP-w**
Nach Ablauf des Gültigkeitszeitraums oder nach dem Widerruf des Zertifikats dürfen die zugehörigen privaten Schlüssel nicht mehr genutzt werden.

Für Zertifikatsnehmer*innen gelten die Bestimmungen aus Abschnitt 1.4.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer*innen
Diese Regelungen sind im TSPS dokumentiert.
4.6 Zertifikatserneuerung (certificate renewal)

Es gelten die Anforderungen aus Abschnitt 4.7 und 3.3.

4.7 Zertifikatserneuerung mit Schlüsselerneuerung

Eine Zertifikatserneuerung ist die erneute Ausstellung eines Zertifikats, das auf den Inhaltsdaten des ursprünglichen Zertifikats beruht. Für die erneuerten Zertifikate gilt die zum Zeitpunkt der Erneuerung aktuelle CP und CPS.

Bei CA-Schlüsseln wird keine Zertifikatserneuerung durchgeführt.

Abweichende Verfahren können kundenindividuell vereinbart werden, deren Umsetzung im Ermessen des TSP liegen, wenn sie keiner Zertifizierung nach EN 319 411-1 unterliegen. Die Bedingungen des Abschnitts 3.3 müssen erfüllt werden.

4.7.1 Bedingungen für eine Zertifikatserneuerung

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


Voraussetzung ist, dass das Zertifikat für denselben*dieselbe Endanwender*in ausgestellt wird. Das zu erneuernde Zertifikat muss zum Zeitpunkt der elektronischen Antragstellung auf Zertifikatserneuerung noch gültig sein oder geprüfte Daten und Nachweise sind für die Erneuerung vorhanden und verwendbar.

**LCP**

Im Rahmen von Verträgen kann ein Nachladeverfahren implementiert werden, bei dem der Antrag durch Beauftragte erfolgt und der*die Zertifikatsnehmer*in im Nachladeverfahren persönlich durch Eingabe der PIN der Aufbringung des neuen Zertifikates auf seiner Karte und ggf. neuen Nutzungsbedingungen zustimmt.

**V-PKI**


4.7.2 Berechtigung zur Zertifikatserneuerung

Jeder*Jede Zertifikatsnehmer*in, der (nach Abschnitt 4.1.1) berechtigt ist, einen Zertifikatantrag zu stellen, kann eine Zertifikatserneuerung beantragen, wenn die Bedingungen nach Abschnitt 4.6 erfüllt sind und der TSP ein entsprechendes Verfahren für das gewählte Produkt anbietet.

4.7.3 Bearbeitung eines Antrags auf Zertifikatserneuerung

Zertifikatsnehmer*innen, die berechtigt sind, Anträge auf Zertifikatserneuerung zu stellen, nutzen eine produktspezifisch bereitgestellte Onlineschnittstelle des TSP zur Antragstellung.
Über die entsprechenden Schnittstellen gestellte Anträge werden automatisiert auf Berechtigung und Inhalt geprüft.

4.7.4 Benachrichtigung des*der Zertifikatsnehmers*innen über die Ausgabe eines neuen Zertifikats
Es gelten die in Abschnitt 4.3.2 festgelegten Regelungen.

4.7.5 Verhalten bei der Ausgabe einer Zertifikaterneuerung
Das erzeugte Zertifikat wird über die bereitgestellte Online-Schnittstelle zur Verfügung gestellt. Weiterhin gelten die in Abschnitt 4.4.1 festgelegten anwendbaren Regelungen.

4.7.6 Veröffentlichung der Zertifikaterneuerung durch den TSP
Es gelten die in Abschnitt 4.4.2 festgelegten Regelungen.

4.7.7 Benachrichtigung anderer PKI-Teilnehmer über die Erneuerung des Zertifikats
Es gelten die in Abschnitt 4.4.3 festgelegten Regelungen.

4.8 Zertifikatsänderung
Diese Regelungen sind im TSPS dokumentiert.

4.9 Widerruf und Suspendierung von Zertifikaten

4.9.1 Bedingungen für einen Widerruf von Zertifikaten
Diese Regelungen sind im TSPS dokumentiert. Sperrberechtigte müssen sich gemäß Abschnitt 0 authentifizieren.

4.9.2 Berechtigung zum Widerruf
Diese Regelungen sind im TSPS dokumentiert.

4.9.3 Verfahren für einen Sperrantrag
Über die vereinbarte Online-Schnittstelle können Zertifikate grundsätzlich 24x7 durch den*die Zertifikatsnehmer*in bzw. seinen*e autorisierten*e Vertreter*in widerrufen werden. Ein Widerruf in der Zukunft wird nicht angeboten. Der Widerruf über die Online-Schnittstelle wird sofort wirksam.

Sperranträge eines*einer Endanwenders*in sind grundsätzlich an den*die technischen*e Ansprechpartner*in der RA zu richten. Dieser löst den Sperrauftrag beim TSP über die vereinbarte Online-Schnittstelle aus. Der*Die technische Ansprechpartner*in der RA muss sich zwingend gegenüber der Online-Schnittstelle des TSPs eindeutig authentifizieren.


Die Verfahrensanweisungen beinhalten strikte Vorgaben für die Erfüllung der Sperrdienstleistung und beschreiben detailliert Abläufe und Verhaltensvorgaben im Fehlerfall.

Die Authentifizierung der Sperrberechtigten erfolgt gemäß Abschnitt 3.4.

**PSD2 spezifisches Sperrverfahren**

Ausschließlich Behörden als Herausgeber von PSD2 spezifischen Attributen können über die folgende E-Mail ihren Sperrantrag einreichen:

E-Mail-Adresse: sperren@d-trust.net

Dieses Sperrverfahren gilt nur für die NCA Behörden im Rahmen des PSD2-Verfahrens.

4.9.4 Fristen für einen Sperrantrag

Diese Regelungen sind im TSPS dokumentiert.

4.9.5 Zeitspanne für die Bearbeitung des Sperrantrags durch den TSP

Sperranträge können 24x7 über die Online-Schnittstelle eingereicht werden. Der Widerruf erfolgt gemäß Abschnitt 4.9 [BRG] innerhalb von 24 Stunden nach erfolgreicher Autorisierung des*der Sperrantragstellers*in.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen


Integrität und Authentizität der Sperrinformationen wird durch eine Signatur der CRL bzw. der OCSP-Antwort gewährleistet.

Status- und Sperrinformationen (OCSP und CRL) sind konsistent.


Sperreinträge in Sperrlisten verbleiben mindestens bis zum Ablauf der Zertifikatsgültigkeit enthalten.

**QCP-I**

Sperreinträge verbleiben nach Ablauf der jeweiligen Zertifikatsgültigkeit in den zugehörigen Sperrlisten.

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Siehe Abschnitt 2.3.

4.9.8 Maximale Latenzzeit für Sperrlisten

Sperrlisten werden unmittelbar erstellt und nach spätestens 60 Minuten veröffentlicht.
4.9.9 Online-Verfügbarkeit von Sperrinformationen
Zur Onlineprüfung steht ein OCSP-Dienst zur Verfügung. Die Erreichbarkeit dieses Dienstes wird in Form einer URL in den Zertifikaten angegeben.

V-PKI
Im Rahmen der V-PKI wird eine Sperrliste erstellt. Die CRL ist in den Zertifikaten in Form einer URL angegeben. Der OCSP Dienst zur Statusabfrage wird nicht angeboten.

4.9.10 Notwendigkeit zur Online-Prüfung von Sperrinformationen
Diese Regelungen sind im TSPS dokumentiert.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen
Diese Regelungen sind im TSPS dokumentiert.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels
Diese Regelungen sind im TSPS dokumentiert.

4.9.13 Bedingungen für eine Suspendierung
Diese Regelungen sind im TSPS dokumentiert.

4.10 Statusabfragdienst für Zertifikate

4.10.1 Funktionsweise des Statusabfragdienstes
Diese Regelungen sind im TSPS dokumentiert.

4.10.2 Verfügbarkeit des Statusabfragdienstes
Diese Regelungen sind im TSPS dokumentiert.

4.10.3 Optionale Leistungen
Diese Regelungen sind im TSPS dokumentiert.

4.11 Austritt aus dem Zertifizierungsdienst
Diese Regelungen sind im TSPS dokumentiert.

4.12 Schlüsselhinterlegung und -wiederherstellung
Schlüsselhinterlegung wird nicht vom TSP angeboten. Dem subscriber steht es frei, Schlüssel im eigenen Verantwortungsbereich zu hinterlegen.

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel
Schlüsselhinterlegung wird nicht vom TSP angeboten.

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln
Schlüsselhinterlegung wird nicht vom TSP angeboten.
5. **Nicht-technische Sicherheitsmaßnahmen**


Die weiteren Regelungen sind im TSPS dokumentiert.

5.1 **Bauliche Sicherheitsmaßnahmen**

Diese Regelungen sind im TSPS dokumentiert.

5.2 **Verfahrensvorschriften**

5.2.1 **Rollenkonzept- und Berechtigungskonzept**

Diese Regelungen sind im TSPS dokumentiert.

5.2.2 **Mehraugenprinzip**

Diese Regelungen sind im TSPS dokumentiert.

5.2.3 **Identifikation und Authentifizierung für einzelne Rollen**

Diese Regelungen sind im TSPS dokumentiert.

5.2.4 **Rollenausschlüsse**

Diese Regelungen sind im TSPS dokumentiert.

5.3 **Eingesetztes Personal**

Der TSP erfüllt die Anforderungen an das Personal aus [EN 319 411-1] und [EN 319 411-2].

5.3.1 **Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit**

Diese Regelungen sind im TSPS dokumentiert.

5.3.2 **Zuverlässigkeitsprüfungen**

Diese Regelungen sind im TSPS dokumentiert.

5.3.3 **Schulungen**

Diese Regelungen sind im TSPS dokumentiert.

5.3.4 **Häufigkeit von Schulungen und Belehrungen**

Diese Regelungen sind im TSPS dokumentiert.

5.3.5 **Häufigkeit und Folge von Job-Rotation**

Diese Regelungen sind im TSPS dokumentiert.

5.3.6 **Maßnahmen bei unerlaubten Handlungen**

Diese Regelungen sind im TSPS dokumentiert.

5.3.7 **Anforderungen an externe Mitarbeiter*innen**

Diese Regelungen sind im TSPS dokumentiert.
5.3.8 Ausgehändigte Dokumentation
Diese Regelungen sind im TSPS dokumentiert.

5.4 Überwachungsmaßnahmen

5.4.1 Überwachung des Zutritts
Diese Regelungen sind im TSPS dokumentiert.

5.4.2 Überwachung von Risiken
Diese Regelungen sind im TSPS dokumentiert.

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen
Diese Regelungen sind im TSPS dokumentiert.

5.5.2 Aufbewahrungsfristen für archivierte Daten
Diese Regelungen sind im TSPS dokumentiert.

5.5.3 Sicherung des Archivs
Diese Regelungen sind im TSPS dokumentiert.

5.5.4 Datensicherung des Archivs
Diese Regelungen sind im TSPS dokumentiert.

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen
Diese Regelungen sind im TSPS dokumentiert.

5.5.6 Archivierung (intern / extern)
Diese Regelungen sind im TSPS dokumentiert.

5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen
Diese Regelungen sind im TSPS dokumentiert.

5.6 Schlüsselwechsel beim TSP
Diese Regelungen sind im TSPS dokumentiert.

5.7 Kompromittierung und Geschäftsweiterführung beim TSP

5.7.1 Behandlung von Vorfällen und Kompromittierungen
Diese Regelungen sind im TSPS dokumentiert.

5.7.2 Wiederherstellung nach Kompromittierung von Ressourcen
Diese Regelungen sind im TSPS dokumentiert.

5.7.3 Kompromittierung des privaten CA-Schlüssels
Diese Regelungen sind im TSPS dokumentiert.

5.7.4 Möglichkeiten zur Geschäftsweiterführung
Diese Regelungen sind im TSPS dokumentiert.

5.8 Schließung des TSP bzw. die Beendigung der Dienste
Diese Regelungen sind im TSPS dokumentiert.

6. Technische Sicherheitsmaßnahmen

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

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren
Die allgemeinen Regelungen sind im TSPS dokumentiert.


V-PKI


6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer*innen
Werden die privaten Schlüssel beim TSP erzeugt, werden sie gemäß Abschnitt 4.4.1 zugestellt. In diesem Fall erfolgt die Speicherung der privaten Schlüssel beim TSP bis zur Auslieferung in einer sicheren Umgebung.

Da keine Schlüsselhinterlegung angeboten wird, wird der private Schlüssel nach der Auslieferung an den*die Zertifikatsnehmer*in beim TSP gelöscht.

6.1.3 Lieferung öffentlicher Schlüssel an den TSP

QCP-w, EVCP, OVCP, DVCP, LCP, V-PKI
Zertifikatsanforderungen können von Zertifikatsnehmern*innen zu einem vorhandenen Schlüsselpaar per PKCS#10-Request gestellt werden, der mit dem entsprechenden privaten Schlüssel signiert werden muss. Der PKCS#10-Request enthält den öffentlichen Schlüssel. Die entsprechende Response gibt das vollständige Zertifikat zurück.

6.1.4 Lieferung öffentlicher CA-Schlüssel an Zertifikatsnutzer*innen
Der öffentliche Schlüssel der CA ist im Zertifikat enthalten. Dieses Zertifikat befindet sich i. d. R. auf dem Token, das dem*der Zertifikatsnehmerin übergeben wird. Darüber hinaus können die
CA-Zertifikate aus dem öffentlichen Verzeichnis bezogen werden, in dem sie nach ihrer Erstellung veröffentlicht werden.

6.1.5 Schlüssellängen
Diese Regelungen sind im TSPS dokumentiert.

6.1.6 Festlegung der Schlüsselparameter und Qualitätskontrolle
Diese Regelungen sind im TSPS dokumentiert.
Signatur- und Verschlüsselungsalgorithmen sind im Abschnitt 7.1.3 genannt.

6.1.7 Schlüsselverwendungen
Diese Regelungen sind im TSPS dokumentiert.

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module
Die allgemeinen Regelungen sind im TSPS dokumentiert.
Wird die private EE-Schlüssel im Verantwortungsbereich des*der Zertifikatsnehmers*in erstellt, so hat dieser ebenfalls dafür zu sorgen, dass eine ausreichende Qualität bei der Schlüsselerzeugung gewährleistet ist.

V-PKI
Für die Schlüsselgenerierung und Speicherung wird das vom BSI zugelassene HSM „CryptoServer CP 5 VS-NfD Version 5.1.0.0“ (BSI-VSA-10370) verwendet.

LCP
Der TSP betreibt geeignete hard- und softwarebasierte Schlüsselgeneratoren um die Qualität der EE-Schlüssel zu sichern.

6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m)
Das HSM, auf dem die CA-Schlüssel aufbewahrt werden, befindet sich in der sicheren Umgebung des Trustcenters. Die Aktivierung des privaten Schlüssels erfordert zwei autorisierte Personen.
Ein Zugriff auf private EE-Schlüssel besteht nur im Fall von Schlüsselhinterlegung gemäß Abschnitt 6.2.3.

6.2.3 Hinterlegung privater Schlüssel (key escrow)
Private EE-Schlüssel werden vom TSP nicht hinterlegt.

6.2.4 Backup privater Schlüssel
Die allgemeinen Regelungen sind im TSPS dokumentiert.
Für private EE-Schlüssel wird kein Backup angeboten, eine Sicherung erfolgt nur im Rahmen der Hinterlegung (key escrow), wenn diese produktspezifisch verfügbar ist oder vereinbart wurde.

6.2.5 Archivierung privater Schlüssel
Diese Regelungen sind im TSPS dokumentiert.

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen
Diese Regelungen sind im TSPS dokumentiert.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen
Die allgemeinen Regelungen sind im TSPS dokumentiert.
EE-Schlüssel liegen bis zur Auslieferung verschlüsselt in einer Datenbank des TSP vor.

6.2.8 Aktivierung privater Schlüssel
Die allgemeinen Regelungen sind im TSPS dokumentiert.
Private EE-Schlüssel werden durch Eingabe des Geheimnisses aktiviert.

6.2.9 Deaktivieren privater Schlüssel
Die allgemeinen Regelungen sind im TSPS dokumentiert.
Die jeweilige Anwendung deaktiviert den privaten EE-Schlüssel, spätestens aber durch das Deaktivieren oder Löschen des Soft-PSEs.

6.2.10 Zerstörung privater Schlüssel
Die allgemeinen Regelungen sind im TSPS dokumentiert.
Schlüssel, die im Bereich des TSPs erstellt wurden, werden nach Auslieferung automatisch gelöscht.

6.2.11 Beurteilung kryptographischer Module
Diese Regelungen sind im TSPS dokumentiert.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel
Diese Regelungen sind im TSPS dokumentiert.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren
Die allgemeinen Regelungen sind im TSPS dokumentiert.
Die Gültigkeitsdauer der EE-Schlüssel und Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximal mögliche Gültigkeitsdauer beträgt:

**QCP-w, EVCP, OVCP, DVCP**
Bis einschließlich 31.08.2020 werden TLS-Zertifikate mit folgender Gültigkeitsdauer ausgestellt:
Max. 825 Tage
Ab 01.09.2020 werden TLS-Zertifikate mit folgender Gültigkeitsdauer ausgestellt:
Max. 398 Tage

**QCP-w mit der Ausprägung PSD2**
Qualifizierte Webseitenzertifikate mit der Ausprägung PSD2 werden mit folgender Gültigkeitsdauer ausgestellt:
Max. 825 Tage
V-PKI
Max. 27 Monate

LCP
63 Monate

QCP-I
EE-Zertifikate werden mit einer maximalen Gültigkeit von 39 Monaten ausgestellt.

Wird ein Zertifikat für einen längeren Zeitraum als 24 Monate ausgestellt, trägt der*die Kunde*in danach das Risiko und die Kosten eines aus sicherheitstechnischen Gründen erforderlichen Austausches.

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation von Aktivierungsdaten
Die allgemeinen Regelungen sind im TSPS dokumentiert.

Wird das Schlüsselpaar von dem*der Zertifikatsnehmer*in erzeugt, wird das Aktivierungsgeheimnis bei diesem Verfahren ebenfalls produziert und steht dem*der Zertifikatsnehmer*in unmittelbar zur Verfügung.

LCP, V-PKI
Erzeugt der TSP die EE-Schlüssel, wird entweder die PIN in einem PIN-Brief an den*die Zertifikatsnehmer*in versandt bzw. übergeben oder dem*der Zertifikatsnehmer*in über eine gesicherte TLS-Verbindung bzw. Onlineschnittstelle zur Verfügung gestellt. Der*Die Zertifikatsnehmer*in ist für die sichere Zustellung der PIN an den*die Endanwender*inverantwortlich, wenn Zertifikatsnehmer*innen und Endanwender*innen voneinander abweichen.

6.4.2 Schutz von Aktivierungsdaten
Die allgemeinen Regelungen sind im TSPS dokumentiert.

Zertifikatsnehmer*in: Die PINs werden durch ein Transport-PIN-Verfahren ausgeliefert oder einmalig in einen besonders gesicherten PIN-Brief gedruckt oder über eine TLS-gesicherte Webseite an den*die Zertifikatsnehmer*in versandt oder übergeben.

6.4.3 Andere Aspekte von Aktivierungsdaten
Keine Vorgaben.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen
Diese Regelungen sind im TSPS dokumentiert.

6.5.2 Beurteilung von Computersicherheit
Diese Regelungen sind im TSPS dokumentiert.

6.5.3 Monitoring
Diese Regelungen sind im TSPS dokumentiert.
6.6 Technische Maßnahmen während des Life Cycles

Diese Regelungen sind im TSPS dokumentiert.

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

Diese Regelungen sind im TSPS dokumentiert.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Diese Regelungen sind im TSPS dokumentiert.

6.6.3 Sicherheitsmaßnahmen während des Life Cycles

Diese Regelungen sind im TSPS dokumentiert.

6.7 Sicherheitsmaßnahmen für Netze

Diese Regelungen sind im TSPS dokumentiert.

6.8 Zeitstempel

Diese Regelungen sind im TSPS dokumentiert.

7. Profile von Zertifikaten, Sperrlisten und OCSP

7.1 Zertifikatsprofile

7.1.1 Versionsnummern

Diese Regelungen sind im TSPS dokumentiert.

7.1.2 Zertifikatserweiterungen

Diese Regelungen sind im TSPS dokumentiert.

7.1.3 Algorithmen-OIDs

In den CA- und EE-Zertifikaten wird derzeit folgender Verschlüsselungsalgorithmus verwendet:

- RSA mit OID 1.2.840.113549.1.1.1
- RSA-PSS mit OID 1.2.840.113549.1.1.10
- ECDSA (secp384r1) mit OID 1.3.132.0.34

Folgende Signaturalgorithmen werden in CA- und EE-Zertifikaten derzeit verwendet:

- SHA512 RSA mit OID 1.2.840.113549.1.1.13
- SHA256 RSA mit OID 1.2.840.113549.1.1.11
- SHA384 ECDSA mit OID 1.2.840.10045.4.3.3

SHA1 wird nicht verwendet.

7.1.4 Namensformate

Diese Regelungen sind im TSPS dokumentiert.
7.1.5 Name Constraints
Diese Regelungen sind im TSPS dokumentiert.

7.1.6 Certificate Policy Object Identifier
Diese Regelungen sind im TSPS dokumentiert.

7.1.7 Nutzung der Erweiterung „PolicyConstraints“
Diese Regelungen sind im TSPS dokumentiert.

7.1.8 Syntax und Semantik von „PolicyQualifiers“
Diese Regelungen sind im TSPS dokumentiert.

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung von CertificatePolicies
Diese Regelungen sind im TSPS dokumentiert.

7.2 Sperrlistenprofile

7.2.1 Versionsnummer(n)
Diese Regelungen sind im TSPS dokumentiert.

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen
Diese Regelungen sind im TSPS dokumentiert.

7.3 Profile des Statusabfragedienstes (OCSP)
Diese Regelungen sind im TSPS dokumentiert.

7.3.1 Versionsnummer(n)
Diese Regelungen sind im TSPS dokumentiert.

7.3.2 OCSP-Erweiterungen
Diese Regelungen sind im TSPS dokumentiert.

8. Auditierungen und andere Prüfungen
Diese Regelungen sind im TSPS dokumentiert.

9. Sonstige finanzielle und rechtliche Regelungen
Bezüglich der entsprechenden Regelungen wird auf Kapitel 9 in der CP verwiesen.