Certification Practice Statement of the D-Trust Root PKI

ENGLISH

DEUTSCH

Certification Practice Statement of the D-TRUST Root PKI

Version 4.0

COPYRIGHT NOTICE AND LICENSE

Certification Practice Statement of the D-TRUST Root PKI

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

The English version is a translation, the contents of which match the German version of the CPS.

Please note that only the German version of this CPS is authoritative.

Document History

Version	Date	Description
2.0	2017-01-01	▪ As part of the introduction of qualified products pursuant to EN 319 411-2 and eIDAS, the document version was raised to 2.0. ▪ The Certificate Policy document history up to this point in time can be found in version 1.15 from 3 October 2016.
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 3.2.2, 3.2.2, 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 ▪ Full annual review of the CPS ▪ Editorial changes
2.6	2019-05-15	▪ Addition of revocation via the website ▪ Addition of the qualified seal (QSealC) with PSD2 extension ▪ 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]
2.8	2019-10-09	▪ Update according to the CAB's observation report ▪ Clarification of section 5.5.2 ▪ Editorial changes
2.9	2020-03-19	▪ 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	▪ 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	2020-08-18	▪ Introduction of an EEC Root CA and two ECC Sub CAs for QCP-n-qscd and QCP-l-qscd
3.0	2020-11-10	▪ From version 3 or higher, the Root CPS is subordinate to the TSPS ▪ Update according to observation report
3.1	2021-04-23	▪ Link replaced in section 1.1.3 ▪ Introduction of the current "CA root inclusion" process in section 1.1.3 ▪ Full annual review of the CPS ▪ Amendments in sections 1.5.3, 2.2, 3.1.4, 3.2.2, 6.1.1, 7.1.3
3.2	2021-05-03	▪ Introduction of the new CAs for QES and QSEAL in section 1.1.3 ▪ Editorial changes in section 7.1.3
3.3	2021-07-06	▪ Introduction of new qualified CAs in section 1.1.3 ▪ Announcement of the introduction of a personalized certificate order portal named "D-TRUST Portal" and the following web address: https://portal.d-trust.net/. The go-live has yet to be announced. ▪ Introduction of a new revocation method in section 4.9.3 in conjunction with the "D-TRUST Portal" to be introduced. ▪ Update in the context of the BR Self Assessment ▪ Editorial changes and amendments in sections 1.6.1, 2.3, 3.1.1, 3.1.4, 3.1.6, 3.2, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 4.3.1, 4.9.5, 7.1.3, 7.1.6
3.4	2021-08-19	▪ Announcement of the D-TRUST portal go-live ▪ Amendments in section 1.1.3, 1.6.1 and 3.1.4
3.5	2021-10-14	▪ Amendments in sections 3.1.4 and 6.1.1
3.6	2022-04-14	▪ Informative introduction of the NCP policy level ▪ Renaming of the QCP-w policy level to QEVCP-w and introduction of the QNCP-w policy level ▪ Amendments in sections 1.1.3 and 6.1.3 ▪ Full annual review of the CPS
3.7	2022-08-22	▪ Amendments and concretisations in section 1.1.3, 3.2.3, 4.2.1, 4.5.1 and 6.3.2 ▪ Introduction of the current "CA root inclusion" in section 1.1.3
3.8	2022-11-17	▪ Concretisations in section 1.1.3 and 4.9.6
3.9	2023-02-14	▪ Introduction of the new qualified sub-CA „D-TRUST CA 3-21-3 2022" in section 1.1.3 ▪ Concretisations in section 1.1.3 and 3.1.4
3.10	2023-05-25	▪ Full annual review of the CPS ▪ Amendments and concretisations in section 1.1.3, 4.4.1, 6.1.1
4.0	2023-10-20	▪ As of 19 July 2023, TLS and S/MIME products will no longer be offered through the website. Therefore, the following policy levels have been deleted: QEVCP-w, QNCP-w, EVCP, OVCP, LCP, NCP and QCP-l with PSD2. ▪ Full review of the CPS

Contents

1. Introduction

1.1 Overview

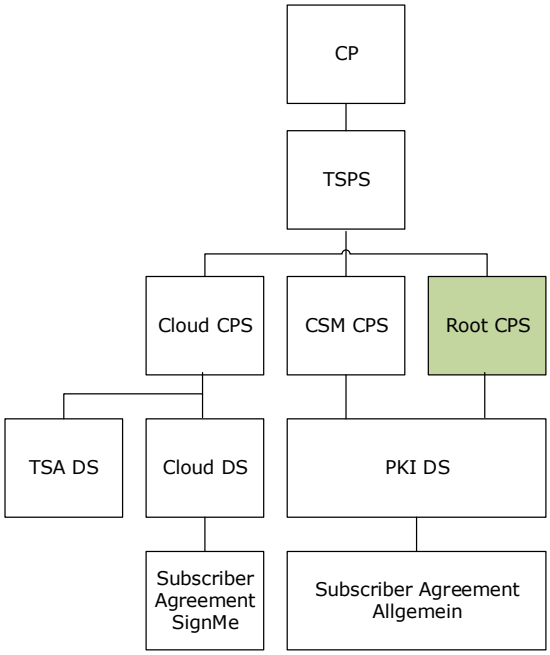
This document is the Certification Practice Statement (CPS) for the trust services operated by D-Trust GmbH that are provided via the D-TRUST Root PKI. The document name is abbreviated **Root CPS** and is subject to the Trust Service Practice Statement of D-TRUST (abbreviated as TSPS) and the Certificate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

1.1.1 Trust service provider

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 TSPS.
- **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.

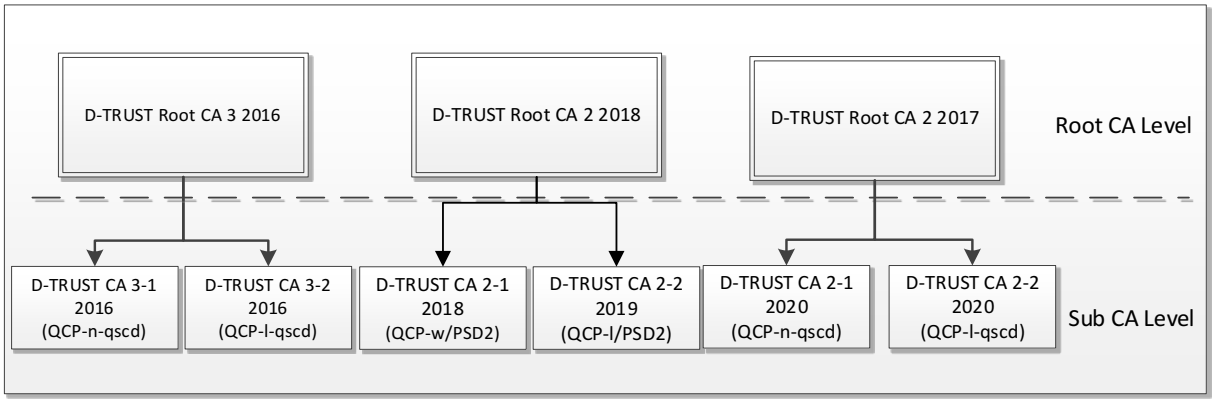
The structure of this document is based on the RFC 3647 Internet standard: *"Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework"*.

Other rules are documented in the TSPS.

1.1.3 Properties of the PKI

The PKI described here features a multi-level hierarchy. Figs. 1, 2 and 3 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.

PKI for qualified trust services



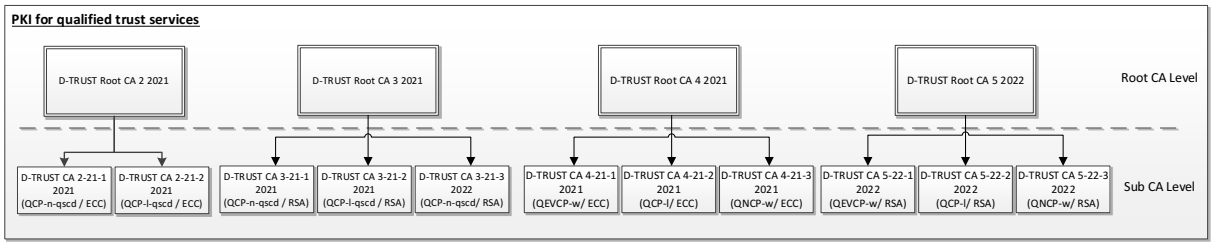


Fig. 1: Currently valid PKI hierarchy for qualified trust services[1]

[1] The following sub-CAs in Fig. 1 are included in the Federal Network Agency's Trusted List and have been put into operation: D-TRUST CA 2-21-1 2021, D-TRUST CA 2-21-2 2021, D-TRUST CA 3-21-1 2021, D-TRUST CA 3-21-2 2021, D-TRUST CA 3-21-3 2022, D-TRUST CA 4-21-1 2021, D-TRUST CA 4-21-2 2021, D-TRUST CA 4-21-3 2021 and the sub-CAs from the D-TRUST Root CA 5 2022.

Remarks: In addition to qualified end-user certificates for signature purposes the sub-CA „D-TRUST CA 3-21-3 2022" issues non-qualified end-user certificates for authentification purposes. These two types of certificates are delivered together to the end-user on a qscd.

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

QCP-n-qscd – Qualified personal certificates on a qualified signature creation device

QCP-l-qscd – Qualified seal certificates on a qualified signature creation device (QSealC)

QCP-l – Qualified seal certificates without a qualified signature creation device (QSealC)

The policy levels are explained in the TSPS.

PKI for publicly trusted services[2] (non-qualified trust services)

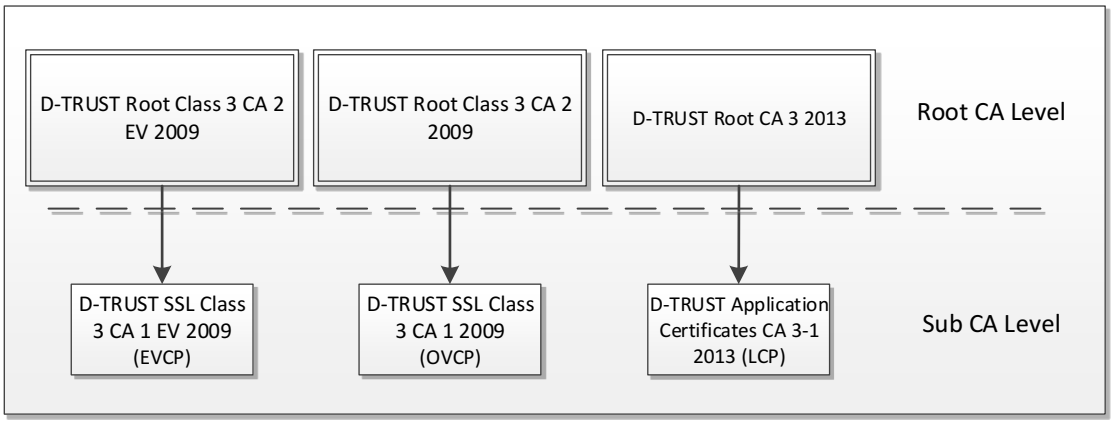


Fig. 2: Currently valid PKI hierarchy for publicly trusted services

This CPS refers to certificates that can be ordered via the website. This request route will be switched off from 19 July 2023 for products with policy level QEVCP-w, QNCP-w, EVCP, OVCP, LCP, NCP and QCP-l with PSD2. Certificates already issued will remain valid since the PKI will continue to operate. Information will still be provided for all certificates, regardless of the request procedure. Certificates with the above policy levels will be offered in future exclusively via the Certificate Service Manager (CSM) and are described in the CSM CPS (https://www.d-trust.net/internet/files/D-TRUST_CSM_PKI_CPS.pdf).

CA certificates

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

https://www.d-trust.net/files/dokumente/pdf/pki_structure_and_applicable_documents.pdf

---

The "D-TRUST Root CA 2 2021" replaces the "D-TRUST Root CA 2 2017" and the "D-TRUST Root CA 3 2021" replaces the "D-TRUST Root CA 3 2016". The "D-TRUST Root CA 4 2021" replaces the "D-TRUST Root CA 2 2018".

No new certificates will be created from the sub CAs of the "D-TRUST Root CA 2 2018" from 14 January 2021 onwards.

[2] "Publicly trusted" services are trust services according to the specifications of the Certificate Consumer members of the CA Browser/Forum combined with the specifications of the CA Browser/Forum.

The following table provides an overview of all root CAs and the associated sub-CAs to which this CPS applies.[3]

D-TRUST Root CA 3 2016 https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_3_2016.crt Fingerprint: SHA1: 16ABFE955BBA80F0D7079D240188C633DF5DDB7F SHA256: 828F0AA17DC578DB836FBCAFB60BEFEBAC1551080AEB60D1264DDBB1561230EA
D-TRUST CA 3-1 2016 https://www.d-trust.net/cgi-bin/D-TRUST_CA_3-1_2016.crt Policy Level: QCP-n-qscd Fingerprint: SHA1: 38A577328FAD50472F94D47AB433D88F8F36A22D SHA256: 454A164B9236CF9C380DF9959F751DED503F91BE3EC646C7042CBB0E1E17A7D5 OID: 1.3.6.1.4.1.4788.2.150.1
D-TRUST CA 3-2 2016 https://www.d-trust.net/cgi-bin/D-TRUST_CA_3-2_2016.crt Policy Level: QCP-l-qscd Fingerprint: SHA1: 7927b0fda41b2a2465aa4e727d8bac8dd0db5aad SHA256: 44AD63979AF0794DB890B96A9BE63A17F5ADF7AC47FE91B008FF04E3EEB9FCCD OID: 1.3.6.1.4.1.4788.2.150.2
D-TRUST Root CA 2 2018 (Legacy) https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_2_2018.crt Fingerprint: SHA1: 4B467FB8D2051D7BC4CDB73377FA7077034BCCE1 SHA256: 113BBD9EFFFA4C743D6D09038DC0AAB1A5F1FAD7492868193917C63D82D74FA1
D-TRUST CA 2-1 2018 (Legacy) https://www.d-trust.net/cgi-bin/D-TRUST_CA_2-1_2018.crt Policy Level: QEVCP-w Fingerprint: SHA1: 5982BDD5E228E4869461713710CC5C3DDE006C43 SHA256: 5F28B888456D21158C5E3E8A31719CF3B305300BC5B436B696BE22F6973F1DF1 OID: 1.3.6.1.4.1.4788.2.150.4

[3] Certificates from the greyed-out CAs are no longer offered via the request channels described in this Root CPS. Certificates already issued will remain valid since the PKI will continue to operate. Information will still be provided for all certificates, regardless of the request procedure. The CAs are expected to be deleted from this CPS at the end of 2025.

D-TRUST CA 2-2 2019 (Legacy) https://www.d-trust.net/cgi-bin/D-TRUST_CA_2-2_2019.crt Policy Level: QCP-l Fingerprint: * SHA1: 455FD6F160938C1FCCE1EF8D4F33700F2148FF87 SHA256: E85F41CE30CF9910CB8D12470F9E312E8F862FFED0581F5995772D8B46CB7E99 OID: 1.3.6.1.4.1.4788.2.150.5
D-TRUST Root CA 2 2017 http://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_2_2017.crt Fingerprint: SHA1: 357BB8CC3855B401F7C64CFF35689F83C860374D SHA256: E152527EB90B3034818589D31C3CC4EE1C896446AC4E29EA8F546B3419165B90
D-TRUST CA 2-1 2020 https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_2-1_2020.crt Policy Level: QCP-n-qscd Fingerprint: * SHA1: D00C842434F42BD4903518CA3B0E9EC49976EE2F SHA256: A5D944F0C6598C8A3A421AB320DD6E82E1C7A373B4812FFB2508F638804082AB OID: 1.3.6.1.4.1.4788.2.150.1
D-TRUST CA 2-2 2020 https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_2-2_2020.crt Policy Level: QCP-l-qscd Fingerprint: * SHA1: ECE3B420B2FE38F56E036A8D507FFDA229024CE3 SHA256: C0671426DE62A9BAA23C28EF9EFF21B5C3DDF0673BEE59EA43B0CE0C6E30FE85 OID: 1.3.6.1.4.1.4788.2.150.2
D-TRUST Root Class 3 CA 2 EV 2009 https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_EV_2009.crt Fingerprint: SHA1: 96C91B0B95B4109842FAD0D82279FE60FAB91683 SHA256: EEC5496B988CE98625B934092EEC2908BED0B0F316C2D4730C84EAF1F3D34881
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: B0935DC04B4E60C0C42DEF7EC57A1B1D8F958D17988E71CC80A8CF5E635BA5B4 OID: 1.3.6.1.4.1.4788.2.202.1

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: 58E8ABB0361533FB80F79B1B6D29D3FF8D5F00F0 SHA256: 49E7A442ACF0EA6287050054B52564B650E4F49E42E348D6AA38E039E957B1C1
D-TRUST SSL Class 3 CA 1 2009 https://www.d-trust.net/cgi-bin/D-TRUST_SSL_Class_3_CA_1_2009.crt Policy Level: OVCP Fingerprint: SHA1: 2FC5DE6528CDBE50A14C382FC1DE524FAABF95FC SHA256: 6AC159B4C2BC8E729F3B84642EF1286BCC80D775FE278C740ADA468D59439025 OID: 1.3.6.1.4.1.4788.2.200.1
D-TRUST Root CA 3 2013 https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_3_2013.crt Fingerprint: SHA1: 6C7CCCE7D4AE515F9908CD3FF6E8C378DF6FeF97 SHA256: A1A86D04121EB87F027C66F53303C28E5739F943FC84B38AD6AF009035DD9457
D-TRUST Application Certificates CA 3-1 2013 https://www.d-trust.net/cgi-bin/D-TRUST_Application_Certificates_CA_3-1_2013.crt Policy Level: LCP (1.3.6.1.4.1.4788.2.200.2), NCP (1.3.6.1.4.1.4788.2.200.3) Fingerprint: SHA1: 1785B07501F0FCEFFC97C6B070C255A8A9B99F12 SHA256: CB0F7B7670EA2B818ABE80587902434B30EF7A8C0273B84884243F89593EA630 OID in CA certificate: 1.3.6.1.4.1.4788.2.200.1 (Legacy)
D-TRUST Root CA 2 2021 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_2_2021.crt Fingerprint: SHA1: 468C467671DD4F1A38145104C353C99276107702 SHA256: E7A79A64F101897903D5B054564672E5D5C803437405D15321A1A5763710AF70
D-TRUST CA 2-21-1 2021 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-TRUST_CA_2-21-1_2021.crt Policy Level: QCP-n-qscd Fingerprint: SHA1: F78B7AA28BACD8E004C1A7FEEE7BD035BC1B5AD7 SHA256: 620BA94502329A506F3A2AFB6500DA9FA437C946E8D6E4B7C2148C29C8E76A8E OID: 1.3.6.1.4.1.4788.2.150.1

D-TRUST CA 2-21-2 2021 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-TRUST_CA_2-21-2_2021.crt Policy Level: QCP-l-qscd Fingerprint: SHA1: BC0FA0A53582E8E5434F0AEACCEE32A2C3CD9443 SHA256: B3472A9A9DB78EBBC260EA628BD44B593C3D7B1367F25DFAD659FF5E9198B0DF OID: 1.3.6.1.4.1.4788.2.150.2
D-TRUST Root CA 3 2021 (RSA, 4096 Bit) https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_3_2021.crt Fingerprint: SHA1: E4F95E877D3D6519336040A2B0C853F8A1B57194 SHA256: 390F7FE59E7AEE6D271527CFA0D53B2E67B3F7FABECEDB65FB10AAFF34F13FF2
D-TRUST CA 3-21-1 2021 (RSA, 4096 Bit) https://www.d-trust.net/cgi-bin/D-TRUST_CA_3-21-1_2021.crt Policy Level: QCP-n-qscd Fingerprint: SHA1: 9F729EFAF98688C7F946ED8012A8773088B037C1 SHA256: C67EBB0BFA6497ACFBD5423ED5A2DA5497E82092A4C475200DCC273CC8CFC69C OID: 1.3.6.1.4.1.4788.2.150.1
D-TRUST CA 3-21-2 2021 (RSA, 4096 Bit) https://www.d-trust.net/cgi-bin/D-TRUST_CA_3-21-2_2021.crt Policy Level: QCP-l-qscd Fingerprint: SHA1: 767E3E3FDE06FE00199205F36B4EA7723562133C SHA256: E628B19986782CEB2094DB982E749ADCD7CA02C58DB0C7B8B2ECE7869A07897A OID: 1.3.6.1.4.1.4788.2.150.2
D-TRUST CA 3-21-3 2022 (RSA, 4096 Bit)[4] https://www.d-trust.net/cgi-bin/D-TRUST_CA_3-21-3_2022.crt Policy Level: QCP-n-qscd Fingerprint: SHA1: 5601F434AB54C3EADDBEBA430ABD9B40065E2341 SHA256: 0DF80683B392814EF75A12F665A810D36D0754FB297F24C65729C7A771022A5B OID: 1.3.6.1.4.1.4788.2.150.1

[4] Remarks: In addition to qualified end-user certificates for signature purposes the sub-CA „D-TRUST CA 3-21-3 2022" issues non-qualified end-user certificates for authentification purposes. These two types of certificates are delivered together to the end-user on a qscd.

D-TRUST Root CA 4 2021 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_4_2021.crt Fingerprint: SHA1: A48CDA4E279A7E8996BF2D1EF1263DD16068092A SHA256: 70A9EF005779FCEE0619A644AF439FD3AF3379E645530F35BD6AE68EFF19D2BF
D-TRUST CA 4-21-1 2021 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-TRUST_CA_4-21-1_2021.crt Policy Level: QEVCP-w Fingerprint: SHA1: 74B857941F0EB9BC0FB9A3FEA83AEA836E0A5E22 SHA256: 4EA66AB8FC54D446F6A46A63F0FCA5FE83A1F433CDE771DE8D1A8BE06647D008 OID: 1.3.6.1.4.1.4788.2.150.4
D-TRUST CA 4-21-2 2021 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-TRUST_CA_4-21-2_2021.crt Policy Level: QCP-l Fingerprint: SHA1: 07BBB6424795283CC3757E91642AF95055DB85D4 SHA256: 5EF6EB4690E15C57C25A0296A9A93488B86AA5878A3DFC0859855CC5EB378A00 OID: 1.3.6.1.4.1.4788.2.150.5
D-TRUST CA 4-21-3 2021 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-TRUST_CA_4-21-3_2021.crt Policy Level: QNCP-w Fingerprint: SHA1: EF175B7CC271EFEC0406EDB610C909DF88FA8202 SHA256: 884864ACDB55E55BF1E5CF648EF434491E2F6990FF4A952E3FA4763A1A6C33BB OID: 1.3.6.1.4.1.4788.2.150.3
D-TRUST Root CA 5 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_5_2022.crt Fingerprint: SHA1: 643211332169B483B55F7046E56CBFC6C11DC5F8 SHA256: D839672F984DCA7CD480CE201627A4DE61C5C1855F450E5B706200E73A23F047
D-TRUST CA 5-22-1 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-TRUST_CA_5-22-1_2022.crt Policy Level: QEVCP-w Fingerprint: SHA1: 5B26CCEEC541B3886A76761A9503667027C8B94A SHA256: A028FB2822D0C2699A451B7083A984318F7A0102A3B42F5B089D99CF3F9149C3 OID: 1.3.6.1.4.1.4788.2.150.4

D-TRUST CA 5-22-2 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-TRUST_CA_5-22-2_2022.crt Policy Level: QCP-l Fingerprint: SHA1: 34156C420F146160795B5E2CC4EF343C258C16BF SHA256: F0A1CA5FC42E6A8514C63415054F14EF7BB961ADBC7A94185D8E410A905B8109 OID: 1.3.6.1.4.1.4788.2.150.5
D-TRUST CA 5-22-3 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-TRUST_CA_5-22-3_2022.crt Policy Level: QNCP-w Fingerprint: SHA1: 8A259DBB8B8C3AB5971B94590C7BABAFE57B5E1F SHA256: D9B38F7314AAB95DE57B63784F7D123D031C4FED6D8F66ED55A91BD05FEA818B OID: 1.3.6.1.4.1.4788.2.150.3

Both CA and EE certificates can contain references to CPs or OIDs which define detailed requirements and restrictions.

1.2 Document name and identification

Document name:	Certification Practice Statement of the D-TRUST Root PKI
Version	4.0

1.3 PKI entities

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

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

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 above, [eIDAS] and [EN 319 411-2] have priority.

1.6 Definitions and acronyms

1.6.1 Definitions and names

D-TRUST Portal (https://portal.d-trust.net/)	In contrast to D-Trust's earlier order pages, with the new certificate order portal named "D-Trust Portal" and the "https://portal.d-trust.net/" web address, the customer or applicant registers and then receives personalized access or an account. The customer or applicant can use this account to manage (request, revoke) personal qualified signature cards or qualified signature cards applied for on behalf of a legal entity.

Further rules are documented in the CP.

1.6.2 Acronyms

CP	Certificate policy

Further 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 test websites
- The TSPS
- This CPS
- The Subscriber Agreement
- PKI user information for qualified trust services

Other rules are documented in the TSPS.

2.3 Publication frequency

QCP-l-qscd, 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.

QCP-n-qscd
EE certificates can be published, i.e. entered in the public repository of the TSP. The subscriber can accept or refuse publication. 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.

Publication will take place immediately after a certificate has been issued, unless publication has been refused.

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

- at least 10 years (QCP-n-qscd, QCP-l-qscd, QCP-l) and until the end of the year.

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 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. If a CA certificate is revoked, the CA revocation list is published within 24 hours.

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.500] or [X.509] standard, these names are given as distinguished names.

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

3.1.2 Need for telling names

The *distinguished name* 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.

Freedom of choice in selecting pseudonyms can be agreed to, see section 3.1.6. The TSP reserves the right to reject assigning a particular pseudonym without having to justify the decision.

In the case of certificates that were created with pseudonyms, the TSP also records the end-entity's (and, if applicable, the subscriber's) real identity in the documentation.

3.1.4 Rules for the interpretation of different name forms

The attributes of the *distinguished name* (DN components) of EE certificates are interpreted as follows:

DN component	Interpretation
G (givenName)	*Given name(s)* of the natural person - QCP-l, QCP-l-qscd: This field is not used. - QCP-n-qscd: According to the proof used for identification

DN component	Interpretation
SN (surname)	*Surname* of the natural person - QCP-l, QCP-l-qscd: This field is not used. - QCP-n-qscd: According to the proof used for identification If pseudonyms are used, SN corresponds to CN.
CN (commonName) (2.5.4.3)	*Common name:* The following variants are used: - Natural persons without a pseudonym: "name(s) surname". - 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. - 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 - Technical components: Name of the server, service or application using the certificate
SAN (subjectAltName)	The following variants are used: - E-mail address of the subscriber - Technical components: Name of the server, service or application using the certificate
PN (pseudonym)	*Pseudonym*: Identical to CN.
Serial Number (serialNumber) (2.5.4.5)	*Serial number*: Name suffix number to ensure unambiguity of the name (typically the application number). Other product-specific uses of the field are possible.
O (organizationName) (2.5.4.10)	Official name of the subscriber or name of the *organization* to which the end-entity belongs or to which he or she is otherwise affiliated (company, public authority, association, etc.) according to the proof of existence; if necessary, reduced to a meaningful name if the maximum number of 64 characters is exceeded.
OU (organizationalUnitName) (2.5.4.11)	Organizational unit of the organization, such as department, division or other sub-division

DN component	Interpretation
OrgID (organizationIdentifier) (2.5.4.97)	**QCP-l-qscd**: *Unambiguous organization number* of the organization. The number of the commercial register as well as the VAT ID number or a number assigned by D-Trust can be entered. 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: DT:DE-1234567890 (DT: D-TRUST; DE: Germany; random number that is unambiguously assigned to the organization).
C (countryName) (2.5.4.6)	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 that issued the document that was used to identify the subscriber.
Street (streetAddress) (2.5.4.9)	Postal address *Street and Number*
Locality (localityName) (2.5.4.7)	Postal address *City*
State (stateOrProvinceName) (2.5.4.8)	Postal address *(Federal) state*
PostalCode (postalCode) (2.5.4.17)	Postal address *Postal code*

Further rules are documented in section 7.1.4 of the TSPS.

QCP-n-qscd
Qualified certificates for natural persons include, as a minimum, the subject DN components: "commonName", "countryName", "serialNumber" as well as either "GivenName" and "Surname" or "Pseudonym".

QCP-l, QCP-l-qscd
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 end-entity's ("Subject" field) name (DistinguishedName) used in EE certificates is always assigned within this PKI to the same subscriber or end-entity, respectively.

The serial number ensures the unambiguity of the certificate.

The TSP ensures the unambiguity of *distinguished names* 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).

3.2 Initial identity verification

A procedure is established which ensures that the data sources for the validation of certificate content are checked and released. All data sources are approved by the D-Trust organizational unit for information security.

3.2.1 Proof of ownership of the private key

Key pairs of subscribers are produced in the TSP's sphere of responsibility. The TSP forwards the signature or seal card (QCP-n-qscd, QCP-l-qscd) 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.

3.2.2 Identification and authentication of organizations

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 checking are subject to the requirements of [EN 319 411-1] and [EN 319 411-2] for QCP-l or QCP-l-qscd. Verification 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 mentioned are described in section 4.2.1.

	QCP-l, QCP-l-qscd
CN	Register/ Non-Register
C	
O	
OrgID	Register
OU	C confirmation / A confirmation / Register
STREET	Register/ Non-Register
L	
State	
PostalCode	

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-l, QCP-l-qscd.

The relevant certificate information, which is taken from the register extracts, is written into the certificate fields exactly as it is published in the extract from the register.

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.

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.

	QCP-n-qscd
G	Pers-Ident/ eID/ NotarIdent/ BotschaftsIdent
SN	
CN	Pers-Ident/ eID/ NotarIdent/ BotschaftsIdent
C	
O	Register/ Non-Register/ C confirmation/ A confirmation
OU	C confirmation/ A confirmation
Alternative applicant (SAN)	e-mail
All other attributes	A confirmation/ out-of-band mechanisms

Documents in non-Latin characters are not accepted.

3.2.4 Non-verified information concerning the subscriber

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 alternative names, e.g. LDAP directories, etc. as well as certificate extensions (AdditionalInformation, monetaryLimit, etc.), if any, are not checked for correctness.

3.2.5 Verification of request authorization

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

In the case of organizations, proof of their existence and the applicant's right 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, however, the end-entity's previously validated data and documents that are still valid can be used.

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] or [EN 319 411-2]. The conditions of section 4.7 must be fulfilled.

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:

- Subscribers with a user account in the D-Trust portal can authenticate themselves using their username and password and revoke their certificates directly in the account (https://portal.d-trust.net/).
- Electronic revocation requests submitted via an online interface can be authorized using a secret transmitted via a previously agreed to and secure channel (e.g. SMS TAN, revocation password).
- Written revocation requests from the subscriber or an authorized third party are checked on the basis of the signature of the party requesting revocation.

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

Revocation procedures are defined in section 4.9.

4. Operational Requirements

4.1 Certificate request and registration

4.1.1 Request authorization

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

The general rules are documented in the TSPS.

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-n-qscd, QCP-l-qscd and QCP-l 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.

4.2 Processing the certificate request

4.2.1 Performing identification and authentication processes

As part of the Root 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
eID
NotarIdent
BotschaftsIdent
Register
Non-Register
C confirmation
A confirmation
Out-of-band mechanisms
E-mail address

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 Root CPS, the following specific rules are also applicable:

QSCD
When QSCDs are created, the TSP logs or records all events in an auditable manner.

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

Smart cards are sent either by post or courier to the address stated, or they are handed over in person to the subscriber by the RA or an authorized employee or representative, or, if requested by the subscriber, handed over to the end-entity.

QCP-l
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.

QCP-n-qscd, QCP-l-qscd
The TSP uses qualified signature/ seal creation devices only and, as long as the issued qualified certificates are valid, monitors the status of these qualified signature/ seal creation devices within the meaning of EN 319 411-2. The PIN is handed over separately to the end-entity.

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

If the subscriber consented to certificate publication in the certificate application, once produced, the certificates will be published in the public repository service. The certificate will not be published if the subscriber has not consented to publication.

4.4.3 Notification of other PKI entities concerning the 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 Private key and certificate use 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 (keyUsage) stated in the certificate.

QCP-n-qscd, QCP-l-qscd, QCP-l
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.

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 TSP offers a corresponding procedure for the chosen product.

4.7.3 Processing an application for certificate renewal

The rules laid down in section 4.3 apply.

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 rules laid down in section 4.4.1 apply.

4.7.6 Publication of the certificate renewal by the TSP

The rules laid down in section 4.4.2 are applicable, depending on the details of the initial application.

4.7.7 Notification of other PKI entities concerning certificate renewal

The rules laid down in section 4.4.3 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 3.4.

4.9.2 Authorization to revoke

These rules are documented in the TSPS.

4.9.3 Revocation request procedure

If a revocation password was agreed to, revocation requests can be submitted by e-mail, by phone or via the online interface.

Certificates can be generally revoked 24/7 using the online interface. Both subscribers and persons authorized to revoke can use the online interface to revoke certificates as long as they authenticate themselves with their agreed revocation password.

Online interface: https://my.d-trust.net/sperren

If necessary, subscribers or persons authorized to revoke can request telephone support when revoking a certificate. In this case, they will be required to provide support staff with their application ID and the pertinent revocation password so that entries can then be made on their behalf via the online interface.

Telephone support: +49 (0)30 / 25 98 – 0

For customers who are registered in the D-Trust Portal (https://portal.d-trust.net/) and order qualified signature or seal cards via this portal:

If qualified signature or seal cards were ordered using a personal account in the D-Trust Portal, revocation must also be carried out there. The organization's authorized party must still revoke the card using the following address: https://my.d-trust.net/sperren.

When the card is revoked, all of the pertinent certificates will also be revoked. Revocation is final and cannot be reversed.

To revoke a certificate via e-mail, the subscriber or the person authorized to revoke states the application ID of the certificate and the pertinent revocation password. Revocation requests received by e-mail are processed the next working day at the latest.

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

A revocation request can also be submitted by post.

Address for written revocation requests:
D-Trust GmbH
Kommandantenstr. 15
10969 Berlin

A written revocation request must unambiguously describe the certificate to be revoked and must therefore contain the following details:

- Name of the party requesting revocation
- Subscriber's name
- Serial number of the certificate in order to enable unambiguous identification of the certificate

The party requesting revocation must know their revocation password because this is then needed for subsequent telephone verification.

A specific date for revocation in the future, in as far as the date is within the validity period of the certificate, can only be stipulated within the scope of a written revocation request; a written revocation request is only accepted when a specimen signature is available. Revocation by telephone or via the online interface comes into effect immediately.

Status changes in the OCSP are available for query immediately after revocation. Status changes in a CRL contain the same revocation information, but it can take up to 60 minutes for the latest CRL to be published.

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. The subscriber or the end-entity, respectively, will be informed once the certificate has been revoked.

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

4.9.4 Revocation request deadlines

These rules are documented in the TSPS.

4.9.5 Time span for processing a revocation request by the TSP

Revocation requests can be submitted 24/7 via by phone or via the online interface. Revocation takes place according to section 4.9 of [BRG].

Revocation requests received in writing are processed the next working day at the latest.

4.9.6 Methods available for checking revocation information

Up-to-date revocation information is maintained in certificate revocation lists which can be retrieved via the LDAP[5] 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.

QCP-n-qscd, QCP-l-qscd, QCP-l
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.

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.

[5] In future, revocation lists will only be offered via an http link.

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

A request can be submitted to deposit private EE keys.

According to [EN 319 411-1] and [EN 319 411-2], the TSP does not offer key escrow for qualified certificates. 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.

QCP-l

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].

QCP-l-qscd, QCP-n-qscd

If EE keys are generated by the TSP, these keys are generated with the help of an HSM or on a qualified signature/ seal creation device in the secure environment of the trust service provider and in accordance with the requirements of [EN 319 411-2].

If EE keys and EE certificates are generated on or attached to smart cards or other hardware-based tokens, the TSP performs procurement, storage, personalization and PIN handling according to the applicable requirements of the smart-card or token manufacturer or certification body.

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-l

Certificate requests can be submitted by subscribers for a key pair generated by the subscriber 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 listed in section of 7.1.3.

6.1.7 Key uses

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.

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.

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 PIN.

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 card is removed from the card reader or the soft PSE is deactivated or deleted.

Private EE keys on smart cards are permanently deactivated when an incorrect PIN was entered several times in succession. The card can be reactivated a limited number of times by entering the PUK. Multiple signature cards do not have a PUK.

6.2.10 Destruction of private keys

The general rules are documented in the TSPS.

QCP-n-qscd, QCP-l-qscd
When the card chip is destroyed or the files containing the private EE key are deleted, the private key is then also destroyed.

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-l, QCP-l-qscd, QCP-n-qscd
EE certificates are issued with a maximum period of validity of 39 months. A longer period of validity can be contractually agreed to.

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.

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

QCP-n-qscd, QCP-l-qscd
If the TSP generates the keys, either a transport PIN process is used or the PINs are printed in a PIN letter that is sent or handed over to the subscriber.

6.4.2 Protection of activation data

The general rules are documented in the TSPS.

Subscriber: In the case of the transport PIN method, the transport PIN shows the card integrity. In other methods, the PINs are printed once in a specially protected PIN letter, or sent via an TLS-secured website or handed over to the subscriber.

6.4.3 Other aspects of activation data

In addition to the PIN, subscribers with a signature card are also offered on a product-specific basis a Personal Unblocking Key (PUK) number to unblock the signature card (after entering an incorrect PIN three times).

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 algorithms are currently used in the subjectPublicKeyInfo in CA and EE certificates:

- rsaEncryption with OID 1.2.840.113549.1.1.1
- id-RSASSA-PSS with OID 1.2.840.113549.1.1.10 (is not used for EVCP, OVCP)

The following curves are currently used for ECC keys in CA and EE certificates:

- secp384r1 with OID 1.3.132.0.34
- secp521r1 with OID: 1.3.132.0.35
- secp256r1 with OID: 1.2.840.10045.3.1.7

The following signature algorithms are currently used in CA and EE certificates:

- sha512WithRSAEncryption with OID 1.2.840.113549.1.1.13
- sha384WithRSAEncryption with OID 1.2.840.113549.1.1.12
- sha256WithRSAEncryption with OID 1.2.840.113549.1.1.11
- ecdsa-with-SHA256 with OID 1.2.840.10045.4.3.2
- ecdsa-with-SHA384 with OID 1.2.840.10045.4.3.3
- ecdsa-with-SHA512 with OID 1.2.840.10045.4.3.4

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

"CertificatePolicies" may contain the OIDs of supported CPs.

Further rules are documented in the section 1.1.3 of the CP.

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 Root PKI

Version 4.0

COPYRIGHT UND NUTZUNGSLIZENZ

Certification Practice Statement der D-TRUST Root PKI

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

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

Dokumentenhistorie

Version	Datum	Beschreibung
2.0	01.01.2017	▪ Im Rahmen der Einführung von qualifizierten Produkten gemäß EN 319 411-2 und eIDAS, wurde die Version des Dokumentes auf 2.0 hochgezählt. ▪ Die Dokumentenhistorie der Zertifikatsrichtlinie bis zu diesem Zeitpunkt kann in der Version 1.15 vom 03.10.2016 nachgelesen werden.
2.1	01.10.2017	▪ Editorische Änderungen und Konkretisierung des Kapitels 6.5
2.2	28.03.2018	▪ Editorische Änderungen und eine Überarbeitung der Kompatibilität mit RFC 3647 ▪ Anpassung Nutzungslizenz an „Creative Commons Attribution" ▪ Angleichung an die Mozilla Root Store Policy 2.5
2.3	05.07.2018	▪ Änderung der Domain-Validierungsmethoden in 3.2.2, 3.2.3, 4.2.1 ▪ Feld OrgID in Abschnitt 3.1.4 wurde gemäß Variante 3 aus Kapitel 5.1.4 der EN 319 412-1 ergänzt. ▪ Redaktionelle Anpassungen
2.4	11.10.2018	▪ Tabellarische Darstellung der CA Zertifikate in Abschnitt 1.1.3 ▪ Ergänzungen in Kapitel 7.3 ▪ Anpassungen der Abschnitte 1.5.2 und 4.9 gemäß Ballot SC6v3 aus dem CAB-Forum
2.5	30.11.2018	▪ Dieses CPS entspricht den Anforderungen der Mozilla Policy 2.6.1 ▪ Jährliches Review des gesamten CPS ▪ Redaktionelle Anpassungen
2.6	15.05.2019	▪ Ergänzung des Widerrufs über die Webseite ▪ Ergänzung der qualifizierten Siegel (QSealC) mit der Ausprägung PSD2 ▪ Ergänzung der qualifizierten Website Authentication Zertifikate (QWACs) mit der Ausprägung PSD2 ▪ Jährliches Review des gesamten CPS ▪ Redaktionelle Anpassungen
2.7	22.05.2019	▪ Ergänzung der qualifizierten Siegelzertifikate mit der Ausprägung PSD2 ohne QSCD ▪ 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.
2.8	09.10.2019	▪ Update nach observation report vom CAB ▪ Präzisierung des Abschnitts 5.5.2 ▪ Editorische Änderungen
2.9	19.03.2020	▪ Dieses CPS entspricht den Anforderungen der Mozilla Policy 2.7 ▪ Jährliches Review des gesamten CPS ▪ Anpassung der Aufbewahrungsfrist für LCP in Abschnitt 5.5.2 ▪ Ergänzung des SHA-256 Fingerprints in Abschnitt 1.1.3 ▪ Ergänzung der Domainvalidierungsmethoden in Abschnitt 4.2.1

2.10	27.04.2020	▪ Ergänzungen zur Verifikation der Zertifikatskette in Abschnitt 4.5.2 ▪ Ergänzungen in den Abschnitten 5.3.7 und 5.5.2 ▪ Reduzierung der Gültigkeitsdauer von TLS-Zertifikaten, siehe 6.3.2
2.11	18.08.2020	▪ Einführung einer EEC Root-CA und zwei ECC Sub-CAs für QCP-n-qscd und QCP-l-qscd
3.0	10.11.2020	▪ Das Root CPS ist ab Version 3.0 der TSPS untergeordnet ▪ Update gemäß observation report
3.1	23.04.2021	▪ Austausch des Links in Abschnitt 1.1.3 ▪ Bekanntmachung des laufenden „CA Root Inclusion" Prozesses in Abschnitt 1.1.3 ▪ Jährliches Review des gesamten CPS ▪ Ergänzungen in den Abschnitten 1.5.3, 2.2, 3.1.4, 3.2.2, 6.1.1, 7.1.3
3.2	03.05.2021	▪ Bekanntmachung der neuen CAs für QES und QSEAL in Abschnitt 1.1.3 ▪ Editorische Änderungen in Abschnitt 7.1.3
3.3	06.07.2021	▪ Bekanntmachung von neuen qualifizierten CAs in Abschnitt 1.1.3 ▪ Bekanntmachung der Einführung eines personalisierten Antragsportals mit dem Namen „D-TRUST Portal" und der Web-Adresse: https://portal.d-trust.net/. Das Go-Live wird noch bekanntgegeben. ▪ Bekanntmachung eines neuen Sperrweges in Abschnitt 4.9.3 in Zusammenhang mit dem einzuführenden „D-TRUST Portal" ▪ Update im Rahmen des BR Self Assessments ▪ Editorische Änderungen und Ergänzungen in den Abschnitten 1.6.1, 2.3, 3.1.1, 3.1.4, 3.1.6, 3.2, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 4.3.1, 4.9.5, 7.1.3, 7.1.6
3.4	19.08.2021	▪ Mitteilung der Inbetriebnahme des D-TRUST-Portals ▪ Ergänzungen in Abschnitt 1.1.3, 1.6.1 und 3.1.4.
3.5	14.10.2021	▪ Ergänzungen in Abschnitt 1.1.3, 3.1.4 und 6.1.1
3.6	14.04.2022	▪ Informative Einführung des Policy Levels NCP ▪ Umbenennung des Policy Levels QCP-w in QEVCP-w und Einführung des Policy Levels QNCP-w ▪ Ergänzungen in Abschnitt 1.1.3 und 6.1.3 ▪ Jährliches Review des gesamten CPS
3.7	22.08.2022	▪ Ergänzungen und Konkretisierungen in Abschnitt 1.1.3, 3.2.3, 4.2.1, 4.5.1 und 6.3.2 ▪ Bekanntmachung des laufenden „CA Root Inclusion" Prozesses in Abschnitt 1.1.3
3.8	17.11.2022	▪ Konkretisierung in Abschnitt 1.1.3 und 4.9.6
3.9	14.02.2023	▪ Bekanntmachung der neuen qualifizierten SubCA „D-TRUST CA 3-21-3 2022" in Abschnitt 1.1.3 ▪ Konkretisierungen in den Abschnitten 1.1.3 und 3.1.4
3.10	25.05.2023	▪ Jährliches Review des gesamten CPS ▪ Ergänzungen und Konkretisierungen in den Abschnitten 1.1.3, 4.4.1 und 6.1.1
4.0	20.10.2023	▪ TLS und S/MIME Produkte werden ab dem 19.07.2023 nicht mehr über die Einzelantragsseiten angeboten. Entfernung der Policy Level: QEVCP-w, QNCP-w, EVCP, OVCP, LCP, NCP und QCP-l mit PSD2. ▪ Review des gesamten CPS

Inhaltsverzeichnis

1. Einleitung

1.1 Überblick

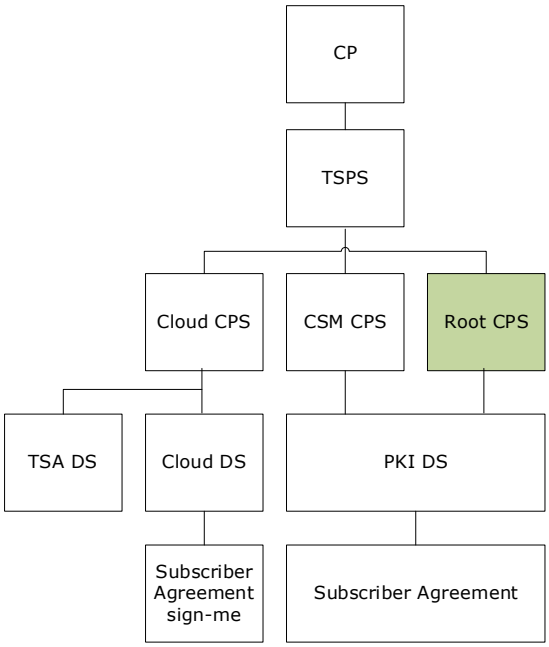
Dieses Dokument ist das Certification Practice Statement (CPS) der von D-Trust GmbH betriebenen Vertrauensdienste, die über die D-TRUST Root PKI bereitgestellt werden. Der Dokumentenname wird mit **Root CPS** abgekürzt verwendet und unterliegt dem Trust Service Practice Statement der D-TRUST (abgekürzt TSPS) und der Zertifikatsrichtlinie (engl. Certificate Policy, im Folgenden CP genannt).

1.1.1 Vertrauensdiensteanbieter

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.



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 TSPS 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 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.

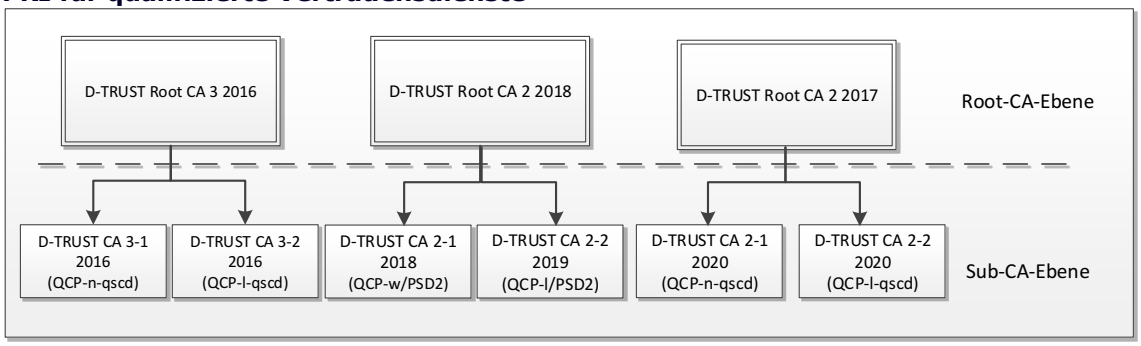
Die Struktur dieses Dokuments folgt dem Internet-Standard RFC 3647 *"Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework"*.

Die weiteren Regelungen sind im TSPS dokumentiert.

1.1.3 Eigenschaften der PKI

Die Hierarchie der hier beschriebenen PKI ist mehrstufig. Abbildung 1, 2 und 3 zeigen schematische Konstellationen der PKI für qualifizierte und nicht-qualifizierte Vertrauensdienste. Sie besteht immer aus einer Kette, die angeführt wird von einer Root-CA (Wurzelinstanz oder Vertrauensanker) und optional gefolgt von weiteren Sub-CAs (Intermediate CAs). Die letzte Sub-CA dieser Kette ist die „ausstellende CA" (Issuing-CA). Von ihr werden EE-Zertifikate ausgestellt.

PKI für qualifizierte Vertrauensdienste



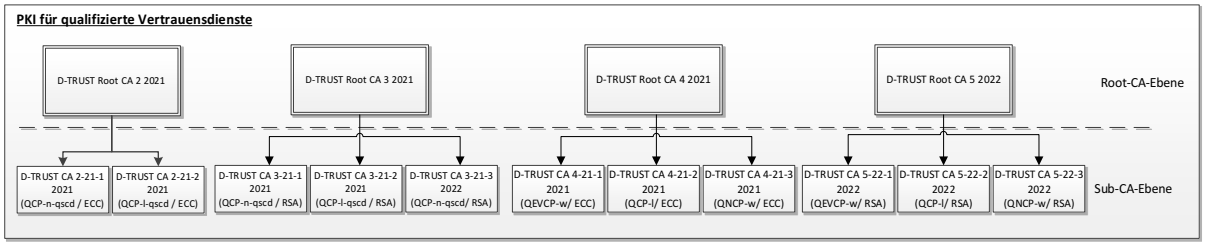


Abbildung 1: Aktuell gültige PKI-Hierarchie für qualifizierte Vertrauensdienste[1]

[1] Die folgenden SubCAs in Abbildung 1 sind in der Trusted List des BNetzA aufgelistet und wurden in Betrieb genommen: D-TRUST CA 2-21-1 2021, D-TRUST CA 2-21-2 2021, D-TRUST CA 3-21-1 2021, D-TRUST CA 3-21-2 2021, D-TRUST CA 3-21-3 2022, D-TRUST CA 4-21-1 2021, D-TRUST CA 4-21-2 2021, D-TRUST CA 4-21-3 2021 und die SubCAs aus der D-TRUST Root CA 5 2022.

Anmerkung: Aus der SubCA „D-TRUST CA 3-21-3 2022" werden zusätzlich zu qualifizierten Zertifikaten für Endanwender zu Signaturzwecken auch fortgeschrittene Zertifikate zu Authentifizierungszwecken erstellt. Diese werden gemeinsam auf einem Trägermedium (QSCD) an den Endanwender übergeben.

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

QCP-n-qscd – Qualifizierte Personenzertifikate auf qualifizierter Signaturerstellungseinheit

QCP-l-qscd – Qualifizierte Siegelzertifikate auf qualifizierter Signaturerstellungseinheit (QSealC)

QCP-l – Qualifizierte Siegelzertifikate ohne qualifizierter Signaturerstellungseinheit (QSealC)

Die Policy Level werden im TSPS erläutert.

PKI für „publicly trusted" Vertrauensdienste[2] (nicht-qualifizierte Vertrauensdienste)

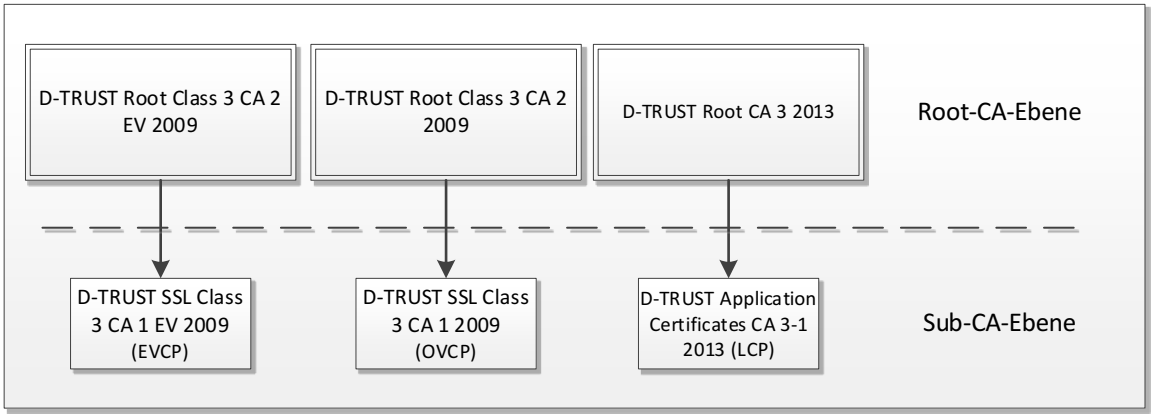


Abbildung 2: Aktuell gültige PKI-Hierarchie für „publicly trusted" Vertrauensdienste

Dieses CPS nimmt Bezug auf die Zertifikate, die über den Einzelantragsweg bestellt werden können. Dieser Antragsweg wird ab dem 19.07.2023 für Produkte mit den Policy Level QEVCP-w, QNCP-w, EVCP, OVCP, LCP, NCP und QCP-l mit PSD2 abgeschaltet. Bereits ausgestellte Zertifikate behalten ihre Gültigkeit, da die PKI weiter betrieben wird. Alle Zertifikate, unabhängig vom Antragsweg, können weiterhin beauskunftet werden. Die Zertifikate mit den o.g. Policy Level werden zukünftig ausschließlich über den Certificate Service Manager (CSM) angeboten und sind im CSM CPS (https://www.d-trust.net/internet/files/D-TRUST_CSM_PKI_CPS.pdf) beschrieben.

CA-Zertifikate

Die Gesamtübersicht aller RootCAs und SubCAs mit den Policy Leveln QEVCP-w, QNCP-w, EVCP, OVCP, NCP und LCP aus der hervorgeht welches Vorgabedokument auf die jeweilige CA Anwendung findet, ist im Repository zu finden:

https://www.d-trust.net/files/dokumente/pdf/pki_structure_and_applicable_documents.pdf

Die folgende Tabelle liefert eine Übersicht über alle RootCAs und der dazugehörigen SubCAs, für die dieses CPS Anwendung findet.[3]

Die „D-TRUST Root CA 2 2021" ersetzt die „D-TRUST Root CA 2 2017" und die „D-TRUST Root CA 3 2021" ersetzt die „D-TRUST Root CA 3 2016". Die „D-TRUST Root CA 4 2021" ersetzt die „D-TRUST Root CA 2 2018".

Aus den SubCAs der „D-TRUST Root CA 2 2018" werden ab dem 14.01.2021 keine neuen Zertifikate mehr erstellt.

[2] „publicly trusted" Vertrauensdienste sind Vertrauensdienste gemäß den Vorgaben der Certificate Consumer Mitglieder des CA Browser/Forums in Kombination mit den Vorgaben des CA Browser/Forums.

[3] Zertifikate aus den ausgegrauten CAs werden über die Antragswege, welche in dieser Root CPS beschrieben sind, nicht mehr angeboten. Bereits ausgestellte Zertifikate behalten ihre Gültigkeit, da die PKI weiter betrieben wird. Alle

D-TRUST Root CA 3 2016 https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_3_2016.crt Fingerprint: SHA1: 16ABFE955BBA80F0D7079D240188C633DF5DDB7F SHA256: 828F0AA17DC578DB836FBCAFB60BEFEBAC1551080AEB60D1264DDBB1561230EA
D-TRUST CA 3-1 2016 https://www.d-trust.net/cgi-bin/D-TRUST_CA_3-1_2016.crt Policy Level: QCP-n-qscd Fingerprint: SHA1: 38A577328FAD50472F94D47AB433D88F8F36A22D SHA256: 454A164B9236CF9C380DF9959F751DED503F91BE3EC646C7042CBB0E1E17A7D5 OID: 1.3.6.1.4.1.4788.2.150.1
D-TRUST CA 3-2 2016 https://www.d-trust.net/cgi-bin/D-TRUST_CA_3-2_2016.crt Policy Level: QCP-l-qscd Fingerprint: SHA1: 7927b0fda41b2a2465aa4e727d8bac8dd0db5aad SHA256: 44AD63979AF0794DB890B96A9BE63A17F5ADF7AC47FE91B008FF04E3EEB9FCCD OID: 1.3.6.1.4.1.4788.2.150.2
D-TRUST Root CA 2 2018 (Legacy) https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_2_2018.crt Fingerprint: SHA1: 4B467FB8D2051D7BC4CDB73377FA7077034BCCE1 SHA256: 113BBD9EFFFA4C743D6D09038DC0AAB1A5F1FAD7492868193917C63D82D74FA1
D-TRUST CA 2-1 2018 (Legacy) https://www.d-trust.net/cgi-bin/D-TRUST_CA_2-1_2018.crt Policy Level: QEVCP-w Fingerprint: SHA1: 5982BDD5E228E4869461713710CC5C3DDE006C43 SHA256: 5F28B888456D21158C5E3E8A31719CF3B305300BC5B436B696BE22F6973F1DF1 OID: 1.3.6.1.4.1.4788.2.150.4

Zertifikate, unabhängig vom Antragsweg, können weiterhin beauskunftet werden. Die CAs werden voraussichtlich Ende 2025 in dieser CPS gelöscht.

D-TRUST CA 2-2 2019 (Legacy) https://www.d-trust.net/cgi-bin/D-TRUST_CA_2-2_2019.crt Policy Level: QCP-l Fingerprint: SHA1: 455FD6F160938C1FCCE1EF8D4F33700F2148FF87 SHA256: E85F41CE30CF9910CB8D12470F9E312E8F862FFED0581F5995772D8B46CB7E99 OID: 1.3.6.1.4.1.4788.2.150.5
D-TRUST Root CA 2 2017 https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_2_2017.crt Fingerprint: SHA1: 357BB8CC3855B401F7C64CFF35689F83C860374D SHA256: E152527EB90B3034818589D31C3CC4EE1C896446AC4E29EA8F546B3419165B90
D-TRUST CA 2-1 2020 https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_2-1_2020.crt Policy Level: QCP-n-qscd Fingerprint: SHA1: D00C842434F42BD4903518CA3B0E9EC49976EE2F SHA256: A5D944F0C6598C8A3A421AB320DD6E82E1C7A373B4812FFB2508F638804082AB OID: 1.3.6.1.4.1.4788.2.150.1
D-TRUST CA 2-2 2020 https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_2-2_2020.crt Policy Level: QCP-l-qscd Fingerprint: SHA1: ECE3B420B2FE38F56E036A8D507FFDA229024CE3 SHA256: C0671426DE62A9BAA23C28EF9EFF21B5C3DDF0673BEE59EA43B0CE0C6E30FE85 OID: 1.3.6.1.4.1.4788.2.150.2
D-TRUST Root Class 3 CA 2 EV 2009 https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_EV_2009.crt Fingerprint: SHA1: 96C91B0B95B4109842FAD0D82279FE60FAB91683 SHA256: EEC5496B988CE98625B934092EEC2908BED0B0F316C2D4730C84EAF1F3D34881
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: B0935DC04B4E60C0C42DEF7EC57A1B1D8F958D17988E71CC80A8CF5E635BA5B4 OID: 1.3.6.1.4.1.4788.2.202.1

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: 58E8ABB0361533FB80F79B1B6D29D3FF8D5F00F0 SHA256: 49E7A442ACF0EA6287050054B52564B650E4F49E42E348D6AA38E039E957B1C1
D-TRUST SSL Class 3 CA 1 2009 https://www.d-trust.net/cgi-bin/D-TRUST_SSL_Class_3_CA_1_2009.crt Policy Level: OVCP Fingerprint: SHA1: 2FC5DE6528CDBE50A14C382FC1DE524FAABF95FC SHA256: 6AC159B4C2BC8E729F3B84642EF1286BCC80D775FE278C740ADA468D59439025 OID: 1.3.6.1.4.1.4788.2.200.1
D-TRUST Root CA 3 2013 https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_3_2013.crt Fingerprint: SHA1: 6C7CCCE7D4AE515F9908CD3FF6E8C378DF6FeF97 SHA256: A1A86D04121EB87F027C66F53303C28E5739F943FC84B38AD6AF009035DD9457
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 (1.3.6.1.4.1.4788.2.200.2), NCP (1.3.6.1.4.1.4788.2.200.3) Fingerprint: SHA1: 1785B07501F0FCEFFC97C6B070C255A8A9B99F12 SHA256: CB0F7B7670EA2B818ABE80587902434B30EF7A8C0273B84884243F89593EA630 OID im CA-Zertifikat: 1.3.6.1.4.1.4788.2.200.1 (Legacy)
D-TRUST Root CA 2 2021 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_2_2021.crt Fingerprint: SHA1: 468C467671DD4F1A38145104C353C99276107702 SHA256: E7A79A64F101897903D5B054564672E5D5C803437405D15321A1A5763710AF70
D-TRUST CA 2-21-1 2021 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-TRUST_CA_2-21-1_2021.crt Policy Level: QCP-n-qscd Fingerprint: SHA1: F78B7AA28BACD8E004C1A7FEEE7BD035BC1B5AD7 SHA256: 620BA94502329A506F3A2AFB6500DA9FA437C946E8D6E4B7C2148C29C8E76A8E OID: 1.3.6.1.4.1.4788.2.150.1

D-TRUST CA 2-21-2 2021 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-TRUST_CA_2-21-2_2021.crt Policy Level: QCP-l-qscd Fingerprint: SHA1: BC0FA0A53582E8E5434F0AEACCEE32A2C3CD9443 SHA256: B3472A9A9DB78EBBC260EA628BD44B593C3D7B1367F25DFAD659FF5E9198B0DF OID: 1.3.6.1.4.1.4788.2.150.2
D-TRUST Root CA 3 2021 (RSA, 4096 Bit) https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_3_2021.crt Fingerprint: SHA1: E4F95E877D3D6519336040A2B0C853F8A1B57194 SHA256: 390F7FE59E7AEE6D271527CFA0D53B2E67B3F7FABECEDB65FB10AAFF34F13FF2
D-TRUST CA 3-21-1 2021 (RSA, 4096 Bit) https://www.d-trust.net/cgi-bin/D-TRUST_CA_3-21-1_2021.crt Policy Level: QCP-n-qscd Fingerprint: SHA1: 9F729EFAF98688C7F946ED8012A8773088B037C1 SHA256: C67EBB0BFA6497ACFBD5423ED5A2DA5497E82092A4C475200DCC273CC8CFC69C OID: 1.3.6.1.4.1.4788.2.150.1
D-TRUST CA 3-21-2 2021 (RSA, 4096 Bit) https://www.d-trust.net/cgi-bin/D-TRUST_CA_3-21-2_2021.crt Policy Level: QCP-l-qscd Fingerprint: SHA1: 767E3E3FDE06FE00199205F36B4EA7723562133C SHA256: E628B19986782CEB2094DB982E749ADCD7CA02C58DB0C7B8B2ECE7869A07897A OID: 1.3.6.1.4.1.4788.2.150.2
D-TRUST CA 3-21-3 2022 (RSA, 4096 Bit)[4] https://www.d-trust.net/cgi-bin/D-TRUST_CA_3-21-3_2022.crt Policy Level: QCP-n-qscd Fingerprint: SHA1: 5601F434AB54C3EADDBEBA430ABD9B40065E2341 SHA256: 0DF80683B392814EF75A12F665A810D36D0754FB297F24C65729C7A771022A5B OID: 1.3.6.1.4.1.4788.2.150.1

[4] Anmerkung: Aus der SubCA „D-TRUST CA 3-21-3 2022" werden zusätzlich zu qualifizierten Zertifikaten für Endanwender zu Signaturzwecken auch fortgeschrittene Zertifikate zu Authentifizierungszwecken erstellt. Diese werden gemeinsam auf einem Trägermedium (QSCD) an den Endanwender übergeben.

D-TRUST Root CA 4 2021 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_4_2021.crt Fingerprint: SHA1: A48CDA4E279A7E8996BF2D1EF1263DD16068092A SHA256: 70A9EF005779FCEE0619A644AF439FD3AF3379E645530F35BD6AE68EFF19D2BF
D-TRUST CA 4-21-1 2021 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-TRUST_CA_4-21-1_2021.crt Policy Level: QEVCP-w Fingerprint: SHA1: 74B857941F0EB9BC0FB9A3FEA83AEA836E0A5E22 SHA256: 4EA66AB8FC54D446F6A46A63F0FCA5FE83A1F433CDE771DE8D1A8BE06647D008 OID: 1.3.6.1.4.1.4788.2.150.4
D-TRUST CA 4-21-2 2021 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-TRUST_CA_4-21-2_2021.crt Policy Level: QCP-l Fingerprint: SHA1: 07BBB6424795283CC3757E91642AF95055DB85D4 SHA256: 5EF6EB4690E15C57C25A0296A9A93488B86AA5878A3DFC0859855CC5EB378A00 OID: 1.3.6.1.4.1.4788.2.150.5
D-TRUST CA 4-21-3 2021 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-TRUST_CA_4-21-3_2021.crt Policy Level: QNCP-w Fingerprint: SHA1: EF175B7CC271EFEC0406EDB610C909DF88FA8202 SHA256: 884864ACDB55E55BF1E5CF648EF434491E2F6990FF4A952E3FA4763A1A6C33BB OID: 1.3.6.1.4.1.4788.2.150.3
D-TRUST Root CA 5 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_5_2022.crt Fingerprint: SHA1: 643211332169B483B55F7046E56CBFC6C11DC5F8 SHA256: D839672F984DCA7CD480CE201627A4DE61C5C1855F450E5B706200E73A23F047
D-TRUST CA 5-22-1 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-TRUST_CA_5-22-1_2022.crt Policy Level: QEVCP-w Fingerprint: SHA1: 5B26CCEEC541B3886A76761A9503667027C8B94A SHA256: A028FB2822D0C2699A451B7083A984318F7A0102A3B42F5B089D99CF3F9149C3 OID: 1.3.6.1.4.1.4788.2.150.4

D-TRUST CA 5-22-2 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-TRUST_CA_5-22-2_2022.crt Policy Level: QCP-l Fingerprint: SHA1: 34156C420F146160795B5E2CC4EF343C258C16BF SHA256: F0A1CA5FC42E6A8514C63415054F14EF7BB961ADBC7A94185D8E410A905B8109 OID: 1.3.6.1.4.1.4788.2.150.5
D-TRUST CA 5-22-3 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-TRUST_CA_5-22-3_2022.crt Policy Level: QNCP-w Fingerprint: SHA1: 8A259DBB8B8C3AB5971B94590C7BABAFE57B5E1F SHA256: D9B38F7314AAB95DE57B63784F7D123D031C4FED6D8F66ED55A91BD05FEA818B OID: 1.3.6.1.4.1.4788.2.150.3

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 Root PKI
Version	4.0

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

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

Zertifikate, bzw. deren Sub- sowie Root-CAs kommen den Anforderungen aus [EN 319 411-1], [EN 319 411-2] und [eIDAS] nach. Im Falle von Inkonsistenzen zwischen diesem Dokument und den genannten Richtlinien, gelten vorrangig [eIDAS] und [EN 319 411-2].

1.6 Begriffe und Abkürzungen

1.6.1 Begriffe und Namen

D-TRUST Portal (https://portal.d-trust.net/)	Das neue Antragsportal mit dem Namen „D-Trust Portal" und der Web-Adresse „https://portal.d-trust.net/" hat zu den bisherigen Antragsseiten der D-Trust die Besonderheit , dass der Kunde bzw. der Antragsteller sich registriert und damit einen personalisierten Zugang bzw. Konto erhält. Über dieses Konto kann der Kunde bzw. der Antragsteller die persönlichen bzw. die im Auftrag einer juristischen Person beantragten qualifizierten Signatur- bzw. Siegelkarten verwalten (beantragen, sperren).

Weitere Regelungen sind in der CP dokumentiert.

1.6.2 Abkürzungen

CP (Certificate Policy)	Zertifikatsrichtlinie

Weitere 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-l-qscd, QCP-l

Der Status der Zertifikate kann mittels OCSP-Abfrage dauerhaft abgerufen werden.

Weitere Regelungen sind in der CP dokumentiert.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Der TSP veröffentlicht folgende Informationen:

- EE-Zertifikate,
- Zertifikatsstatus von TLS Test-Webseiten
- das TSPS,
- dieses CPS,
- die Verpflichtungserklärung,
- die PKI-Nutzerinformation für qualifizierte Vertrauensdienste.

Die weiteren Regelungen sind im TSPS dokumentiert.

2.3 Häufigkeit von Veröffentlichungen

QCP-l-qscd, QCP-l
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.

QCP-n-qscd
EE-Zertifikate können veröffentlicht, d.h. in das öffentliche Verzeichnis des TSP aufgenommen werden. Der Zertifikatsnehmer kann der Veröffentlichung zustimmen oder diese ablehnen. Veröffentlichte EE-Zertifikate bleiben bis zum Ende ihrer Gültigkeit sowie mindestens für zehn Jahre und bis zum Jahresende abrufbar.

Die Veröffentlichung findet sofort nach Ausstellung eines Zertifikats statt, sofern die Veröffentlichung nicht abgelehnt wurde.

CA-Zertifikate werden nach ihrer Erstellung veröffentlicht und:

- mindestens 10 Jahre (QCP-n-qscd, QCP-l-qscd, QCP-l) und bis zum Jahresende

nach Ablauf der Gültigkeit der CA vorgehalten.

Sperrlisten werden regelmäßig und bis zum Ende der Gültigkeit des ausstellenden CA-Zertifikats ausgestellt. Sperrlisten werden unmittelbar nach dem Widerruf von Zertifikaten erstellt und veröffentlicht. Auch wenn kein Widerruf von Zertifikaten erfolgt, stellt der TSP sicher, dass alle 12 Stunden eine neue Sperrliste ausgestellt wird. Die Sperrlisten werden mindestens ein Jahr 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. Wird ein CA-Zertifikat widerrufen, wird die CA-Sperrliste innerhalb von 24 Stunden veröffentlicht.

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

CA- und EE-Zertifikate enthalten grundsätzlich Angaben zu Aussteller (issuer) und Zertifikatsnehmer bzw. Endanwender (subject). Diese Namen werden entsprechend dem Standard [X.500] bzw. [X.509] als *distinguished names* vergeben.

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

3.1.2 Notwendigkeit für aussagefähige Namen

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

Eine eindeutige Zuordnung des Zertifikats zum Zertifikatsnehmer (bei Zertifikaten für natürliche Personen auch zu dem Endanwender 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.

Die Freiwählbarkeit von Pseudonymen kann vereinbart werden, siehe Abschnitt 3.1.6. Der TSP behält sich vor, die Vergabe eines Pseudonyms abzulehnen. Die Ablehnung bedarf keiner Begründung.

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

3.1.4 Regeln für die Interpretation verschiedener Namensformen

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

DN-Bestandteil	Interpretation
G (givenName)	*Vorname(n)* der natürlichen Person - QCP-l, QCP-l-qscd: Feld wird nicht verwendet - QCP-n-qscd: gemäß dem zur Identifizierung verwendeten Nachweis
SN (surname)	*Familienname* der natürlichen Person - QCP-l-qscd: Feld wird nicht verwendet - QCP-n-qscd: gemäß dem zur Identifizierung verwendeten Nachweis Bei der Verwendung von Pseudonymen entspricht der SN dem CN.

DN-Bestandteil	Interpretation
CN (commonName) (2.5.4.3)	*Gebräuchlicher Name:* Folgende Varianten werden verwendet: - Natürlichen Personen ohne Pseudonym: „Vorname(n) Nachname". - Natürliche Personen mit Pseudonym: „Pseudonym:PN". - Juristischen Personen: offizielle Bezeichnung der Organisation (Firma, Behörde, Verein etc.), ggf. sinnvolle Abkürzung bei Überschreiten der Zeichenbegrenzung von 64 Zeichen. - Funktion oder Personengruppe: Name der Funktion oder Personengruppe mit der vorangestellten Abkürzung „GRP:" als Hinweis, dass es sich um ein Gruppenzertifikat handelt - Technische Komponenten: Name des Servers, des Dienstes oder der Applikation, der/die das Zertifikat benutzt.
SAN (subjectAltName)	Folgende Varianten werden verwendet: - E-Mail-Adresse des Zertifikatsnehmers - Technische Komponenten: Name des Servers, des Dienstes oder der Applikation, der/die das Zertifikat benutzt.
PN (pseudonym)	*Pseudonym*: ist identisch zu CN.
Serial Number (serialNumber) (2.5.4.5)	*Seriennummer*: Namenszusatznummer, welche die Eindeutigkeit des Namens sicherstellt (i.d.R. die Antragsnummer). Produktspezifisch kann das Feld anderweitig verwendet werden.
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.
OU (organizationalUnitName) (2.5.4.11)	Organisationseinheit der Organisation, wie z.B. Abteilung, Bereich oder andere Unterteilung
OrgID (organizationIdentifier) (2.5.4.97)	**QCP-l-qscd**: *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).

DN-Bestandteil	Interpretation
C (countryName) (2.5.4.6)	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 Zertifikatsnehmer identifiziert wurde.
Street (streetAddress) (2.5.4.9)	Postalische Adresse Straße und Hausnummer
Locality (localityName) (2.5.4.7)	Postalische Adresse *Ort*
State (stateOrProvinceName) (2.5.4.8)	Postalische Adresse *(Bundes-)Land*
PostalCode (postalCode) (2.5.4.17)	Postalische Adresse *Postleitzahl*

Weitere Regelungen sind in der TSPS in Abschnitt 7.1.4 dokumentiert.

QCP-n-qscd
Qualifizierte Zertifikate für natürliche Personen enthalten mindestens die subject-DN-Bestandteile „commonName", „countryName", „serialNumber" sowie entweder „GivenName" und „Surname" oder „Pseudonym".

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

Es müssen nicht alle genannten DN-Bestandteile verwendet werden. Weitere können ergänzt werden. Ergänzende DN-Bestandteile müssen [RFC 5280], [RFC 6818] und ETSI [ETSI EN 319 412] entsprechen.

3.1.5 Eindeutigkeit von Namen

Der TSP stellt sicher, dass ein in EE-Zertifikaten verwendeter Name (DistinguishedName) des Zertifikatsnehmers bzw. des Endanwenders (Feld subject) innerhalb dieser PKI stets dem gleichen Zertifikatsnehmer bzw. Endanwender zugeordnet ist.

Die Eindeutigkeit des Zertifikats wird mittels der Seriennummer erzielt.

Der TSP stellt die Eindeutigkeit von *distinguished names* in CA-Zertifikaten sicher.

3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen

Der Zertifikatsnehmer haftet für die Einhaltung geistiger Eigentumsrechte in den Antrags- und Zertifikatsdaten (siehe Zertifikatsrichtlinie der D-Trust GmbH, Abschnitt 9.5).

3.2 Initiale Überprüfung der Identität

Es ist ein Verfahren etabliert, das sicherstellt, dass die Datenquellen zur Validierung von Zertifikatsinhalten geprüft und freigegeben werden. Alle Datenquellen sind von der D-Trust Organisationseinheit für Informationssicherheit freigegeben.

3.2.1 Nachweis für den Besitz des privaten Schlüssels

Schlüsselpaare von Zertifikatsnehmern werden im Verantwortungsbereich des TSP produziert. Mit der Übergabe der Signatur- bzw. Siegelkarte (QCP-n-qscd, QCP-l-qscd) und ggf. PIN-Briefe gemäß Abschnitt 4.4.1 an die Zertifikatsnehmer durch den TSP wird sichergestellt, dass die privaten Schlüssel in den Besitz der Zertifikatsnehmer gelangen.

3.2.2 Identifizierung und Authentifizierung von Organisationen

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

Für die Teilnehmeridentifizierung und die Antragsprüfung gelten die Vorgaben aus [EN 319 411-1] und [EN 319 411-2] für QCP-l oder QCP-l-qscd. Die Prüfung erfasst alle DN-Bestandteile.

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.

	QCP-l, QCP-l-qscd
CN	Register/ Non-Register
C	
O	
OrgID	Register
OU	Z-Bestätigung/ A-Bestätigung/ Register
STREET	Register/ Non-Register
L	
State	
PostalCode	

Wird der Antrag im Auftrag einer juristischen Person gestellt, muss der Vertreter (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-l, QCP-l-qscd.

Relevante Informationen zum Zertifikat, die den Registerauszügen entnommen sind, werden genauso in die Zertifikatinhalte geschrieben, wie sie im Registerauszug veröffentlicht sind.

Nachweise in nicht lateinischer Schrift werden nicht akzeptiert.

3.2.3 Identifizierung und Authentifizierung natürlicher Personen

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

	QCP-n-qscd
G	Pers-Ident/ eID/ NotarIdent/ BotschaftsIdent
SN	
CN	Pers-Ident/ eID/ NotarIdent/ BotschaftsIdent
C	
O	Register/ Non-Register/ Z-Bestätigung/ A-Bestätigung
OU	Z-Bestätigung/ A-Bestätigung
Alternativer Antragsteller (SAN)	E-Mail
Alle weiteren Attribute	A-Bestätigung/ Out-of-band mechanisms

Nachweise in nicht lateinischer Schrift werden nicht akzeptiert.

3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Die Angaben des Zertifikatsnehmers 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 Alternative Namen wie z.B. LDAP-Verzeichnisse etc. sowie eventuelle Zertifikats-Extensions (AdditionalInformation, monetaryLimit, etc.) werden nicht auf Korrektheit geprüft.

3.2.5 Prüfung der Berechtigung zur Antragstellung

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

Bei Organisationen wird der Existenznachweis sowie die Vertretungsberechtigung des Antragstellers nach Abschnitt 3.2.2 geprüft bzw. bestätigt. Weiterhin wird mindestens ein technischer Vertreter 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)

Eine Schlüsselerneuerung ist gleichbedeutend mit der erneuten Produktion von Zertifikaten ggf. Token und Schlüsseln für denselben Endanwender, dennoch kann auf bereits geprüfte und noch verwertbare Daten und Nachweise des Endanwenders zurückgegriffen werden.

Abweichende Verfahren können kundenindividuell vereinbart werden, deren Umsetzung im Ermessen des TSP liegen, wenn sie keiner Zertifizierung nach [EN 319 411-1] oder [EN 319 411-2] unterliegen. Die Bedingungen des Abschnitts 4.7 müssen erfüllt werden.

Schlüsselerneuerung auf Basis eines widerrufenen Zertifikats wird nicht angeboten.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Sperrberechtigung wird wie folgt geprüft:

- Subscriber mit einem Benutzerkonto im D-Trust Portal können sich dort mittels Nutzername und Passwort authentifizieren und ihre Zertifikate direkt im Konto (https://portal.d-trust.net/) sperren.
- Elektronische Sperranträge über eine Online-Schnittstelle können mittels eines, über einen sicheren und vorher vereinbarten Kanal übertragenen Geheimnisses autorisiert werden (z.B. SMS-TAN, Sperrpasswort).
- Schriftliche Sperranträge vom Subscriber bzw. vom Sperrberechtigten Dritten werden anhand der Unterschrift des Sperrantragstellers überprüft.

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

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 (deren autorisierten Vertretern) gestellt werden.

Die allgemeinen Regelungen sind im TSPS dokumentiert.

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

4.1.2 Registrierungsprozess und Zuständigkeiten

Die allgemeinen Regelungen sind im TSPS dokumentiert.

In diesem CPS finden die in Abschnitt 1.1.3 genannten Policy Level QCP-n-qscd, QCP-l-qscd und QCP-l Anwendung. Der Registrierungsprozess und die Zuständigkeiten für die jeweiligen Policy Level werden in der TSPS beschrieben.

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Im Rahmen des Root 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
eID
NotarIdent
BotschaftsIdent
Register
Non-Register
Z-Bestätigung
A-Bestätigung
out-of-band-Mechanismen
E-Mail-Adresse

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

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Diese Regelungen sind im TSPS dokumentiert.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

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 Root CPS folgende spezifische Regelungen:

QSCD
Bei der Erstellung von QSCDs werden vom TSP alle Ereignisse auditierbar geloggt bzw. protokolliert.

4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausstellung des Zertifikats

Diese Regelungen sind im TSPS dokumentiert.

4.4 Zertifikatsübergabe

4.4.1 Verhalten bei der Zertifikatsübergabe

Chipkarten werden entweder an die angegebene Adresse per Briefdienstleister oder Kurier versendet oder persönlich durch die RA oder einen autorisierten Mitarbeiter oder Funktionsträger an den Zertifikatsnehmer oder auf dessen Wunsch an den Endanwender ausgehändigt.

QCP-l
Wird ein Zertifikat zu einem beim Zertifikatsnehmer vorhandenen Schlüsselpaar ausgestellt, wird das Zertifikat entweder zum Download bereitgestellt (z. B. im Verzeichnisdienst veröffentlicht) oder elektronisch versendet.

QCP-n-qscd, QCP-l-qscd
Der TSP verwendet ausschließlich qualifizierte Signatur-/Siegelerstellungseinheiten und überwacht während der Gültigkeit der ausgegebenen qualifizierten Zertifikate den Status dieser qualifizierten Signatur-/Siegelerstellungseinheiten im Sinne EN 319 411-2. Die PIN wird separat an den Endanwender übergeben.

Kundenspezifisch können abweichende Verfahren vereinbart werden.

Die allgemeinen Regelungen sind im TSPS dokumentiert.

4.4.2 Veröffentlichung des Zertifikats durch den TSP

Hat der Zertifikatsnehmer im Zertifikatsantrag der Veröffentlichung der Zertifikate zugestimmt, werden die Zertifikate nach der Produktion in den öffentlichen Verzeichnisdienst eingestellt. Hat der Zertifikatsnehmer die Veröffentlichung abgelehnt, wird das Zertifikat nicht veröffentlicht.

4.4.3 Benachrichtigung anderer PKI-Teilnehmer 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 sperrberechtigten Dritten vereinbart wurde.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

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

QCP-n-qscd, QCP-l-qscd, QCP-l
Nach Ablauf des Gültigkeitszeitraums oder nach dem Widerruf des Zertifikats dürfen die zugehörigen privaten Schlüssel nicht mehr genutzt werden.

Für Zertifikatsnehmer gelten die Bestimmungen aus Abschnitt 1.4.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

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 Zertifikatsnehmer darüber informiert. Der Zertifikatsnehmer bestätigt die neuen Bedingungen.

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

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

4.7.2 Berechtigung zur Zertifikatserneuerung

Jeder Zertifikatsnehmer, der (nach Abschnitt 4.1.1) berechtigt ist, einen Zertifikatsantrag zu stellen, kann eine Zertifikatserneuerung beantragen, wenn der TSP ein entsprechendes Verfahren für das gewählte Produkt anbietet.

4.7.3 Bearbeitung eines Antrags auf Zertifikatserneuerung

Es gelten die in Abschnitt 4.3 festgelegten Regelungen.

4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Es gelten die in Abschnitt 4.3.2 festgelegten Regelungen.

4.7.5 Verhalten bei der Ausgabe einer Zertifikatserneuerung

Es gelten die in Abschnitt 4.4.1 festgelegten Regelungen.

4.7.6 Veröffentlichung der Zertifikatserneuerung durch den TSP

Es gelten die in Abschnitt 4.4.2 festgelegten Regelungen, je nach Angaben im Erstantrag.

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 3.4 authentifizieren.

4.9.2 Berechtigung zum Widerruf

Diese Regelungen sind im TSPS dokumentiert.

4.9.3 Verfahren für einen Sperrantrag

Soweit ein Sperrpasswort vereinbart wurde, können Sperranträge per E-Mail, telefonisch oder via Online-Schnittstelle gestellt werden.

Über die Online-Schnittstelle können Zertifikate grundsätzlich 24x7 widerrufen werden. Sowohl Zertifikatsnehmer als auch Sperrberechtigte können über die Online-Schnittstelle sperren und müssen sich dafür mit ihrem vereinbarten Sperrpasswort authentifizieren.

Online-Schnittstelle: https://my.d-trust.net/sperren

Der Zertifikatsnehmer bzw. der Sperrberechtigte können im Bedarfsfall telefonische Unterstützung beim Widerrufen eines Zertifikats einholen. Dafür übergibt der Sperrantragsteller (Zertifikatsnehmer bzw. Sperrberechtigte) dem Support Mitarbeiter die Antrags-ID und das zugehörige Sperrpasswort, damit der Support Mitarbeiter für den Sperrantragsteller die Eingabe über die Online-Schnittstelle tätigt.

Telefonischer Support: +49 (0)30 / 25 98 – 0

Kunden, die im D-Trust Portal (https://portal.d-trust.net/) registriert sind und darüber qualifizierte Signatur-bzw. Siegelkarten bestellen:

Wenn qualifizierte Signatur- bzw. Siegelkarten über ein persönliches Konto im D-Trust Portal bestellt wurden, muss die Sperrung auch dort durchgeführt werden. Der sperrberechtigte der Organisation muss die Sperrung weiterhin über die folgende Adresse vornehmen: https://my.d-trust.net/sperren.

Mit der Sperrung der Karte werden alle dazugehörigen Zertifikate widerrufen. Ein Widerruf kann grundsätzlich nicht rückgängig gemacht werden.

Für die Sperrung eines Zertifikats via E-Mail teilt der Zertifikatsnehmer bzw. der Sperrberechtigte die Antrags-ID des Zertifikats und das zugehörige Sperrpasswort mit. Per E-Mail eintreffende Sperranträge werden spätestens am folgenden Arbeitstag bearbeitet.

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

Ein Sperrantrag kann auch per Briefpost eingereicht werden.

Anschrift für Sperranträge: D-Trust GmbH
Kommandantenstr. 15
10969 Berlin

Ein schriftlicher Antrag zum Widerruf muss eindeutig das zu widerrufende Zertifikat beschreiben und daher folgende Angaben enthalten:

- Name des Sperrantragstellers,
- Name des Zertifikatsnehmers,
- Zertifikatsseriennummer, damit das Zertifikat eindeutig identifiziert werden kann.

Der Antragsteller muss in Kenntnis seines Sperrpasswortes sein, da im Anschluss eine telefonische Verifikation über das Sperrpasswort durchgeführt wird.

Einen Terminwunsch für einen Widerruf in der Zukunft, sofern der Termin im Rahmen der Zertifikatslaufzeit ist, kann nur im Rahmen des schriftlichen Sperrantrags angenommen werden, wenn ein schriftlicher Sperrantrag durch das Vorliegen einer Unterschriftsprobe möglich ist. Ein Widerruf per Telefon bzw. über die Online-Schnittstelle wird sofort wirksam.

Statusänderungen im OCSP sind unverzüglich nach einem Widerruf zur Abfrage verfügbar. Statusänderungen in einer CRL beinhalten dieselben Sperrinformationen, aber es kann bis 60 Minuten dauern bis die aktuelle CRL veröffentlicht wird.

Andere Sperrverfahren können vereinbart werden.

Der Widerruf eines Zertifikats wird in der Verantwortung des TSP durchgeführt. Ungeachtet dessen kann der TSP Teilaufgaben an vertraglich gebundene Dritte weitergeben. Die Sperrdienstleistung kann von Dritten übernommen werden, die nach den Maßgaben des TSP handeln.

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

Die vom Sperrantragsteller angegebenen Sperrgründe werden dokumentiert. Nach erfolgtem Widerruf des Zertifikats wird der Zertifikatsnehmer bzw. der Endanwender über den Widerruf informiert.

Die Authentifizierung der Sperrberechtigten erfolgt gemäß Abschnitt 3.4.

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 telefonisch oder über die Online-Schnittstelle eingereicht werden. Der Widerruf erfolgt gemäß Abschnitt 4.9 [BRG].

Schriftlich eintreffende Sperranträge werden spätestens am folgenden Arbeitstag bearbeitet.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Aktuelle Sperrinformationen sind in Sperrlisten vorgehalten, die über das Protokoll LDAP[5] oder über den in Abschnitt 2.1 angegebenen Link abgerufen werden können. Zusätzlich steht ein OCSP-Dienst zur Verfügung. Die Erreichbarkeit dieser Dienste wird in Form von URLs in den Zertifikaten angegeben. Ferner können Sperrinformationen über die Webseite des TSP (siehe Abschnitt 2.1) bezogen werden. Delta-CRLs werden nicht genutzt.

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

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

Statusänderungen im OCSP sind unverzüglich nach einem Widerruf zur Abfrage verfügbar. Statusänderungen in einer CRL beinhalten dieselben Sperrinformationen. Die Distribution einer neuen CRL erfolgt jedoch zeitversetzt zum Widerruf.

QCP-n-qscd, QCP-l-qscd, QCP-l
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 eines URL in den Zertifikaten angegeben.

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.

[5] Zukünftig werden Sperrlisten nur noch über einen http-Link angeboten.

4.10 Statusabfragedienst für Zertifikate

4.10.1 Funktionsweise des Statusabfragedienstes

Diese Regelungen sind im TSPS dokumentiert.

4.10.2 Verfügbarkeit des Statusabfragedienstes

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

Das Hinterlegen privater EE-Schlüssel kann beantragt werden.

Schlüsselhinterlegung wird für qualifizierte Zertifikate gemäß [EN 319 411-1] und [EN 319 411-2] 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 Beschreibungen dieses Kapitels beziehen sich auf die CAs, die bei der D-Trust GmbH im Rahmen von [EN 319 411-1] und [EN 319 411-2] betrieben werden

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

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 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.

QCP-l

Der Zertifikatsnehmer ist bei der Erzeugung von EE-Schlüsseln verpflichtet, diese entsprechend der Vorgaben aus [EN 319 411-1] und [EN 319 411-2] kryptografisch sicher zu erzeugen.

QCP-l-qscd, QCP-n-qscd

Werden EE-Schlüssel vom TSP erzeugt, werden diese mit Hilfe eines HSMs oder auf einer qualifizierten Signatur-/Siegelerstellungseinheit in der sicheren Umgebung des Trustcenters erzeugt und entsprechen den Vorgaben aus [EN 319 411-2].

Werden EE-Schlüssel und EE-Zertifikate auf Chipkarten oder anderen hardwarebasierten Token erzeugt oder aufgebracht, verfährt der TSP bei der Beschaffung, Lagerung, Personalisierung und beim PIN-Handling gemäß den entsprechend anwendbaren Vorgaben des Herstellers oder des Zertifizierers der Chipkarte bzw. des Tokens.

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

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 Zertifikatsnehmer beim TSP gelöscht.

6.1.3 Lieferung öffentlicher Schlüssel an den TSP

QCP-l

Zertifikatsanforderungen können von Zertifikatsnehmern zu einem von ihnen erzeugten 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

Der öffentliche Schlüssel der CA ist im Zertifikat enthalten. Dieses Zertifikat befindet sich i. d. R. auf dem Token, das dem Zertifikatsnehmer 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 Verschlüsselungsalgorithmus 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.

Werden die privaten EE-Schlüssel im Verantwortungsbereich des Zertifikatsnehmers erstellt, so hat dieser ebenfalls dafür zu sorgen, dass eine ausreichende Qualität bei der Schlüsselerzeugung gewährleistet ist.

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 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 der PIN aktiviert.

6.2.9 Deaktivieren privater Schlüssel

Die allgemeinen Regelungen sind im TSPS dokumentiert.

Die jeweilige Anwendung deaktiviert den privaten EE-Schlüssel, spätestens aber das Ziehen der Karte aus dem Kartenleser bzw. das Deaktivieren oder Löschen des Soft-PSEs.

Eine dauerhafte Deaktivierung der privaten EE-Schlüssel auf Chipkarten erfolgt, wenn die PIN-Eingabe aufeinander folgend mehrfach fehlerhaft ist. Die Anzahl der Reaktivierungsvorgänge der Karte durch Eingabe der PUK ist begrenzt. Mehrfachsignaturkarten verfügen nicht über eine PUK.

6.2.10 Zerstörung privater Schlüssel

Die allgemeinen Regelungen sind im TSPS dokumentiert.

QCP-n-qscd, QCP-l-qscd
Wird der Chip der Karte zerstört oder werden die Dateien, die den privaten EE-Schlüssel enthalten, gelöscht, so ist der private Schlüssel zerstört.

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 für

QCP-l, QCP-l-qscd, QCP-n-qscd
EE-Zertifikate werden mit einer maximalen Gültigkeit von 39 Monaten ausgestellt. Eine längere Gültigkeit kann vertraglich vereinbart werden.

Wird ein Zertifikat für einen längeren Zeitraum als 24 Monate ausgestellt, trägt der Kunde 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.

QCP-l
Wird das Schlüsselpaar vom Zertifikatsnehmer erzeugt, wird das Aktivierungsgeheimnis bei diesem Verfahren ebenfalls produziert und steht dem Zertifikatsnehmer somit zur Verfügung.

QCP-n-qscd, QCP-l-qscd
Erzeugt der TSP die Schlüssel, wird entweder ein Transport-PIN-Verfahren genutzt oder die PINs werden in einen PIN-Brief gedruckt und an den Zertifikatsnehmer versandt oder übergeben.

6.4.2 Schutz von Aktivierungsdaten

Die allgemeinen Regelungen sind im TSPS dokumentiert.

Zertifikatsnehmer: Beim Transport-PIN-Verfahren ist die Unversehrtheit der Karte über die Transport-PIN erkennbar. In anderen Verfahren werden die PINs einmalig in einen besonders gesicherten PIN-Brief gedruckt oder über eine TLS-gesicherte Webseite an den Zertifikatsnehmer versandt oder übergeben.

6.4.3 Andere Aspekte von Aktivierungsdaten

Produktspezifisch wird Zertifikatsnehmern mit Signaturkarte zusätzlich zu der PIN eine Personal Unblocking Key-Nummer (PUK) zum Entsperren der Signaturkarte (nach dreimaliger Fehleingabe der PIN) angeboten.

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 werden in der subjectPublicKeyInfo derzeit folgende Algorithmen verwendet:

- rsaEncryption mit OID 1.2.840.113549.1.1.1
- id-RSASSA-PSS mit OID 1.2.840.113549.1.1.10 (wird nicht verwendet bei EVCP, OVCP)

Für ECC-Schlüssel werden in den CA- und EE-Zertifikaten derzeit folgende Kurven verwendet:

- secp384r1 mit OID 1.3.132.0.34
- secp521r1 mit OID: 1.3.132.0.35
- secp256r1 mit OID: 1.2.840.10045.3.1.7

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

- sha512WithRSAEncryption mit OID 1.2.840.113549.1.1.13
- sha384WithRSAEncryption mit OID 1.2.840.113549.1.1.12
- sha256WithRSAEncryption mit OID 1.2.840.113549.1.1.11
- ecdsa-with-SHA256 mit OID 1.2.840.10045.4.3.2
- ecdsa-with-SHA384 mit OID 1.2.840.10045.4.3.3
- ecdsa-with-SHA512 mit OID 1.2.840.10045.4.3.4

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

„CertificatePolicies" kann die OIDs unterstützter CPs enthalten.

Weitere Regelungen sind in der CP in Abschnitt 1.1.3 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 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.