Certification Practice Statement of the D-TRUST CSM PKI

ENGLISH

DEUTSCH

Teil der Bundesdruckerei-Gruppe

Certification Practice Statement of the D-TRUST CSM PKI

Version 3.8

Teil der Bundesdruckerei-Gruppe

COPYRIGHT NOTICE AND LICENSE

Certification Practice Statement of the D-TRUST CSM PKI
©2022 D-Trust GmbH

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

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

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

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

2.8	2019-10-09	Update according to observation report Clarification of section 5.5.2 Editorial changes
2.9	2020-03-19	▪ Introduction of domain-validated TLS certificates (DVCP) according to EN 319 411-1 and BRG ▪ This CPS complies with the requirements of Mozilla Policy 2.7 ▪ Full annual review of the CPS ▪ Adjustment of the archiving period for LCP in section 5.5.2 ▪ SHA-256 fingerprints added in section 1.1.3 ▪ Domain validation methods added in section 4.2.1
2.10	2020-04-27	▪ Activation of the sub-CA for issuing DV certificates, see section 1.1.3. ▪ Integration of new sub-CAs for issuing EV and OV certificates, see section 1.1.3. ▪ Amendments to certificate chain verification in section 4.5.2. ▪ Amendments in sections 5.3.7 and 5.5.2 ▪ Reduction of the validity period of TLS certificates, see section 6.3.2.
2.11	2020-06-17	▪ Introduction of administration-PKI (V-PKI) certificates according to BSI TR-03145-1
2.12	2020-09-28	▪ Assignment of a D TRUST OID for the V-PKI ▪ Publication and commissioning of the V-PKI sub CA ▪ Link added in section 4.2.1 for publication of registration or incorporating agency information in the repository
3.0	2020-11-10	▪ From version 3 or higher, the CSM CPS is subordinate to the TSPS ▪ Update according to observation report ▪ Amendment in section 3.3.1
3.1	2021-02-10	▪ Amendments in sections 3.1.4 and 3.2.2 ▪ Link replaced in section 1.1.3
3.2	2021-04-23	▪ 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, 3.3.1, 6.1.1, 7.1.3
3.3	2021-07-02	▪ Introduction of new qualified CAs in section 1.1.3 ▪ Introduction of qualified seal certificates without QSCD for the EU digital vaccination certificate, see sections 2.1, 3.1.4, 4.4.2, 4.9.9 ▪ Update in the context of the BR Self Assessment ▪ Editorial changes and amendments in sections 2.1, 2.3, 3.1.1, 3.1.4, 3.1.6, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.3.1, 4.3.1, 4.4.2, 4.9.5, 4.9.9, 7.1.3, 7.16
3.4	2021-10-14	▪ Amendments in sections 3.1.4 and 6.1.1
3.5	2021-12-16	▪ Adjustments and concretisations in sections 1.1.3, 3.1.4, 3.2.1, 4.4.1, 4.7, 6.2.1 and 6.4.1.

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 section 1.1.3 ▪ Full annual review of the CPS
3.7	2022-06-13	▪ Inclusion of certificate issuance for external employees as part of the V-PKI, see section 1.1.3 and 3.1.4 ▪ Concretisations in section 1.1.3, 3.1.4, 3.2.4, 4.2.1 and 6.3.2
3.8	2022-11-14	▪ More detailed information in sections 2.1 and 4.5.1 ▪ Introduction of the current "CA root inclusion" process in section 1.1.3

Contents

1. Introduction

1.1 Overview

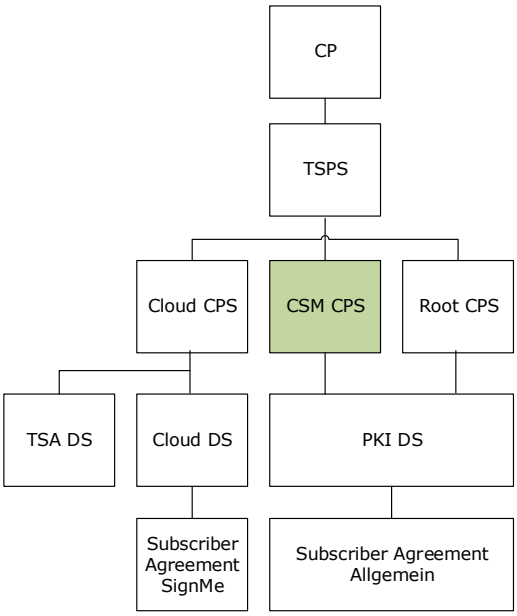
This document is the Certification Practice Statement (CPS) of the trust services operated by D-Trust GmbH that are provided via the Certificate Service Manager (CSM). The document name is abbreviated **CSM CPS** and is subject to the Trust Service Practice Statement of D-TRUST (abbreviated as TSPS)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

1.1.1 Trust service provider (TSP)

These rules are documented in the CP.

1.1.2 About this document

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



References are shown as follows:

- **These rules are documented in the CP.**
  Rules that refer to certificate policies are documented in the CP.
- **The general rules are documented in the TSPS.**
  The general rules are documented in the TSPS and the specific rules remain in the CPS.
- **Other rules are documented in the TSPS.**
  In addition to the specific rules in the CPS, there are also other rules that are documented in the 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 trust services provided via the CSM are based on a multi-level PKI. 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[1]

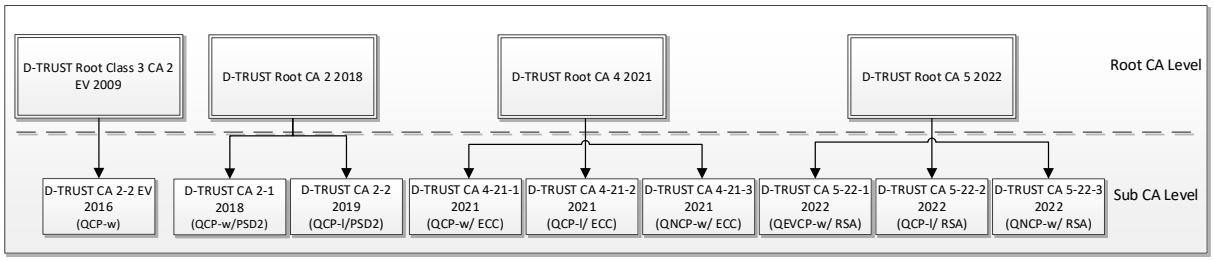


Fig. 1: PKI hierarchy for qualified trust services

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

QEVCP-w und QNCP-w – Qualified Website Authentication Certificates (QWACs)

QCP-l – Qualified Seal Certificates (QSealCs)

The policy levels are explained in the TSPS.

---

[1] D-TRUST CA 4-21-1 2021 and D-TRUST CA 4-21-2 2021 have been published in the Trusted List of the Federal Network Agency (BNetzA) and are now in operation. D-TRUST CA 4-21-3 2021 has been created, but is not yet in operation. Following publication in the Federal Network Agency's Trusted List, the sub-CA will be put into operation.

The sub-CAs from the D-TRUST Root CA 5 2022 have been created but are not yet in operation. Following publication in the Federal Network Agency's Trusted List, the sub-CAs will be put into operation.

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

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

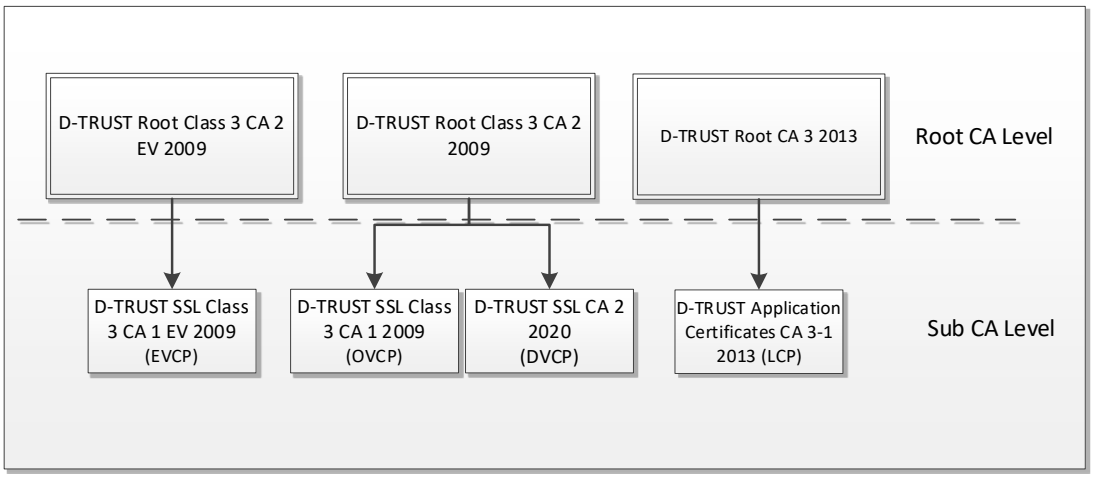


Fig. 2: Currently valid PKI hierarchy for publicly trusted services

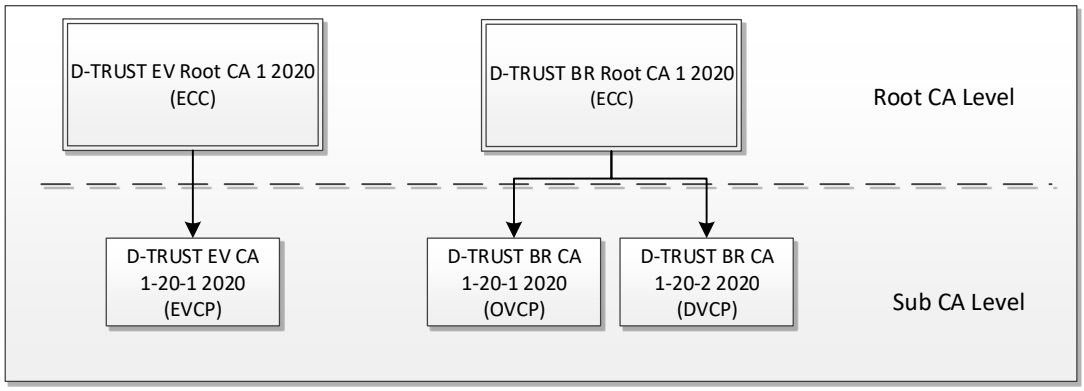


Fig. 3: PKI hierarchy for publicly trusted TLS services in the "CA root inclusion" process[3]

[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.

[3] In future, the "D-TRUST EV Root CA 1 2020" root CA is to replace the existing "D-TRUST Root Class 3 CA 2 EV 2009" root CA and is listed here for information purposes. In future, the "D-TRUST BR Root CA 1 2020" root CA is to replace the existing "D-TRUST Root Class 3 CA 2 2009" root CA and is listed here for information purposes.

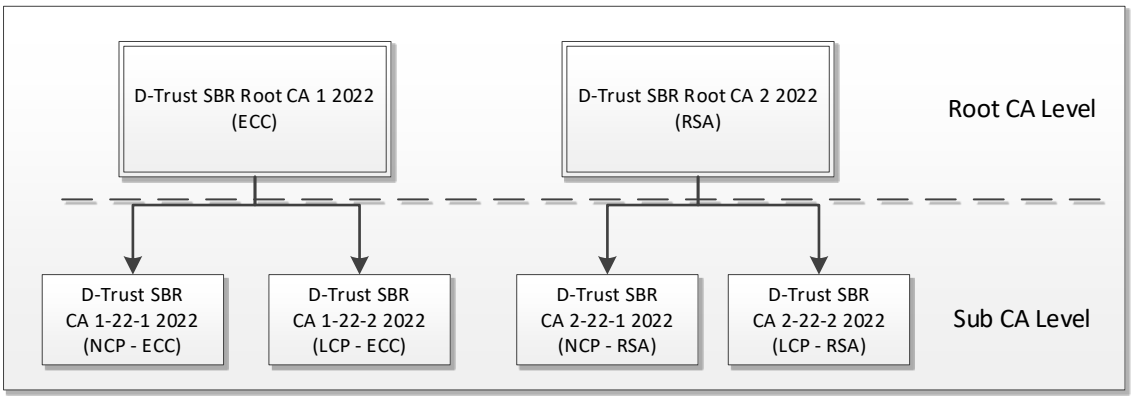


Fig. 4: PKI hierarchy for publicly trusted S/MIME trust services in the "CA root inclusion" process[4]

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

NCP - Normalized Certificate Policy (currently only informative)

LCP – Lightweight Certificate Policy

DVCP – Domain Validation Certificate Policy

OVCP – Organizational Validation Certificate Policy

EVCP – Extended Validation Certificate Policy

The policy levels are explained in the TSPS.

[4] The root CA "D-Trust SBR Root CA 1 2022" with ECC keys and "D-Trust SBR Root CA 2 2022" with RSA keys are in the "CA Root Inclusion" process and are to replace the existing root CA "D-TRUST Root CA 3 2013" and are listed here for information purposes.

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

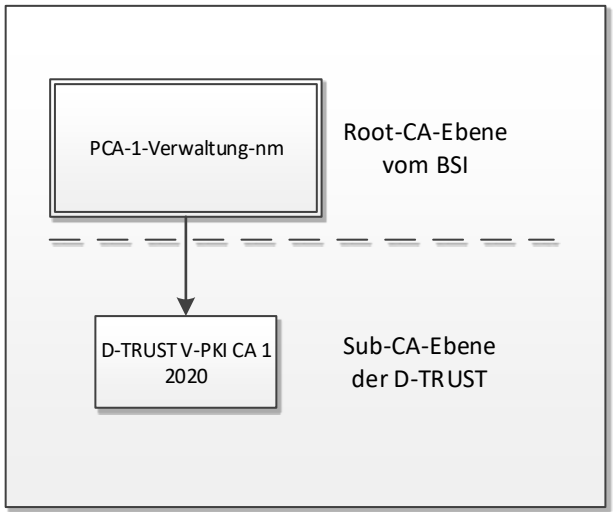


Fig. 5: PKI hierarchy for the trust service of the administration PKI (V-PKI)

The root authority PCA-1-Administration is operated by the Federal Office for Information Security in accordance with the "Security guidelines of the administration root certification authority", version 3.2 dated 9 January 2003 and the related amendments, version 1.1, dated 29 January 2013 (abbreviated as: **CP V-PKI BSI**).

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

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

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

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

It is not foreseen for the "D-TRUST V-PKI CA 1 2020" sub-CA to issue further sub-CAs or issuing CAs.

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

CA certificates

The complete overview of all root CAs and sub-CAs with policy levels QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, 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 following table provides an overview of all root CAs and the associated sub-CAs to which this CPS applies.

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 CA 2-2 EV 2016 https://www.d-trust.net/cgi-bin/D-TRUST_CA_2-2_EV_2016.crt Policy Level: QEVCP-w Fingerprint: SHA1: 8423CDA13FF6025BCD3188DDB37F8618C31D85D9 SHA256: 2316D05A2E2D347FA141135B98ED09F56E81F1CF5679793D3B39DD6D8E461A48 OID: 1.3.6.1.4.1.4788.2.150.4
D-TRUST SSL Class 3 CA 1 EV 2009 https://www.d-trust.net/cgi-bin/D-TRUST_SSL_Class_3_CA_1_EV_2009.crt Policy Level: EVCP Fingerprint: SHA1: 1069423D308D0FC54575059638560FC7556E32B3 SHA256: B0935DC04B4E60C0C42DEF7EC57A1B1D8F958D17988E71CC80A8CF5E635BA5B4 OID: 1.3.6.1.4.1.4788.2.202.1
VR IDENT EV SSL CA 2020[5] - sub-CA revoked https://www.d-trust.net/cgi-bin/VR_IDENT_EV_SSL_CA_2020.crt Policy Level: EVCP Fingerprint: SHA1: AC4126DEB7907EE1BBC00A6504BD2AB224237915 SHA256: 9E6C8035C0F1C8A945310E72D83E531947B571F9292E42A4248A370BF7B305BE OID: 1.3.6.1.4.1.4788.2.230.1

[5] The Sub-CA "VR IDENT EV SSL CA 2020" has been revoked.

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 SSL CA 2 2020 https://www.d-trust.net/cgi-bin/D-TRUST_SSL_CA_2_2020.crt Policy Level: DVCP Fingerprint: SHA1: AEB9682B91D20B50384A2C6B6DACBB851F629962 SHA256: 972A181B60294EBA07333B9C1982440D43395ABA91D450EC0EFB485AED49D5A7 OID: 1.3.6.1.4.1.4788.2.202.3
VR IDENT SSL CA 2020[6]- sub-CA revoked https://www.d-trust.net/cgi-bin/VR_IDENT_SSL_CA_2020.crt Policy Level: OVCP Fingerprint: SHA1: C3A6BC49BC9936E9450A9775465B7235E78EE705 SHA256: 007108194115F3C899F54EE67CB4DA87275EDC1D6798DA787E0758CFA6AE96B1 OID: 1.3.6.1.4.1.4788.2.230.2
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

[6] The Sub-CA "VR IDENT SSL CA 2020" has been revoked.

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
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 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)
PCA-1-Administration Refer to the BSI website: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/VerwaltungsPKIVPKI/Wurzelzertifizierungsstelle/FingerprintsderWurzelzertifikate/pcafingerprint.html
D-TRUST V-PKI CA 1 2020 https://www.d-trust.net/cgi-bin/D-TRUST_V-PKI_CA_1_2020.crt or http://x500.bund.de/ Policy Level: V-PKI OID: 0.4.0.127.0.7.3.6.1.1.4.4 (BSI) OID: 1.3.6.1.4.1.4788.2.201.2 (D-TRUST)

D-TRUST EV Root CA 1 2020 (ECC) – Currently in the "CA root inclusion" process https://www.d-trust.net/cgi-bin/D-TRUST_EV_Root_CA_1_2020.crt Fingerprint: SHA1: 61DB8C2159690390D87C9C128654CF9D3DF4DD07 SHA256: 08170D1AA36453901A2F959245E347DB0C8D37ABAABC56B81AA100DC958970DB
D-TRUST EV CA 1-20-1 2020 – Currently in the "CA root inclusion" process https://www.d-trust.net/cgi-bin/D-TRUST_EV_CA_1-20-1_2020.crt Policy Level: EVCP Fingerprint: SHA1: 8D01990148D7148C61B3C0B3F743A353F401BA6C SHA256: 41C897473B0369FA74B1F4F9D7F89129485C1A305C0719A867DC8714E0870200 OID: 1.3.6.1.4.1.4788.2.202.1 (D-TRUST EV OID) OID: 2.23.140.1.1 (CA/Browser Forum EV OID)
D-TRUST BR Root CA 1 2020 (ECC) – Currently in the "CA root inclusion" process https://www.d-trust.net/cgi-bin/D-TRUST_BR_Root_CA_1_2020.crt Fingerprint: SHA1: 1F5B98F0E3B5F7743CEDE6B0367D32CDF4094167 SHA256: E59AAA816009C22BFF5B25BAD37DF306F049797C1F81D85AB089E657BD8F0044
D-TRUST BR CA 1-20-1 2020 – Currently in the "CA root inclusion" process https://www.d-trust.net/cgi-bin/D-TRUST_BR_CA_1-20-1_2020.crt Policy Level: OVCP Fingerprint: SHA1: 16407AFD6EE36C777730AE95D6C6286ECE4C389F SHA256: 199AB2AAAFFF40401E0A3B7B87EE9964659EFFA94A1FECBE918AE136E4B4E0A8 OID: 1.3.6.1.4.1.4788.2.202.2 (D-TRUST OV OID) OID: 2.23.140.1.2.2 (CA/Browser Forum OV OID)
D-TRUST BR CA 1-20-2 2020 – Currently in the "CA root inclusion" process https://www.d-trust.net/cgi-bin/D-TRUST_BR_CA_1-20-2_2020.crt Policy Level: DVCP Fingerprint: SHA1: 5714DF60B3F5CA276413244F419C1C61496624A1 SHA256: B268D16934AB5BA232F179CD9F5C7FC07EA8583A56A9A7C1D6CB58FE0823BF5A OID: 1.3.6.1.4.1.4788.2.202.3 (D-TRUST DV OID) OID: 2.23.140.1.2.1 (CA/Browser Forum DV OID)

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[7] 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[7] Fingerprint: SHA1: 643211332169B483B55F7046E56CBFC6C11DC5F8 SHA256: D839672F984DCA7CD480CE201627A4DE61C5C1855F450E5B706200E73A23F047

[7] The link is activated when the CA is registered in the EU Trusted List and preparations are made for operation.

D-TRUST CA 5-22-1 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-TRUST_CA_5-22-1_2022.crt[7] 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[7] 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[7] Policy Level: QNCP-w Fingerprint: SHA1: 8A259DBB8B8C3AB5971B94590C7BABAFE57B5E1F SHA256: D9B38F7314AAB95DE57B63784F7D123D031C4FED6D8F66ED55A91BD05FEA818B OID: 1.3.6.1.4.1.4788.2.150.3
D-Trust SBR Root CA 1 2022 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-Trust_SBR_Root_CA_1_2022.crt Fingerprint: SHA1: 0F523A6B4E7D1D1805A548F94DCDE4C31E1BE9E6 SHA256: D92C171F5CF890BA428019292927FE22F3207FD2B54449CB6F675AF4922146E2
D-Trust SBR CA 1-22-1 2022 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-Trust_SBR_CA_1-22-1_2022.crt Policy Level: NCP Fingerprint: SHA1: 51575F287395A0B53EC2807631ED205134E4AAA9 SHA256: 31FFA8D3F2439C62F2363FE56F4E245382A6D69D8A828B3539FA3875F8C5235B OID: 1.3.6.1.4.1.4788.2.200.3

D-Trust SBR CA 1-22-2 2022 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-Trust_SBR_CA_1-22-2_2022.crt Policy Level: LCP Fingerprint: SHA1: C3288BB25E4E49AC4590999BF73875B1D48F6037 SHA256: 200E2C50111A71B07555E921D3BFB7EBDE47F7E41873E06753474362BC017BA2 OID: 1.3.6.1.4.1.4788.2.200.2
D-Trust SBR Root CA 2 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-Trust_SBR_Root_CA_2_2022.crt Fingerprint: SHA1: 27FF63B9EF34293103381AD86060DACC602835E1 SHA256: DBA84DD7EF622D485463A90137EA4D574DF8550928F6AFA03B4D8B1141E636CC
D-Trust SBR CA 2-22-1 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-Trust_SBR_CA_2-22-1_2022.crt Policy Level: NCP Fingerprint: SHA1: 557FFA0723CF6B21B88D2576C13615251E309668 SHA256: CED8E0893E52A1C96AE65D9955A908C45003D7CEADE56B3E4717FD8F00EE0743 OID: 1.3.6.1.4.1.4788.2.200.3
D-Trust SBR CA 2-22-2 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-Trust_SBR_CA_2-22-2_2022.crt Policy Level: LCP Fingerprint: SHA1: 6A1460777BA94726D2215D8853E9AC775A0D9C5A SHA256: 6E87C6E63C8BEE394908B97D1079F8FF88C3930E0EBEC5708C159E2B83247FF0 OID: 1.3.6.1.4.1.4788.2.200.2

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 CSM PKI
Version	3.8

1.3 PKI participants

1.3.1 Certification authorities (CAs)

These rules are documented in the TSPS.

1.3.2 Registration authorities (RAs)

These rules are documented in the TSPS.

1.3.3 Subscribers and end-entities (EEs)

These rules are documented in the TSPS.

1.3.4 Relying parties (RPs)

These rules are documented in the TSPS.

1.4 Certificate usage

1.4.1 Permitted certificate usage

These rules are documented in the TSPS.

1.4.2 Forbidden certificate usage

These rules are documented in the TSPS.

1.4.3 Service certificate usage

These rules are documented in the TSPS.

1.5 Policy administration

1.5.1 Responsibility for the document and contact data

These rules are documented in the TSPS.

1.5.2 Reporting security incidents with certificates

These rules are documented in the CP.

1.5.3 Compatibility of CPs of external CAs with this CPS

The general rules are documented in the TSPS.

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP

TLS certificates or their sub-CAs and root CAs comply with the requirements of the "Baseline Requirements of the CA/Browser Forum" [BRG] in the version according to the references in the latest CP of D-Trust GmbH as well as [EN 319 411-1].

Moreover, TLS certificates or their sub-CAs and root CAs of QEVCP-w and EVCP policy levels additionally comply with the requirements of the "Forum Guidelines for Extended Validation Certificates" [EVGL] in the version according to the references in section 1.6.3 of the CP as well as [EN 319 411-2].

In the event of inconsistencies between this document and the guidelines referred to, [BRG] and [EN 319 411-1] as well as [EVGL] and [EN 319 411-2] (if applicable) have priority.

QEVCP-w, QNCP-w with PSD2 extension

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

QCP-l

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

1.6 Definitions and acronyms

1.6.1 Definitions and names

These rules are documented in the CP.

1.6.2 Acronyms

Certificate Policy (CP)	Certificate policy.
UPN	User Principal Name

Other rules are documented in the CP.

1.6.3 References

These rules are documented in the CP.

2. Publication and Repository Responsibility

2.1 Repositories

If OSCP is available, 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.

QCP-l for the EU digital vaccination certificate

A certificate status query via OCSP is prohibited according to the [eHealth Network Guidelines] and is not offered.

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

Teil der Bundesdruckerei-Gruppe

- This CPS
- The Subscriber Agreement
- PKI Disclosure Statement for qualified trust services

Other rules are documented in the TSPS.

2.3 Publication frequency

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP

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

QCP-l

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

Publication takes place immediately after the certificate is issued.

V-PKI

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

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

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

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 name*.

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.

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

3.1.4 Rules for the interpretation of different name forms

The attributes of the *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, QEVCP-w, QNCP-w, EVCP, OVCP, DVCP: This field is not used. LCP, V-PKI: According to the proof used for identification
SN (surname)	*Surname* of the natural person QCP-l, QEVCP-w, QNCP-w, EVCP, OVCP, DVCP: This field is not used. NCP, LCP, V-PKI: According to the proof used for identification If pseudonyms are used, SN corresponds to CN.

DN component	Interpretation
CN (commonName) (2.5.4.3)	*Common name:* The following variants are used: ▪ Natural persons without a pseudonym: "Surname, name used". ▪ 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. ▪ Domain name: A FQDN can be included in the CN. If available, this must also be stored as a SAN entry. ▪ QEVCP-w, QNCP-w, EVCP: Wildcards are not used in TLS certificates for this policy level. ▪ OVCP, DVCP: Wildcards can be requested. ▪ Function or group of persons: Name of the function or group of persons preceded by the abbreviation "GRP:" in order to indicate that this is a group certificate. ▪ V-PKI: ▪ Function certificates/group certificates In the V-PKI, certificates that are issued for a group of people are referred to as function certificates. If the CN does not indicate the function, the entry in the CN begins with "FKT". The subscriber is responsible for ensuring that the private key of a function certificate from the V-PKI is not used by more than 30 people at the same time. ▪ External staff: In the V-PKI, "Ext.:" at the beginning of the CN is added to certificates issued to external staff of the certificate holder's organization. ▪ Technical components: Name of the server, service or application using the certificate

DN component	Interpretation
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 V-PKI: The SAN can be filled with otherName and the User Principal Name (UPN) contained there or by entering the RegisteredID. Special case: It is also possible to include one or more domain names in the SAN. QEVCP-w, QNCP-w, EVCP: Wildcards are not used in TLS certificates for this policy level. OVCP, DVCP: Wildcards can be requested.
PN (pseudonym)	*Pseudonym*: Identical to CN. V-PKI: No pseudonyms are assigned.
Serial Number (serialNumber) (2.5.4.5)	*Serial number*: Name suffix number to ensure unambiguity of the name (typically the application number). Special case for EV certificates according to [EVGL]: Register number if assigned, date of registration or establishment. If the Government Entity does not have a registration number or the date of establishment identified, the field is completed with "Government Entity". 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 affiliated (company, public authority, association, etc.) according to the proof of existence; if necessary, abbreviated to a meaningful name if the maximum number of 64 characters is exceeded. **EVCP:** If a trade name is included in field O, the organization name must be listed in brackets after it according to section 9.2.1 [EVGL]. **OVCP:** If a trade name is included in field O, the specifications from section 7.1.4.2.2 (b) [BRG] must be observed. **DVCP:** This field is not used.
OU (organizationalUnit Name) (2.5.4.11)	Organizational unit of the organization, such as department, division or other sub-division or QEVCP-w, QNCP-w: Trade name of the organization EVCP, OVCP: Trade name of the organization (from 1 September 2022, this field will no longer be used for EVCP and OVCP) DVCP: This field is not used.

DN component	Interpretation
OrgID (organizationIdentifier) (2.5.4.97)	**LCP (Seal ID):** *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). **QEVCP-w, EVCP, OVCP, DVCP:** This field is not used. **QCP-l, QEVCP-w and QNCP-w with PSD2 extension:** *PSD2 Authorisation Number* In the case of certificates that are used in PSD2 according to [TS 119 495], the organization identifier (2.5.4.97) must be used. The "Authorisation Number" ensures unambiguity. The "Authorisation Number" comprises the following characters: **PSD<cc>-<x..x>-<y..y>** where "PSD" – "legal person identity type", contains three characters; <cc> ISO 3166 country code of the national competent authority (NCA) – precisely two characters minus hyphen "-" <x..x> Identifier of the NCA – 2 – 8 capital letters A – Z, no blanks minus hyphen "-" <y..y> Identifier of the payment service provider, as defined by the NCA - any sequence of characters Example: PSDDE-BAFIN-1234Ab
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 which issued the document that was used to identify the subscriber. EVCP: According to section 9.2.6 [EVGL] DVCP: This field is not used.

DN component	Interpretation
Street (streetAddress) (2.5.4.9)	Postal address *Street* and *Number* EVCP: According to section 9.2.6 [EVGL] DVCP: This field is not used.
Locality (localityName) (2.5.4.7)	Postal address *City* EVCP: According to section 9.2.6 [EVGL] DVCP: This field is not used.
State (stateOrProvinceName) (2.5.4.8)	Postal address *(Federal) state* EVCP: According to section 9.2.6 [EVGL] DVCP: This field is not used.
PostalCode (postalCode) (2.5.4.17)	Postal address *Postal code* EVCP: According to section 9.2.6 [EVGL] DVCP: This field is not used.
BusinessCategory (businessCategory) (2.5.4.15)	Business Category according to [EVGL] Used only in the case of EVCP The business category field must contain one of the following: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity".
Jurisdiction Of Incorporation Locality (jurisdictionLocalityName)	Jurisdiction of the organization according to [EVGL]: *City* (1.3.6.1.4.1.311.60.2.1.1) Used only in the case of EVCP and when applicable according to the level of actual registration.
Jurisdiction Of Incorporation State Or Province Name (jurisdictionStateOrProvinceName)	Jurisdiction of the organization: *(Federal) state* (1.3.6.1.4.1.311.60.2.1.2) Used only in the case of EVCP and when applicable according to the level of actual registration.
Jurisdiction Of Incorporation CountryName (jurisdictionCountryName)	Jurisdiction of the organization according to [EVGL]: *Country* (1.3.6.1.4.1.311.60.2.1.3) Used only in the case of EVCP and when applicable according to the level of actual registration.

Further rules are documented in section 7.1.4 of the TSPS.

QEVCP-w[8], QNCP-w, EVCP

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

TLS certificates may only contain the subject DN components defined in section 9.2 [EVGL].

QCP-l

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

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

3.1.5 Unambiguity of names

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

The TSP ensures the unambiguity of *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).

QEVCP-w, QNCP-w, EVCP

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

QEVCP-w, QNCP-w, EVCP, OVCP

The TSP takes the steps needed to ensure that, at the time of certificate issuance, the applicant has the proven right to use the brand name included in the certificate. The requirements of section 3.2.2.2 [BRG] and, if applicable, section 11.3 [EVGL] are complied with.

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 in accordance with section 3.2.2.7 [BRG]. All data sources are approved by the D-Trust organizational unit for information security.

D-Trust qualifies and uses Qualified Independent Information Sources (QIIS) according to section 11.11.5 [EVGL]. QIIS is a part of the "Register" verification methods in section 4.2.1 of the TSPS.

---

[8] In the case of QEVCP-w and QNCP-w certificates with PSD2 extension, the "organizationIdentifier" is additionally used and checked.

A procedure has been established to ensure that the applicant can be reliably contacted via a verified communication method according to 11.5 [EVGL] and can confirm that they are aware of the request and agree to it.

3.2.1 Proof of ownership of the private key

Two cases are distinguished:

a) Key pairs of subscribers are produced in the TSP's sphere of responsibility. The TSP forwards the encrypted tokens or encrypted soft PSE 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.
Is not offered for QEVCP-w, QNCP-w, EVCP, OVCP, DVCP and V-PKI.

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

3.2.2 Identification and authentication of organizations and domains

Organizations that are either named in the certificate or in whose names certificates are issued must provide unambiguous proof of their identity.

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

On the different policy levels, the DN components are subjected to the validation procedures above according to section 3.1.4 plus further attributes, if necessary. The procedures shown in the table below are described in section 4.2.1.

	QEVCP-w, EVCP	QEVCP-w and QNCP-w with PSD2	OVCP	DVCP	QCP-l	LCP	NCP[9]
CN	Register/ Non-Register/ Domain/ CAA	Register/ Non-Register/ Domain/ CAA	Register/ Non-Register/ Domain/ CAA	Domain	Register/ Non-Register	HR-DB/ Register/ Non-Register	Register/ Non-Register
C O	Register/ Non-Register/ Domain	Register/ Non-Register/ Domain	Register/ Non-Register/ Domain	n.a.		Register/ Non-Register	Register/ Non-Register
OrgID	n.a.	Register	n.a.	n.a.	Register	n.a.	n.a.
OU[10]	C confirmation/ A confirmation/ Register	C confirmation/ A confirmation/ Register	C confirmation/ A confirmation Register	n.a.	C confirmation/ A confirmation/ Register	C confirmation/ A confirmation	C confirmation/ A confirmation
STREET L State PostalCode	Register/ Non-Register	Register/ Non-Register	Register/ Non-Register	n.a.	Register/ Non-Register	n.a.	n.a.
Alternative applicant (SAN)	Domain/ CAA	Domain/ CAA	Domain/ CAA	Domain/ CAA	n.a.	Domain/ e-mail/ HR-DB	Domain/ CAA/ e-mail/ HR-DB
All other attributes	n.a.	n.a.	n.a.	n.a.	n.a.	A confirmation/ Dok-Ident/ out-of-band mechanisms	A confirmation/ Dok-Ident/ out-of-band mechanisms

[9] Applies only to organization and machine certificates, except for TLS certificates.

BusinessCategory (businessCategory)	**Private Organization** Register **Government Entity** Register/ Non-Register **Business Entity** Register in combination with Pers-Ident **Non-Commercial Entity** Non-Register/ C confirmation	For QEVCP-w only: **Private Organization** Register **Government Entity** Register/ Non-Register **Business Entity** Register in combination with Pers-Ident **Non-Commercial Entity** Non-Register/ C confirmation	n.a.	n.a.	n.a.	n.a.	n.a.

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, according to NCP for advanced organization and machine certificates (except for TLS certificates) and according to QEVCP-w, QNCP-w and EVCP for website certificates.

A procedure has been established to ensure that the operational existence of the applicant (legal entity) is reliably verified in accordance with 11.6 [EVGL].

D-Trust obtains its information from various registration or incorporating agencies according to the "Register" verification methods in section 4.2.1 of the TSPS; these agencies are published in a table in the repository:

[10] For EVCP, OVCP, DVCP, LCP and NCP, the "OU" field will be omitted in the future.

https://www.d-trust.net/internet/files/D-TRUST_Agency-Information.pdf

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.

NCP, LCP, V-PKI

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

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

	V-PKI	LCP	NCP
G	Pers-Ident/ eID	HR-DB/ Dok-Ident/ Pers-Ident/ eID	HR-DB/ Pers-Ident/ eID
SN			
CN	Register/ Non-Register	HR-DB/ Register/ Non-Register	HR-DB/ Register/ Non-Register
C	DE	Register/ Non-Register	Register/ Non-Register
O	Register/ Non-Register	Register/ Non-Register	Register/ Non-Register
OU	C confirmation/ A confirmation	C confirmation/ A confirmation	C confirmation/ A confirmation
STREET	n.a.	n.a.	n.a.
L			
State			
PostalCode			
Alternative applicant (SAN)	e-mail	Domain/ e-mail/ HR-DB	Domain/ CAA/ e-mail/ HR-DB
All other attributes	n.a.	A confirmation/ Dok-Ident/ out-of-band mechanisms	A confirmation/ out-of-band mechanisms

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

Documents in non-Latin characters are not accepted.

3.2.4 Non-verified subscriber information

Verification of the subscriber's information is carried out or skipped according to sections 3.2.2, 3.2.3 and 4.2.1.

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, LCP, NCP
All of the information in the certificate is verified.

V-PKI
According to TSPS 7.1.2, EE certificates can contain the non-critical certificate extension subjectAltName. In EE certificates from the V-PKI, the subjectAltName certificate field may be filled with otherName and the User Principal Name (UPN) contained there or by entering a RegisteredID. This information in the subjectAltName extension is used within the subscriber's organization and is not verified by the TSP.

In the case of alternative names, only the e-mail addresses or their domain components are generally verified. Other certificate contents, e.g. LDAP directories, etc. as well as certificate extensions (AdditionalInformation, monetaryLimit, etc.), if any, are not checked for correctness.

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

3.2.5 Verification of request authorization

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

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

3.2.6 Criteria for interoperation

See section 1.5.3.

3.3 Identification and authentication for re-keying requests

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

3.3.1 Routine re-keying applications

Identification does not have to be repeated in the case of re-keying applications as long as the proof deposited at the TSP can still be used. Already validated data may only be used for a maximum period of 397 days. After that, this data must be validated once again. Re-keying applications must be submitted electronically via the agreed interface.

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

3.3.2 Re-keying following certificate revocation

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

3.4 Identification and authentication of revocation requests

Revocation authorization is verified as follows:

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

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

NCP, LCP, V-PKI

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

Revocation procedures are defined in section 4.9.

4. Operational Requirements

4.1 Certificate request and registration

4.1.1 Request authorization

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

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

QEVCP-w, EVCP

Subscribers must fulfil the requirements of [EVGL].

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

4.1.2 Registration process and responsibilities

The general rules are documented in the TSPS.

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

In addition to the TSPS, the following rule is also applicable to OVCP level:
In the CSM, the customer can choose an OVCP product with or without CT logging.

4.2 Processing the certificate request

4.2.1 Performing identification and authentication processes

The general rules are documented in the TSPS.

As part of the CSM CPS, different methods of identification are permitted depending on the policy level. The tables in sections 3.2.2 and 0 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
Dok-Ident
Register
Non-Register
HR-DB
C confirmation
A confirmation
Out-of-band mechanisms
Domain
E-mail address
CAA

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

4.2.2 Acceptance or rejection of certificate requests

These rules are documented in the TSPS.

4.2.3 Deadlines for processing certificate requests

These rules are documented in the TSPS.

4.3 Certificate issuance

4.3.1 Procedure of the TSP for issuing certificates

The general rules are documented in the TSPS.

As part of the CSM CPS, the following specific rules are also applicable:

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

This only applies if the product is offered with CT logging and this option was selected in the order process.

For TLS certificates, pre-issuance linting is carried out.

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

NCP, LCP

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

V-PKI

Certificates are made available for access-protected and TLS-encrypted download and/or via a TLS-protected interface (CSM) or by e-mail. Only certificates with a private key that was generated by the applicant are created.

QCP-l, QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP

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

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

The general rules are documented in the TSPS.

4.4.2 Publication of the certificate by the TSP

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

The status can be retrieved via OCSP after production.

V-PKI

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

QCP-l for the EU digital vaccination certificate

A certificate status query via OCSP is prohibited according to the [eHealth Network Guidelines] and is not offered.

4.4.3 Notification of other PKI entities concerning issuance of the certificate

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

4.5 Key pair and certificate usage

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

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

QCP-l, QEVCP-w, QNCP-w

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

The provisions in section 1.4 apply to subscribers.

4.5.2 Public key and certificate usage by relying parties

These rules are documented in the TSPS.

4.6 Certificate renewal

The rules laid down in sections 4.7 and 3.3 apply.

4.7 Certificate renewal with re-keying

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

Certificate renewal is not offered under the CSM request route.

With the CSM request route, the applicant obtains the certificates via an online interface. The registration and identification data of the organization and its authorized representatives (contract signer, technical contact partner and operators) stored in the system are revalidated each year, irrespective of the term of their certificates, and can thus be used for further certificate requests at any time.

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.

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.

4.8 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

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

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

Certificate revocation by phone is not possible.

Other revocation methods can be agreed to.

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

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

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

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

PSD2-specific revocation procedure

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

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

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

4.9.4 Revocation request deadlines

These rules are documented in the TSPS.

4.9.5 Time span for processing a revocation request by the TSP

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

4.9.6 Methods available for validating revocation information

Up-to-date revocation information is maintained in certificate revocation lists which can be retrieved via the LDAP[11] 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.

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

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

Information on status and revocation (OCSP and CRL) is consistent.

Status changes in the OCSP are available for query immediately after revocation. Status changes in a CRL contain the same revocation information. However, distribution of a new CRL takes place with a time delay after revocation.

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

QCP-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.

V-PKI, QCP-l for the EU digital vaccination certificate

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

4.9.10 Need for online verification of revocation information

These rules are documented in the TSPS.

4.9.11 Other forms for notification of revocation information

These rules are documented in the TSPS.

4.9.12 Special requirements if the private key is compromised

These rules are documented in the TSPS.

4.9.13 Conditions for suspension

These rules are documented in the TSPS.

4.10 Certificate status services

4.10.1 Operation of the certificate status service

These rules are documented in the TSPS.

4.10.2 Availability of the certificate status service

These rules are documented in the TSPS.

4.10.3 Optional services

These rules are documented in the TSPS.

4.11 Withdrawal from the certification service

These rules are documented in the TSPS.

4.12 Key escrow and recovery

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

4.12.1 Escrow and recovery procedures for private keys

The TSP does not offer key escrow.

4.12.2 Conditions and procedures for escrow and recovery of session keys

The TSP does not offer key escrow.

5. Facility, Management and Operational Controls

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

Other rules are documented in the TSPS.

5.1 Physical controls

These rules are documented in the TSPS.

5.2 Procedural controls

5.2.1 Role and authorization concept

These rules are documented in the TSPS.

5.2.2 Four-eyes principle

These rules are documented in the TSPS.

5.2.3 Identification and authentication for individual roles

These rules are documented in the TSPS.

5.2.4 Role exclusions

These rules are documented in the TSPS.

5.3 Personnel controls

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

5.3.1 Qualifications, experience and clearance requirements

These rules are documented in the TSPS.

5.3.2 Background checks

These rules are documented in the TSPS.

5.3.3 Training

These rules are documented in the TSPS.

5.3.4 Frequency of training and information

These rules are documented in the TSPS.

5.3.5 Job rotation frequency and sequence

These rules are documented in the TSPS.

5.3.6 Sanctions for unauthorized actions

These rules are documented in the TSPS.

5.3.7 Independent contractor requirements

These rules are documented in the TSPS.

5.3.8 Documentation supplied to personnel

These rules are documented in the TSPS.

5.4 Audit logging procedures

5.4.1 Monitoring access

These rules are documented in the TSPS.

5.4.2 Risk monitoring

These rules are documented in the TSPS.

5.5 Records archival

5.5.1 Types of records archived

These rules are documented in the TSPS.

5.5.2 Retention period for archive

These rules are documented in the TSPS.

5.5.3 Archive protection

These rules are documented in the TSPS.

5.5.4 Archive data backup

These rules are documented in the TSPS.

5.5.5 Requirements for time stamping of records

These rules are documented in the TSPS.

5.5.6 Archiving (internally/externally)

These rules are documented in the TSPS.

5.5.7 Procedure for obtaining and verifying archive information

These rules are documented in the TSPS.

5.6 Key change at the TSP

These rules are documented in the TSPS.

5.7 Compromise and disaster recovery at the TSP

5.7.1 Incident and compromise handling procedures

These rules are documented in the TSPS.

5.7.2 Recovery after resources have been compromised

These rules are documented in the TSPS.

5.7.3 Compromising of the private CA key

These rules are documented in the TSPS.

5.7.4 Disaster recovery options

These rules are documented in the TSPS.

5.8 Closure of the TSP or termination of services

These rules are documented in the TSPS.

6. Technical Security Controls

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

6.1 Key pair generation and installation

6.1.1 Generation of key pairs

The general rules are documented in the TSPS.

During generation of EE keys, the subscriber is required to generate these in a cryptographically secure manner in accordance with the requirements of [EN 319 411-1] and [EN 319 411-2].

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP

The subscriber may only submit a certificate request with a new self-generated key pair. This applies particularly to EE service certificate requests. If the TSP finds that the new certificate is being requested with the same key pair and/or a key pair is being used for the certificate request that matches one or more of the conditions in section 6.1.1.3 of [BRG], the certificate request will be denied.

V-PKI

The certificate subscriber may only submit a certificate request with a new, self-generated key pair and, in the case of Federal Government projects, is required to generate these in a cryptographically secure manner in accordance with the requirements of BSI [TR-02102-1].

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

6.1.2 Private key delivery to the subscriber

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

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

6.1.3 Public key delivery to the TSP

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP, V-PKI

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 mentioned in section 7.1.3.

6.1.7 Key usage purposes

These rules are documented in the TSPS.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

The general rules are documented in the TSPS.

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

V-PKI

The HSM "Utimaco CP5 SE 500" Version 5.1.0.0 is used for key generation and storage.

NCP, LCP

The TSP operates suitable hardware-based and software-based key generators in order to warrant the quality of the EE keys.

6.2.2 Private key (n out of m) multi-person control

The HSM on which the CA keys are stored is located in the secure environment of the trust service provider. A private key must be activated by two authorized persons.

Access to private EE keys is only possible in the case of keys in escrow according to section 6.2.3.

6.2.3 Private key escrow

The TSP does not offer escrow of private EE keys.

6.2.4 Private key backup

The general rules are documented in the TSPS.

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

6.2.5 Private key archival

These rules are documented in the TSPS.

6.2.6 Transfer of private keys to or from cryptographic modules

These rules are documented in the TSPS.

6.2.7 Storage of private keys in cryptographic modules

The general rules are documented in the TSPS.

Before being delivered, EE keys are contained in encrypted form in a database of the TSP.

6.2.8 Activation of private keys

The general rules are documented in the TSPS.

Private EE keys are activated by entering the secret.

6.2.9 Deactivation of private keys

The general rules are documented in the TSPS.

The respective application deactivates the private EE key, at the latest when the soft PSE is deactivated or deleted.

6.2.10 Destruction of private keys

The general rules are documented in the TSPS.

Keys that were generated within the TSP's area are automatically deleted after delivery.

6.2.11 Assessment of cryptographic modules

These rules are documented in the TSPS.

6.3 Other aspects of key pair management

6.3.1 Archiving of public keys

These rules are documented in the TSPS.

6.3.2 Validity periods of certificates and key pairs

The general rules are documented in the TSPS.

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

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP

Up until 31 August 2020, TLS certificates will be issued with the following validity period:

825 days max.

Since 1 September 2020, TLS certificates have been issued with the following validity period:

398 days max.

In 2022, the maximum validity period was reduced by one day. TLS certificates are now issued with the following validity period:

397 days max.

QEVCP-w and QNCP-w with PSD2 extension

Qualified website certificates with PSD2 extension are issued with the following validity period:

397 days max.

V-PKI

27 months max.

NCP, LCP

63 months max.

QCP-l

EE certificates are issued with a maximum period of validity of 39 months.

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

6.4 Activation data

6.4.1 Activation data generation and installation

The general rules are documented in the TSPS.

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

NCP, LCP

If EE keys are generated by the TSP, the PIN is either sent or handed over to the subscriber in a PIN letter or made available to the subscriber via a secured TLS connection or online interface.

NCP, LCP, V-PKI

If the subscriber is not the end-entity, then the subscriber is responsible for the secure delivery of the PIN to the end-entity.

6.4.2 Protection of activation data

The general rules are documented in the TSPS.

Subscriber: The PINs are delivered using a transport PIN method or are printed once as a specially protected PIN letter or sent or handed over to the subscriber via a TLS-secured website.

6.4.3 Other aspects of activation data

No stipulation.

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

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

- 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, DVCP)

The following curves are 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[12]
- secp256r1 with OID: 1.2.840.10045.3.1.7

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

- sha512 WithRSAEncryption with OID 1.2.840.113549.1.1.13
- sha256 WithRSAEncryption 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.

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP
The requirements of section 7.1.3.2 of [BRG] are observed.

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.

[12] This curve is not used for EVCP, OVCP, DVCP, LCP and NCP.

7.1.8 Syntax and semantics of "PolicyQualifiers"

These rules are documented in the TSPS.

7.1.9 Processing the semantics of the critical "CertificatePolicies" extension

These rules are documented in the TSPS.

7.2 CRL profiles

7.2.1 Version number(s)

These rules are documented in the TSPS.

7.2.2 Extensions of certificate revocation lists and certificate revocation list entries

These rules are documented in the TSPS.

7.3 OCSP profiles

These rules are documented in the TSPS.

7.3.1 Version number(s)

These rules are documented in the TSPS.

7.3.2 OCSP extensions

These rules are documented in the TSPS.

8. Compliance Audit and Other Assessments

These rules are documented in the TSPS.

9. Other Business and Legal Matters

With regard to the corresponding provisions, see section 9 in the CP.

Certification Practice Statement der D-TRUST CSM PKI

Version 3.8

Teil der Bundesdruckerei-Gruppe

COPYRIGHT UND NUTZUNGSLIZENZ

Certification Practice Statement der D-TRUST CSM PKI
©2022 D-Trust GmbH

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

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

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

Dokumentenhistorie

Version	Datum	Beschreibung
1.0	09.02.2015	▪ Initialversion
1.1	23.02.2015	▪ Editorische Änderungen im Rahmen der Erstzertifizierung gemäß ETSI 102 042 LCP. Es wurden diverse Inhalte aus der CP der D-Trust GmbH in das CPS überführt.
1.2	05.10.2015	▪ Editorische Änderungen ▪ Konkretisierung der Möglichkeit das Schlüsselmaterial durch den TSP erzeugen und ausliefern zu lassen ▪ Sperrung nur noch über Online-Schnittstelle und wenn ein Sperrpasswort vereinbart wurde telefonisch ▪ Alle neuen Zertifikate werden immer im LDAP der D-Trust veröffentlicht
1.3	03.10.2016	▪ Umstellung auf EN 319 411-1
2.0	01.01.2017	▪ Einführung von qualifizierten TLS-Zertifikaten (QWACs) gemäß EN 319 411-2 und eIDAS
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 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 ▪ Der Hotline Dienst wird eingestellt (Abschnitt 4.9.3) ▪ Jährliches Review des gesamten CPS ▪ Redaktionelle Anpassungen
2.6	15.05.2019	▪ 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.

Teil der Bundesdruckerei-Gruppe

2.8	09.10.2019	▪ Update nach observation report ▪ Präzisierung des Abschnitts 5.5.2 ▪ Editorische Änderungen
2.9	19.03.2020	▪ Einführung von Domain validierten TLS-Zertifikaten (DVCP) gemäß EN 319 411-1 und BRG ▪ 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	▪ Aktivierung der SubCA zur Ausstellung von DV-Zertifikaten, siehe Abschnitt 1.1.3 ▪ Einbindung neuer SubCAs zur Ausstellung von EV- und OV-Zertifikaten, siehe Abschnitt 1.1.3 ▪ 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	17.06.2020	▪ Einführung von Verwaltungs-PKI (V-PKI) Zertifikaten gemäß BSI TR-03145-1
2.12	28.09.2020	▪ Vergabe einer D-Trust OID für V-PKI ▪ Veröffentlichung und Inbetriebnahme der V-PKI SubCA ▪ Ergänzung eines Links in Abschnitt 4.2.1 zur Veröffentlichung von Registerführenden Stellen im Repository
3.0	10.11.2020	▪ Einführung eines übergeordnetes Practice Statements (TSPS, V1.0) für das CSM CPS ab Version 3.0. ▪ Update nach observation report ▪ Ergänzung in Abschnitt 3.3.1
3.1	10.02.2021	▪ Ergänzungen in Abschnitt 3.1.4 und 3.2.2 ▪ Austausch Link in Abschnitt 1.1.3
3.2	23.04.2021	▪ 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, 3.3.1, 6.1.1, 7.1.3
3.3	02.07.2021	▪ Bekanntmachung von neuen qualifizierten CAs in Abschnitt 1.1.3 ▪ Einführung von qualifizierten Siegelzertifikaten ohne QSCD für den digitalen EU Impfnachweis, siehe Abschnitte 2.1, 3.1.4, 4.4.2, 4.9.9 ▪ Update im Rahmen des BR Self Assessments ▪ Editorische Änderungen und Ergänzungen in den Abschnitten 2.1, 2.3, 3.1.1, 3.1.4, 3.1.6, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.3.1, 4.3.1, 4.4.2, 4.9.5, 4.9.9, 7.1.3, 7.1.6
3.4	14.10.2021	▪ Ergänzungen in Abschnitt3.1.4 und 6.1.1
3.5	16.12.2021	▪ Anpassungen und Konkretisierungen in den Abschnitten 1.1.3, 3.1.4, 3.2.1, 4.4.1, 4.7, 6.2.1 und 6.4.1.

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 ▪ Jährliches Review des gesamten CPS
3.7	13.06.2022	▪ Aufnahme der Zertifikatsausstellung für externe Mitarbeiter im Rahmen der V-PKI, siehe Abschnitt 1.1.3 und 3.1.4 ▪ Konkretisierungen in Abschnitt 1.1.3, 3.1.4, 3.2.4, 4.2.1 und 6.3.2
3.8	14.11.2022	▪ Konkretisierung in Abschnitt 2.1 und 4.5.1 ▪ Bekanntmachung des laufenden „CA Root Inclusion" Prozesses in Abschnitt 1.1.3

Teil der Bundesdruckerei-Gruppe

Inhaltsverzeichnis

Teil der Bundesdruckerei-Gruppe

Teil der Bundesdruckerei-Gruppe

1. Einleitung

1.1 Überblick

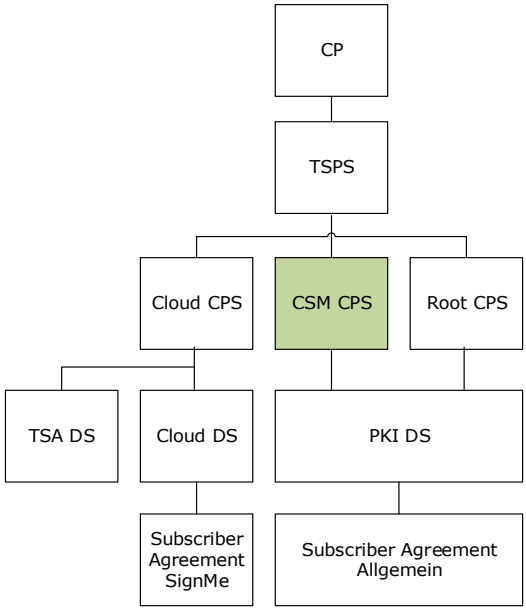
Dieses Dokument ist das Certification Practice Statement (CPS) der von D-Trust GmbH betriebenen Vertrauensdienste, die über den Certificate Service Manager (CSM) bereitgestellt werden. Der Dokumentenname wird mit **CSM CPS** abgekürzt verwendet und unterliegt dem Trust Service Practice Statement der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

1.1.1 Trust Service Provider (TSP - 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 LevelnPolicy 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 Vertrauensdienste, die über den CSM bereitgestellt werden, beruhen auf einer mehrstufigen PKI. Die Abbildungen 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), 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[1]

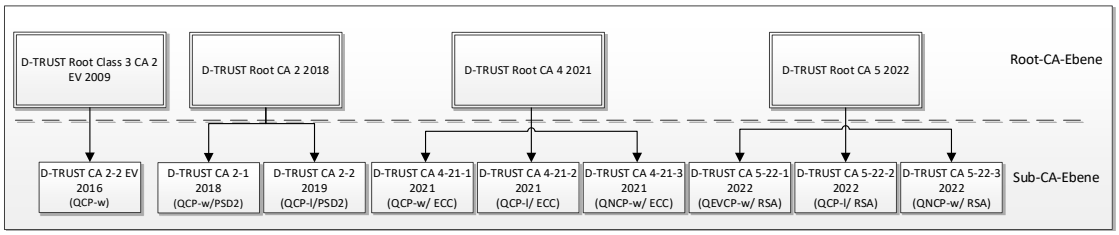


Abbildung 1: PKI-Hierarchie für qualifizierte Vertrauensdienste

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

QEVCP-w und QNCP-w – Qualifizierte Webseitenzertifikate (QWAC)

QCP-l – Qualifizierte Siegelzertifikate (QSealC)

Die Policy Level werden im TSPS erläutert.

---

[1] Die D-TRUST CA 4-21-1 2021 und D-TRUST CA 4-21-2 2021 sind in der Trusted List des BNetzA veröffentlicht und sind in Betrieb. Die D-TRUST CA 4-21-3 2021 ist erstellt, jedoch noch nicht in Betrieb. Die SubCA wird nach ihrer Veröffentlichung in der Trusted List der BNetzA in Betrieb genommen.

Die SubCAs aus der D-TRUST Root CA 5 2022 sind erstellt, jedoch noch nicht in Betrieb. Die SubCAs werden nach ihrer Veröffentlichung in der Trusted List der BNetzA in Betrieb genommen.

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

Teil der Bundesdruckerei-Gruppe

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

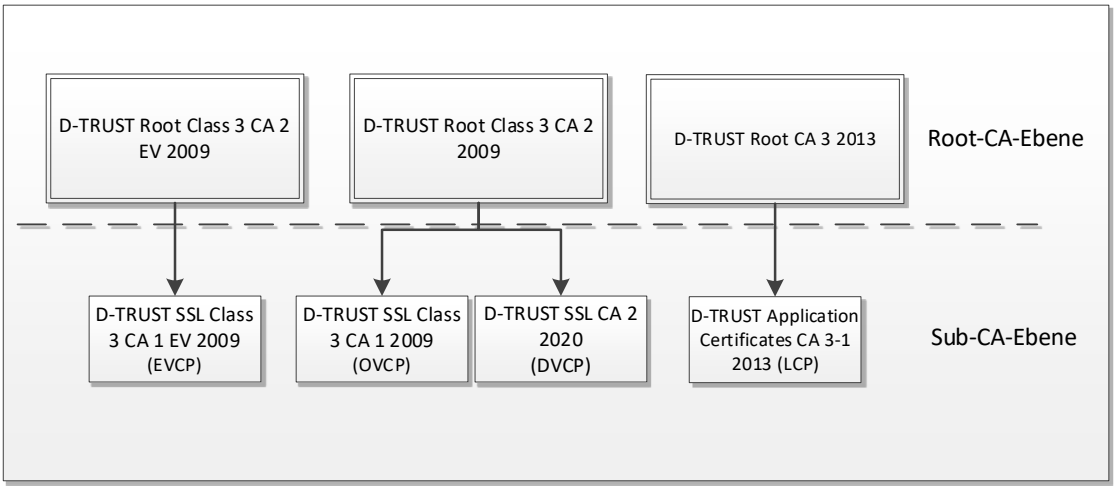


Abbildung 2: Aktuell gültige PKI-Hierarchie für „publicly trusted" Vertrauensdienste

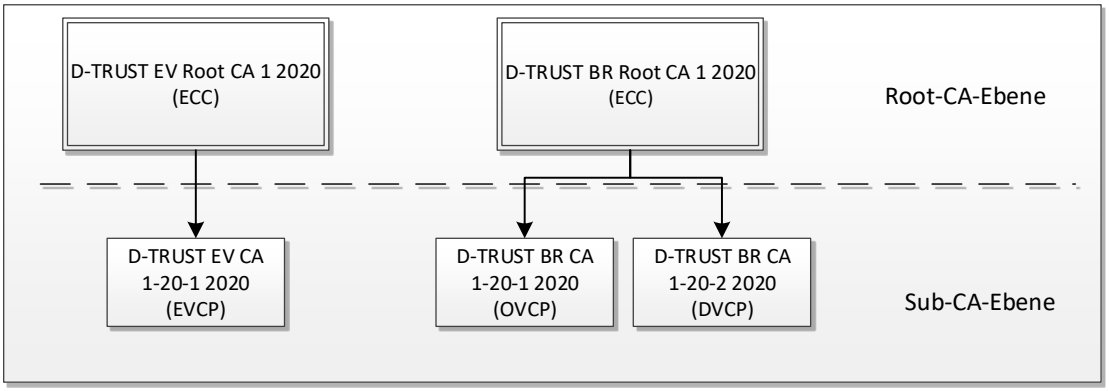


Abbildung 3: PKI-Hierarchie für publicly trusted TLS-Vertrauensdienste im „CA Root Inclusion" Prozess[3]

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

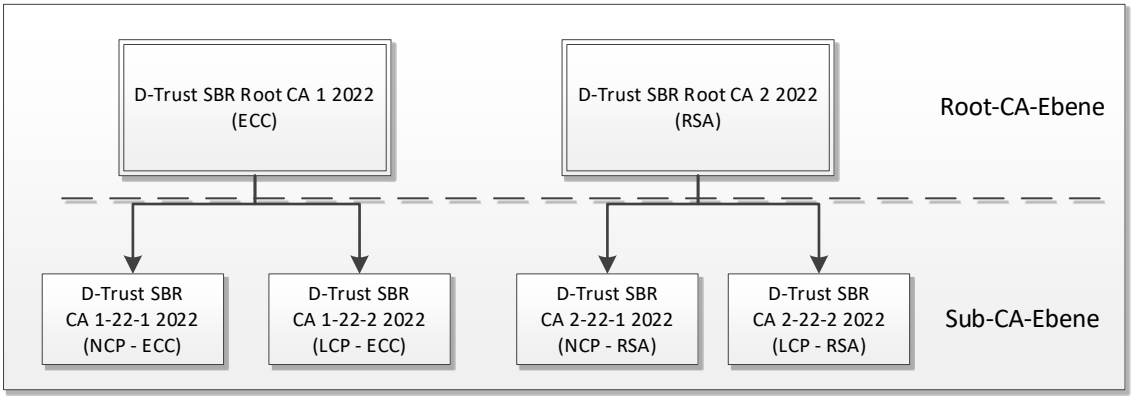


Abbildung 4: PKI-Hierarchie für publicly trusted S/MIME-Vertrauensdienste im „CA Root Inclusion" Prozess[4]

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

NCP - Normalized Certificate Policy (aktuell nur informativ)

LCP – Leightweight Certificate Policy

DVCP – Domain Validation Certificate Policy

OVCP – Organizational Validation Certificate Policy

EVCP – Extended Validation Certificate Policy

Die Policy Level werden im TSPS erläutert.

[4] Die RootCA „D-Trust SBR Root CA 1 2022" mit ECC-Schlüsseln und „D-Trust SBR Root CA 2 2022" mit RSA-Schlüsseln sind im „CA Root Inclusion" Prozess und sollen zukünftig die bestehende RootCA „D-TRUST Root CA 3 2013" ersetzen und werden hier informativ aufgeführt.

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

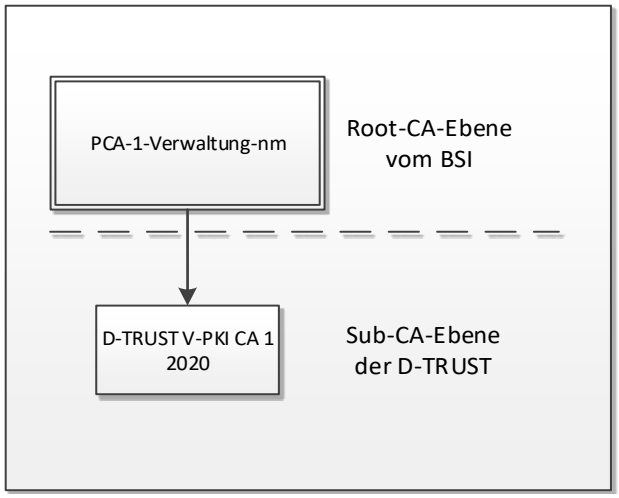


Abbildung 5: PKI-Hierarchie für den Vertrauensdienst Verwaltungs-PKI (V-PKI)

Die Wurzelinstanz PCA-1-Verwaltung wird entsprechend den „Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung" Version 3.2 vom 09.01.2003 und den dazugehörigen Ergänzungen und Änderungen Version 1.1 vom 29.01.2013 (kurz: **CP V-PKI BSI**) durch das Bundesamt für Sicherheit in der Informationstechnik betrieben.

Die SubCA „D-TRUST V-PKI CA 1 2020" ist beim Bundesamt für Sicherheit in der Informationstechnik (kurz: **BSI**) registriert und stellt ausschließlich V-PKI-Zertifikate aus.

In der Root Instanz erfolgt ein regelmäßiger Schlüsselwechsel im jährlichen Rhythmus. Bei Wechsel des Schlüssels der Zertifizierungsstelle wird ein neues Zertifizierungsstellen-Zertifikat von der Wurzelzertifizierungsstelle ausgestellt. Entsprechend CP V-PKI BSI Abschnitt 6.6. kann es somit mehrere gültige Zertifizierungsstellen-Zertifikate geben. Das „nm" im Namen vom RootCA wird entsprechend fortgezählt.

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

Zertifikate aus der V-PKI sowie deren Sub-CA werden gemäß den Anforderungen von BSI [TR-03145-1] ausgestellt. Die EE-Zertifikate aus der V-PKI lassen sich in ihrer Ausprägung den Anforderungen der einzelnen Richtlinien innerhalb der BSI [TR-03145-1] zuordnen.

Aus der Sub-CA „D-TRUST V-PKI CA 1 2020" ist die Ausstellung von weiteren Sub-CAs bzw. Issuing-CAs nicht vorgesehen.

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

CA-Zertifikate

Die Gesamtübersicht aller RootCAs und SubCAs mit den Policy Level QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, 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.

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 CA 2-2 EV 2016 https://www.d-trust.net/cgi-bin/D-TRUST_CA_2-2_EV_2016.crt Policy Level: QEVCP-w Fingerprint: SHA1: 8423CDA13FF6025BCD3188DDB37F8618C31D85D9 SHA256: 2316D05A2E2D347FA141135B98ED09F56E81F1CF5679793D3B39DD6D8E461A48 OID: 1.3.6.1.4.1.4788.2.150.4
D-TRUST SSL Class 3 CA 1 EV 2009 https://www.d-trust.net/cgi-bin/D-TRUST_SSL_Class_3_CA_1_EV_2009.crt Policy Level: EVCP Fingerprint: SHA1: 1069423D308D0FC54575059638560FC7556E32B3 SHA256: B0935DC04B4E60C0C42DEF7EC57A1B1D8F958D17988E71CC80A8CF5E635BA5B4 OID: 1.3.6.1.4.1.4788.2.202.1
VR IDENT EV SSL CA 2020[5] - Sub-CA gesperrt https://www.d-trust.net/cgi-bin/VR_IDENT_EV_SSL_CA_2020.crt Policy Level: EVCP Fingerprint: SHA1: AC4126DEB7907EE1BBC00A6504BD2AB224237915 SHA256: 9E6C8035C0F1C8A945310E72D83E531947B571F9292E42A4248A370BF7B305BE OID: 1.3.6.1.4.1.4788.2.230.1

[5] Die SubCA „VR IDENT EV SSL CA 2020“ wurde gesperrt.

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 SSL CA 2 2020 https://www.d-trust.net/cgi-bin/D-TRUST_SSL_CA_2_2020.crt Policy Level: DVCP Fingerprint: SHA1: AEB9682B91D20B50384A2C6B6DACBB851F629962 SHA256: 972A181B60294EBA07333B9C1982440D43395ABA91D450EC0EFB485AED49D5A7 OID: 1.3.6.1.4.1.4788.2.202.3
VR IDENT SSL CA 2020[6] - Sub-CA gesperrt https://www.d-trust.net/cgi-bin/VR_IDENT_SSL_CA_2020.crt Policy Level: OVCP Fingerprint: SHA1: C3A6BC49BC9936E9450A9775465B7235E78EE705 SHA256: 007108194115F3C899F54EE67CB4DA87275EDC1D6798DA787E0758CFA6AE96B1 OID: 1.3.6.1.4.1.4788.2.230.2
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

[6] Die SubCA „VR IDENT SSL CA 2020“ wurde gesperrt.

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
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 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 im CA-Zertifikat: 1.3.6.1.4.1.4788.2.200.1 (Legacy)
PCA-1-Verwaltung Siehe Webseite des BSI: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/VerwaltungsPKIVPKI/Wurzelzertifizierungsstelle/FingerprintsderWurzelzertifikate/pcafingerprint.html
D-TRUST V-PKI CA 1 2020 https://www.d-trust.net/cgi-bin/D-TRUST_V-PKI_CA_1_2020.crt bzw. http://x500.bund.de/ Policy Level: V-PKI OID: 0.4.0.127.0.7.3.6.1.1.4.4 (BSI) OID: 1.3.6.1.4.1.4788.2.201.2 (D-TRUST)

Teil der Bundesdruckerei-Gruppe

D-TRUST EV Root CA 1 2020 (ECC) – Aktuell im „CA Root Inclusion" Prozess https://www.d-trust.net/cgi-bin/D-TRUST_EV_Root_CA_1_2020.crt Fingerprint: SHA1: 61DB8C2159690390D87C9C128654CF9D3DF4DD07 SHA256: 08170D1AA36453901A2F959245E347DB0C8D37ABAABC56B81AA100DC958970DB
D-TRUST EV CA 1-20-1 2020 – Aktuell im „CA Root Inclusion" Prozess https://www.d-trust.net/cgi-bin/D-TRUST_EV_CA_1-20-1_2020.crt Policy Level: EVCP Fingerprint: SHA1: 8D01990148D7148C61B3C0B3F743A353F401BA6C SHA256: 41C897473B0369FA74B1F4F9D7F89129485C1A305C0719A867DC8714E0870200 OID: 1.3.6.1.4.1.4788.2.202.1 (D-TRUST EV OID) OID: 2.23.140.1.1 (CA/Browser Forum EV OID)
D-TRUST BR Root CA 1 2020 (ECC) – Aktuell im „CA Root Inclusion" Prozess https://www.d-trust.net/cgi-bin/D-TRUST_BR_Root_CA_1_2020.crt Fingerprint: SHA1: 1F5B98F0E3B5F7743CEDE6B0367D32CDF4094167 SHA256: E59AAA816009C22BFF5B25BAD37DF306F049797C1F81D85AB089E657BD8F0044
D-TRUST BR CA 1-20-1 2020 – Aktuell im „CA Root Inclusion" Prozess https://www.d-trust.net/cgi-bin/D-TRUST_BR_CA_1-20-1_2020.crt Policy Level: OVCP Fingerprint: SHA1: 16407AFD6EE36C777730AE95D6C6286ECE4C389F SHA256: 199AB2AAAFFF40401E0A3B7B87EE9964659EFFA94A1FECBE918AE136E4B4E0A8 OID: 1.3.6.1.4.1.4788.2.202.2 (D-TRUST OV OID) OID: 2.23.140.1.2.2 (CA/Browser Forum OV OID)
D-TRUST BR CA 1-20-2 2020 – Aktuell im „CA Root Inclusion" Prozess https://www.d-trust.net/cgi-bin/D-TRUST_BR_CA_1-20-2_2020.crt Policy Level: DVCP Fingerprint: SHA1: 5714DF60B3F5CA276413244F419C1C61496624A1 SHA256: B268D16934AB5BA232F179CD9F5C7FC07EA8583A56A9A7C1D6CB58FE0823BF5A OID: 1.3.6.1.4.1.4788.2.202.3 (D-TRUST DV OID) OID: 2.23.140.1.2.1 (CA/Browser Forum DV OID)

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[7] 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[7] Fingerprint: SHA1: 643211332169B483B55F7046E56CBFC6C11DC5F8 SHA256: D839672F984DCA7CD480CE201627A4DE61C5C1855F450E5B706200E73A23F047

[7] Der Link wird aktiviert, wenn die CA in der EU Trusted List eingetragen ist und infolgedessen die Inbetriebnahme vorbereitet wird.

Teil der Bundesdruckerei-Gruppe

D-TRUST CA 5-22-1 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-TRUST_CA_5-22-1_2022.crt[7] 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[7] 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
D-Trust SBR Root CA 1 2022 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-Trust_SBR_Root_CA_1_2022.crt Fingerprint: SHA1: 0F523A6B4E7D1D1805A548F94DCDE4C31E1BE9E6 SHA256: D92C171F5CF890BA428019292927FE22F3207FD2B54449CB6F675AF4922146E2
D-Trust SBR CA 1-22-1 2022 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-Trust_SBR_CA_1-22-1_2022.crt Policy Level: NCP Fingerprint: SHA1: 51575F287395A0B53EC2807631ED205134E4AAA9 SHA256: 31FFA8D3F2439C62F2363FE56F4E245382A6D69D8A828B3539FA3875F8C5235B OID: 1.3.6.1.4.1.4788.2.200.3

Teil der Bundesdruckerei-Gruppe

D-Trust SBR CA 1-22-2 2022 (ECC, P-384) https://www.d-trust.net/cgi-bin/D-Trust_SBR_CA_1-22-2_2022.crt Policy Level: LCP Fingerprint: SHA1: C3288BB25E4E49AC4590999BF73875B1D48F6037 SHA256: 200E2C50111A71B07555E921D3BFB7EBDE47F7E41873E06753474362BC017BA2 OID: 1.3.6.1.4.1.4788.2.200.2
D-Trust SBR Root CA 2 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-Trust_SBR_Root_CA_2_2022.crt Fingerprint: SHA1: 27FF63B9EF34293103381AD86060DACC602835E1 SHA256: DBA84DD7EF622D485463A90137EA4D574DF8550928F6AFA03B4D8B1141E636CC
D-Trust SBR CA 2-22-1 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-Trust_SBR_CA_2-22-1_2022.crt Policy Level: NCP Fingerprint: SHA1: 557FFA0723CF6B21B88D2576C13615251E309668 SHA256: CED8E0893E52A1C96AE65D9955A908C45003D7CEADE56B3E4717FD8F00EE0743 OID: 1.3.6.1.4.1.4788.2.200.3
D-Trust SBR CA 2-22-2 2022 (RSA, 4096) https://www.d-trust.net/cgi-bin/D-Trust_SBR_CA_2-22-2_2022.crt Policy Level: LCP Fingerprint: SHA1: 6A1460777BA94726D2215D8853E9AC775A0D9C5A SHA256: 6E87C6E63C8BEE394908B97D1079F8FF88C3930E0EBEC5708C159E2B83247FF0 OID: 1.3.6.1.4.1.4788.2.200.2

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

1.2 Name und Kennzeichnung des Dokuments

Dokumentname:	Certification Practice Statement der D-TRUST CSM PKI
Version	3.8

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (CA)

Diese Regelungen sind im TSPS dokumentiert.

1.3.2 Registrierungsstellen (RA)

Diese Regelungen sind im TSPS dokumentiert.

1.3.3 Zertifikatsnehmer (ZNE) und Endanwender (EE)

Diese Regelungen sind im TSPS dokumentiert.

1.3.4 Zertifikatsnutzer (ZNU)

Diese Regelungen sind im TSPS dokumentiert.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

Diese Regelungen sind im TSPS dokumentiert.

1.4.2 Verbotene Verwendungen von Zertifikaten

Diese Regelungen sind im TSPS dokumentiert.

1.4.3 Verwendung von Dienstezertifikaten

Diese Regelungen sind im TSPS dokumentiert.

1.5 Administration der Policy

1.5.1 Zuständigkeit für das Dokument und Kontaktdaten

Diese Regelungen sind im TSPS dokumentiert.

1.5.2 Meldung von Sicherheitsvorfällen mit Zertifikaten

Diese Regelungen sind in der CP dokumentiert.

1.5.3 Verträglichkeit von CPs fremder CAs mit diesem CPS

Die allgemeinen Regelungen sind im TSPS dokumentiert.

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP

TLS-Zertifikate bzw. deren Sub- sowie Root-CAs kommen den Anforderungen der „Baseline Requirements of the CA/Browser Forum" [BRG] in der Version gemäß den Referenzen in der aktuellen CP der D-Trust GmbH sowie [EN 319 411-1] nach.

Darüber hinaus kommen TLS-Zertifikate bzw. deren Sub- sowie Root-CAs der Policy Level QEVCP-w und EVCP zusätzlich den Anforderungen der „Forum Guidelines for Extended Validation Certificates" [EVGL] in der Version gemäß den Referenzen in der CP 1.6.3 sowie [EN 319 411-2] nach.

Im Falle von Inkonsistenzen zwischen diesem Dokument und den genannten Guidelines gelten vorrangig die [BRG] und [EN 319 411-1] sowie, wenn anwendbar, die [EVGL] und [EN 319 411-2].

QEVCP-w und QNCP-w mit der Ausprägung PSD2

TLS-Zertifikate bzw. deren Sub- sowie Root-CAs kommen den Anforderungen von [EN 319 411-1], [EN 319 411-2] sowie [TS 119 495] nach. Im Falle von Inkonsistenzen zwischen diesem Dokument und den genannten Guidelines gelten vorrangig [EN 319 411-1], [EN 319 411-2] sowie [TS 119 495].

QCP-l

Siegelzertifikate, 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

Diese Regelungen sind in der CP dokumentiert.

1.6.2 Abkürzungen

Certificate Policy (CP)	Zertifikatsrichtlinie.
UPN	User Principal Name

Die weiteren Regelungen sind in der CP dokumentiert.

1.6.3 Referenzen

Diese Regelungen sind in der CP dokumentiert.

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Der Status von Zertifikaten kann mittels OCSP-Abfrage, sofern OCSP angeboten wird, 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.

QCP-l für den digitalen EU Impfnachweis

Eine Statusabfrage der Zertifikate mittels OCSP ist gemäß der [eHealth Network Guidelines] untersagt und wird nicht angeboten.

Die weiteren Regelungen sind in der CP dokumentiert.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Der TSP veröffentlicht folgende Informationen:

- EE-Zertifikate,
- Zertifikatsstatus von TLS 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

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP

Die Zustimmung zur Veröffentlichung von EE-Zertifikaten ist Voraussetzung für ihre Beantragung. Veröffentlichte EE-Zertifikate bleiben bis zum Ende ihrer Gültigkeit sowie mindestens bis zum Ablauf des darauffolgenden Jahres abrufbar.

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.

Die Veröffentlichung findet sofort nach Ausstellung eines Zertifikats statt.

V-PKI

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

CA-Zertifikate werden nach ihrer Erstellung veröffentlicht und:

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

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 Std. 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 name* 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 zum 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.

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

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, QEVCP-w, QNCP-w, EVCP, OVCP, DVCP: Feld wird nicht verwendet NCP, LCP, V-PKI: gemäß dem zur Identifizierung verwendeten Nachweis
SN (surname)	*Familienname* der natürlichen Person QCP-l, QEVCP-w, QNCP-w, EVCP, OVCP, DVCP: Feld wird nicht verwendet NCP, LCP, V-PKI: 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: „Familienname, Rufname". - Juristische Personen: offizielle Bezeichnung der Organisation (Firma, Behörde, Verein etc.), ggf. sinnvolle Abkürzung bei Überschreiten der Zeichenbegrenzung von 64 Zeichen. - Domainnamen: ein FQDN kann in den CN aufgenommen werden. Wenn vorhanden, dann muss dieser zusätzlich als SAN Eintrag hinterlegt werden. - QEVCP-w, QNCP-w, EVCP: Wildcards werden in TLS-Zertifikaten für diese Policy Level nicht verwendet. - OVCP, DVCP: Wildcards können beantragt werden. - Funktion oder Personengruppe: Name der Funktion oder Personengruppe mit der vorangestellten Abkürzung „GRP:" als Hinweis, dass es sich um ein Gruppenzertifikat handelt. - V-PKI: ▪ Funktionszertifikate/Gruppenzertifikate: In der V-PKI werden Zertifikate, die für eine Personengruppe ausgestellt werden, Funktionszertifikate genannt. Wenn die Funktion aus dem CN nicht erkennbar ist, beginnt der Eintrag im CN mit dem Hinweis „FKT:". Der Zertifikatsnehmer ist dafür verantwortlich, dass der private Schlüssel eines Funktionszertifikats aus der V-PKI von maximal 30 Personen gleichzeitig genutzt wird. ▪ Externe Mitarbeiter: In der V-PKI werden Zertifikate, die für externe Mitarbeiter der Organisation des Zertifikatsnehmers ausgestellt werden, durch die Ergänzung „Ext.:" am Anfang des CN kenntlich gemacht. - Technische Komponenten: Name des Servers, des Dienstes oder der Applikation, der/die das Zertifikat benutzt.

DN-Bestandteil	Interpretation
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. V-PKI: Der SAN kann mit otherName und darin enthaltenem User Principal Name (UPN) oder der Angabe einer RegisteredID belegt werden. Sonderfall: ein oder mehrere Domainnamen können ebenfalls in den SAN aufgenommen werden. QEVCP-w, QNCP-w, EVCP: Wildcards werden in TLS-Zertifikaten für diese Policy Level nicht verwendet. OVCP, DVCP: Wildcards können beantragt werden.
PN (Pseudonym)	*Pseudonym*: ist identisch zu CN. V-PKI: Es werden keine Pseudonyme vergeben.
Serial Number (serialNumber) (2.5.4.5)	*Seriennummer*: Namenszusatznummer, welche die Eindeutigkeit des Namens sicherstellt (i.d.R. die Antragsnummer). Sonderfall bei EV-Zertifikaten gemäß [EVGL]: Registernummer falls vergeben, Datum der Registrierung oder Gründung. Wenn bei Behörden (Government Entity) keine Registernummer oder Gründungsdatum ermittelbar ist, wird das Feld mit dem Text „Government Entity" befüllt. 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. **EVCP:** Wird im Feld O ein Markenname aufgenommen, so muss der Organisationsname in Klammern gemäß Abschnitt 9.2.1 [EVGL] dahinter aufgeführt werden. **OVCP:** Wird im Feld O ein Markenname aufgenommen, so müssen die Vorgaben aus Abschnitt 7.1.4.2.2 (b) [BRG] eingehalten werden. **DVCP:** Feld wird nicht verwendet

DN-Bestandteil	Interpretation
OU (organizationalUnit Name) (2.5.4.11)	Organisationseinheit der Organisation, wie z.B. Abteilung, Bereich oder andere Unterteilung oder QEVCP-w, QNCP-w: Markenname der Organisation EVCP, OVCP: Markenname der Organisation (Feld wird für EVCP und OVCP ab 01.09.2022 nicht mehr verwendet) DVCP: Feld wird nicht verwendet
OrgID (organizationIdentifier) (2.5.4.97)	**LCP (Seal ID):** *Eindeutige Organisationsnummer* der Organisation. Es kann die Nummer des Handelsregistereintrags sowie die Umsatzsteueridentnummer oder eine von D-Trust vergebene Nummer eingetragen werden. Die von D-Trust vergebene Nummer ist an das Format gemäß Variante 3 aus Kapitel 5.1.4 der EN 319 412-1 angelehnt und setzt sich wie folgt zusammen: DT:DE-1234567890 (DT: D-Trust; DE: Deutschland; zufällige Nummer, die der Organisation eindeutig zugeordnet wird). **QEVCP-w, EVCP, OVCP, DVCP:** Feld wird nicht verwendet. **QCP-l, QEVCP-w und QNCP-w mit der Ausprägung PSD2:** *PSD2 Authorisation Number* Bei Zertifikaten, die im Rahmen des PSD2-Verfahrens gemäß [TS 119 495] eingesetzt werden, ist das Setzen des organization identifiers (2.5.4.97) verpflichtend. Die Eindeutigkeit wird über die „Authorisation Number" gewährleistet. Die „Authorisation Number" besteht aus den Zeichen: **PSD<cc>-<x..x>-<y..y>** Wobei "PSD" - "legal person identity type", enthält 3 Zeichen; <cc> ISO 3166 Ländercode der nationalen zuständigen Behörde (NCA) - genau 2 Zeichen Hyphen-minus „-„ <x..x> Identifikator der NCA - 2 - 8 Großbuchstaben A – Z, keine Leerzeichen Hyphen-minus „-„ <y..y> Identifikator des Zahlungsdienstleisters, wie von der NCA festgelegt - Beliebige Zeichenfolge Beispiel: PSDDE-BAFIN-1234Ab

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. EVCP: gemäß Abschnitt 9.2.6 [EVGL] DVCP: Feld wird nicht verwendet
Street (streetAddress) (2.5.4.9)	Postalische Adresse *Straße und Hausnummer* EVCP: gemäß Abschnitt 9.2.6 [EVGL] DVCP: Feld wird nicht verwendet
Locality (localityName) (2.5.4.7)	Postalische Adresse *Ort* EVCP: gemäß Abschnitt 9.2.6 [EVGL] DVCP: Feld wird nicht verwendet
State (stateOrProvinceName) (2.5.4.8)	Postalische Adresse *(Bundes-)Land* EVCP: gemäß Abschnitt 9.2.6 [EVGL] DVCP: Feld wird nicht verwendet
PostalCode (postalCode) (2.5.4.17)	Postalische Adresse *Postleitzahl* EVCP: gemäß Abschnitt 9.2.6 [EVGL] DVCP: Feld wird nicht verwendet
BusinessCategory (businessCategory) (2.5.4.15)	Business Category gemäß [EVGL] Wird nur bei EVCP verwendet. Das Feld „businessCategory" muss eines der folgenden Werte enthalten: "Private Organization", "Government Entity", "Business Entity" oder "Non-Commercial Entity".
Jurisdiction Of Incorporation Locality (jurisdictionLocalityName)	Gerichtsstand der Organisation gemäß [EVGL]: *Ort* (1.3.6.1.4.1.311.60.2.1.1) Wird nur bei EVCP und wenn es gemäß der Ebene der tatsächlichen Registrierung anwendbar ist, verwendet.
Jurisdiction Of Incorporation State Or Province Name (jurisdictionStateOrProvinceName)	Gerichtsstand der Organisation: *(Bundes-)Land* (1.3.6.1.4.1.311.60.2.1.2) Wird nur bei EVCP und wenn es gemäß der Ebene der tatsächlichen Registrierung anwendbar ist, verwendet.

DN-Bestandteil	Interpretation
Jurisdiction Of Incorporation CountryName (jurisdictionCountry Name)	Gerichtsstand der Organisation gemäß [EVGL]: *Land* (1.3.6.1.4.1.311.60.2.1.3) Wird nur bei EVCP und wenn es gemäß der Ebene der tatsächlichen Registrierung anwendbar ist, verwendet.

Weitere Regelungen sind in der TSPS in Abschnitt 7.1.4 dokumentiert.

QEVCP-w, QNCP-w[8], EVCP

TLS-Zertifikate enthalten mindestens die subject-DN-Bestandteile „organizationName", „commonName", „serialNumber", "jurisdictionCountryName" „localityName", "streetAddress", „countryName", „postalCode", "businessCategory" sowie „subjectAltName".

TLS-Zertifikate dürfen nur die subject-DN-Bestandteile enthalten, die in Abschnitt 9.2 [EVGL] definiert sind.

QCP-l

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 der über den CSM bereitgestellten 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).

QEVCP-w, QNCP-w, EVCP

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

[8] Bei QEVCP-w und QNCP-w Zertifikaten mit der Ausprägung PSD2 wird der "organizationIdentifier" zusätzlich gesetzt und geprüft.

QEVCP-w, QNCP-w, EVCP, OVCP

Der TSP unternimmt notwendige Schritte, um sicherzustellen, dass zum Zeitpunkt der Ausstellung des Zertifikates, der Antragsteller nachweislich das Recht hat, den im Zertifikat aufgenommene Markennamen zu nutzen. Die Vorgaben aus Abschnitt 3.2.2.2 [BRG] ggf. Abschnitt 11.3 [EVGL] werden eingehalten.

3.2 Initiale Überprüfung der Identität

Es ist ein Verfahren etabliert, das sicherstellt, dass die Datenquellen zur Validierung von Zertifikatsinhalten gemäß Abschnitt 3.2.2.7 [BRG] geprüft und freigegeben werden. Alle Datenquellen sind von der D-Trust Organisationseinheit für Informationssicherheit freigegeben.

D-Trust qualifiziert und verwendet Qualifizierte Unabhängige Informationsquellen (QIIS) gemäß Abschnitt 11.11.5 [EVGL]. QIIS ist ein Teil des Prüfverfahrens „Register" in Abschnitt 4.2.1 des TSPS.

Es ist ein Verfahren etabliert, das sicherstellt, dass der Antragsteller über eine verifizierte Kommunikationsmethode gemäß 11.5 [EVGL] zuverlässig kontaktiert werden kann und darüber bestätigen kann, dass er die Anfrage kennt und diesem zustimmt.

3.2.1 Nachweis für den Besitz des privaten Schlüssels

Es werden zwei Fälle unterschieden:

a) Schlüsselpaare von Zertifikatsnehmern werden im Verantwortungsbereich des TSP produziert. Mit der Übergabe der verschlüsselten Token oder verschlüsselten Soft-PSE 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.
Wird nicht angeboten für QEVCP-w, QNCP-w, EVCP, OVCP, DVCP und V-PKI.

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

3.2.2 Identifizierung und Authentifizierung von Organisationen und Domains

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

Für die Teilnehmeridentifizierung und die Antragsprüfung gelten die Vorgaben aus [EN 319 411-1] je nach Anwendbarkeit NCP, LCP, EVCP, OVCP oder DVCP bzw. aus [EN 319 411-1] und [EN 319 411-2] für QEVCP-w, QNCP-w oder QCP-l. 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.

	QEVCP-w, EVCP	QEVCP-w und QNCP-w mit PSD2	OVCP	DVCP	QCP-l	LCP	NCP[9]
CN	Register/ Non-Register/ Domain/ CAA	Register/ Non-Register/ Domain/ CAA	Register/ Non-Register/ Domain/ CAA	Domain	Register/ Non-Register	HR-DB/ Register/ Non-Register	Register/ Non-Register
C	Register/ Non-Register/ Domain	Register/ Non-Register/ Domain	Register/ Non-Register/ Domain	n.a.		Register/ Non-Register	Register/ Non-Register
O				n.a.			
OrgID	n.a.	Register	n.a.	n.a.	Register	n.a.	n.a.
OU[10]	Z-Bestätigung/ A-Bestätigung/ Register	Z-Bestätigung/ A-Bestätigung/ Register	Z-Bestätigung/ A-Bestätigung/ Register	n.a.	Z-Bestätigung/ A-Bestätigung/ Register	Z-Bestätigung/ A-Bestätigung	Z-Bestätigung/ A-Bestätigung/
STREET	Register/ Non-Register	Register/ Non-Register	Register/ Non-Register	n.a.	Register/ Non-Register	n.a.	n.a.
L				n.a.		n.a.	n.a.
State				n.a.		n.a.	n.a.
PostalCode				n.a.		n.a.	n.a.
Alternativer Antragsteller (SAN)	Domain/ CAA	Domain/ CAA	Domain/ CAA	Domain/ CAA	n.a.	Domain/ E-Mail/ HR-DB	Domain/ CAA/ E-Mail/ HR-DB

[9] Gilt nur für Organisations- und Maschinenzertifikate, außer für TLS-Zertifikate.

[10] Für EVCP, OVCP, DVCP, LCP und NCP wird perspektivisch das Feld „OU" entfallen.

Teil der Bundesdruckerei-Gruppe

	QEVCP-w, EVCP	QEVCP-w und QNCP-w mit PSD2	OVCP	DVCP	QCP-l	LCP	NCP[9]
Alle weiteren Attribute	n.a.	n.a.	n.a.	n.a.	n.a.	A-Bestätigung/ Dok-Ident/ out-of-band mechanisms	A-Bestätigung/ Dok-Ident/ out-of-band mechanisms.
Business Category (businessCategory)	**Private Organization** Register **Government Entity** Register/ Non-Register **Business Entity** Register in Verbindung mit Pers-Ident **Non-Commercial Entity** Non-Register/ Z-Bestätigung	Nur für QEVCP-w: **Private Organization** Register **Government Entity** Register/ Non-Register **Business Entity** Register in Verbindung mit Pers-Ident **Non-Commercial Entity** Non-Register/ Z-Bestätigung	n.a.	n.a.	n.a.	n.a.	n.a.

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, für fortgeschrittene Organisations- und Maschinenzertifikate (außer TLS-Zertifikate) gemäß NCP und für Webseitenzertifikate gemäß QEVCP-w, QNCP-w und EVCP.

Es ist ein Verfahren etabliert, das sicherstellt, dass die operative Existenz des Antragstellers (juristische Person) gemäß 11.6 [EVGL] zuverlässig geprüft wird.

D-Trust bezieht ihre Informationen von verschiedenen „Registerführenden Stellen" (Registration Agency oder Incorporating Agency) gemäß des Prüfverfahrens „Register" im Abschnitt 4.2.1 des TSPS, die in einer Tabelle im Repository veröffentlicht ist:

https://www.d-trust.net/internet/files/D-TRUST_Agency-Information.pdf

Relevante Informationen zum Zertifikat, die den Registerauszügen entnommen sind, werden genauso in die Zertifikatsfelder 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 authentifizieren und ggf. ihre Berechtigung zur Antragstellung durch die Organisation nachweisen.

NCP, LCP, V-PKI

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

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

	V-PKI	LCP	NCP
G	Pers-Ident/ eID	HR-DB/ Dok-Ident/ Pers-Ident/ eID	HR-DB/ Pers-Ident/ eID
SN			
CN	Register/Non-Register	HR-DB/Register/Non-Register	HR-DB/Register/ Non-Register
C	DE	Register/ Non-Register	Register/ Non-Register
O	Register/Non-Register	Register/Non-Register	Register/Non-Register
OU	Z-Bestätigung/A-Bestätigung	Z-Bestätigung/ A-Bestätigung	Z-Bestätigung/ A-Bestätigung
STREET	n.a.	n.a.	n.a.
L			
State			
PostalCode			
Alternativer Antragsteller (SAN)	E-Mail	Domain/E-Mail/HR-DB	Domain/ CAA/ E-Mail/ HR-DB
Alle weiteren Attribute	n.a.	A-Bestätigung/ Dok-Ident/ out-of-band mechanisms	A-Bestätigung/ out-of-band mechanisms

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

Nachweise in nicht lateinischer Schrift werden nicht akzeptiert.

3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Die Angaben des Zertifikatsnehmers werden entsprechend den Abschnitten 3.2.2, 3.2.3 und 4.2.1 geprüft bzw. nicht geprüft.

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, LCP, NCP
Alle Angaben im Zertifikat werden verifiziert.

V-PKI
Gemäß TSPS 7.1.2 können EE-Zertifikate die unkritische Zertifikatserweiterung subjectAltName enthalten. In EE-Zertifikaten aus der V-PKI darf das Zertifikatsfeld subjectAltName mit otherName und darin enthaltenem User Principal Name (UPN) oder der Angabe einer RegisteredID belegt werden. Diese Angaben in der subjectAltName-Erweiterung werden innerhalb der Organisation des Zertifikatsnehmers genutzt und werden vom TSP nicht geprüft.

Bei alternativen Namen werden generell nur die E-Mail-Adressen bzw. deren Domainbestandteile geprüft. Andere Zertifikatsinhalte wie z.B. LDAP-Verzeichnisse etc. sowie eventuelle Zertifikats-Extensions (AdditionalInformation, monetaryLimit, etc.) werden nicht auf Korrektheit geprüft.

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

3.2.5 Prüfung der Berechtigung zur Antragstellung

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

Bei Organisationen wird der Existenznachweis sowie die Vertretungsberechtigung eines Zeichnungsberechtigten nach Abschnitt 3.2.2 geprüft bzw. bestätigt. Weiterhin wird mindestens ein 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. Schlüsselerneuerungen werden nur für OVCP-, DVCP-, V-PKI-, NCP- und LCP-Zertifikate, aber nicht für TLS-Zertifikate gemäß EVCP, QEVCP-w oder QNCP-w angeboten. Bei diesen Zertifikaten muss der gesamte Identifizierungs- und Registrierungsprozess wie bei einem Erstantrag durchlaufen werden, ggf. können aber bereits vorliegende Nachweisdokumente wiederverwendet werden, wenn sie nach [EVGL] noch verwertbar sind.

3.3.1 Routinemäßige Anträge zur Schlüsselerneuerung

Bei Anträgen zur Schlüsselerneuerung ist keine erneute Identifizierung erforderlich, so lange die beim TSP hinterlegten Nachweise noch verwertbar sind. Die Verwendung bereits validierter Daten ist auf 397 Tage begrenzt. Anschließend muss eine neue Validierung durchgeführt werden. Der Auftrag zur Schlüsselerneuerung muss elektronisch über die vereinbarte Schnittstelle übertragen werden.

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

3.3.2 Schlüsselerneuerung nach Widerruf eines Zertifikats

Schlüsselerneuerung auf Basis eines widerrufenen Zertifikats wird nicht angeboten.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Sperrberechtigung wird wie folgt geprüft:

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

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

NCP, LCP, V-PKI

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

Sperrverfahren werden in Abschnitt 4.9 definiert.

4. Betriebsanforderungen

4.1 Zertifikatsantrag und Registrierung

4.1.1 Berechtigung zur Antragstellung

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

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

QEVCP-w, EVCP

Zertifikatsnehmer müssen den Anforderungen aus [EVGL] entsprechen.

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

4.1.2 Registrierungsprozess und Zuständigkeiten

Die allgemeinen Regelungen sind in dem TSPS dokumentiert.

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

Für das Policy Level OVCP gilt zusätzlich zur TSPS folgende Regelung:
Der Kunde hat in CSM die Option ein OVCP Produkt mit oder ohne CT-Logging auszuwählen.

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Die allgemeinen Regelungen sind im TSPS dokumentiert.

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

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

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

4.2.2 Annahme oder Ablehnung von 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 CSM CPS folgende spezifische Regelungen:

EVCP, QEVCP-w, OVCP, DVCP
Die D-Trust GmbH verwendet bei der Ausstellung von TLS-Zertifikaten Certificate Transparency (CT) gemäß RFC 6962. Einige Browser verpflichten zur Veröffentlichung aller durch die CA ausgestellten TLS-Zertifikate in mindestens drei revisionssicheren Logs externer Anbieter.

Dies gilt nur, wenn das Produkt mit CT-Logging angeboten wird und im Bestellprozess entsprechend ausgewählt wurde.

Bei TLS-Zertifikaten wird ein Pre-Issuance Linting durchgeführt.

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

NCP, LCP

Zertifikate, deren privater Schlüssel im Bereich des TSP erstellt wurde, werden mittels zugriffsgeschütztem und TLS-verschlüsseltem Download bzw. TLS-geschützter Schnittstelle (CSM) oder per E-Mail bereitgestellt (die PKCS#12-Datei ist mit einer PIN geschützt).

V-PKI

Zertifikate werden mittels zugriffsgeschütztem und TLS-verschlüsseltem Download bzw. TLS-geschützter Schnittstelle (CSM) oder per E-Mail bereitgestellt. Es werden ausschließlich Zertifikate erstellt, deren privater Schlüssel durch den Antragsteller erzeugt wurde.

QCP-l, QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP

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.

Kundenspezifisch können abweichende Verfahren vereinbart werden.

Die allgemeinen Regelungen sind im TSPS dokumentiert.

4.4.2 Veröffentlichung des Zertifikats durch den TSP

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

Der Status ist nach Produktion über OCSP abrufbar.

V-PKI

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

QCP-l für den digitalen EU Impfnachweis

Eine Statusabfrage der Zertifikate mittels OCSP ist gemäß der [eHealth Network Guidelines] untersagt und wird nicht angeboten.

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-l, QEVCP-w, QNCP-w

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.

Eine Zertifikatserneuerung wird im Rahmen des Antragsweges CSM nicht angeboten.

Beim Antragsweg CSM bezieht der Antragsteller die Zertifikate über eine online Schnittstelle. Die im System hinterlegten Registrierungs- und Identifizierungsdaten der Organisation und ihrer Bevollmächtigten (Vertragsunterzeichner, Technischer Ansprechpartner und Operatoren) werden unabhängig von der Laufzeit ihrer Zertifikate, jährlich revalidiert und sind somit jederzeit für weitere Zertifikatsanträge verwendbar.

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

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.

4.8 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.

Teil der Bundesdruckerei-Gruppe

4.9.2 Berechtigung zum Widerruf

Diese Regelungen sind im TSPS dokumentiert.

4.9.3 Verfahren für einen Sperrantrag

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

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

Ein telefonischer Widerruf von Zertifikaten wird nicht angeboten.

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 von dem Sperrantragsteller angegebenen Sperrgründe werden dokumentiert. Nach erfolgter Sperrung wird der Zertifikatsnehmer bzw. der Endanwender über die Sperrung informiert. Die Information des Endanwenders kann durch den Zertifikatsnehmer erfolgen, wenn dies vereinbart wurde.

Die Authentifizierung der Sperrberechtigten erfolgt gemäß Abschnitt 3.4.

PSD2 spezifisches Sperrverfahren

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

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

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

4.9.4 Fristen für einen Sperrantrag

Diese Regelungen sind im TSPS dokumentiert.

4.9.5 Zeitspanne für die Bearbeitung des Sperrantrags durch den TSP

Sperranträge können 24x7 über die Online-Schnittstelle eingereicht werden. Der Widerruf erfolgt gemäß Abschnitt 4.9 [BRG].

Teil der Bundesdruckerei-Gruppe

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Aktuelle Sperrinformationen sind in Sperrlisten vorgehalten, die über das Protokoll LDAP[11] 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.

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

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 einer URL in den Zertifikaten angegeben.

V-PKI, QCP-l für den digitalen EU Impfnachweis

Im Rahmen der V-PKI und der digitalen EU Impfnachweise werden Sperrlisten erstellt. Die CRL ist in den Zertifikaten in Form einer URL angegeben. Der OCSP Dienst zur Statusabfrage wird nicht angeboten.

4.9.10 Notwendigkeit zur Online-Prüfung von Sperrinformationen

Diese Regelungen sind im TSPS dokumentiert.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Diese Regelungen sind im TSPS dokumentiert.

---

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

Teil der Bundesdruckerei-Gruppe

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Diese Regelungen sind im TSPS dokumentiert.

4.9.13 Bedingungen für eine Suspendierung

Diese Regelungen sind im TSPS dokumentiert.

4.10 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 Schlüsselwiederherstellung

Schlüsselhinterlegung wird nicht vom TSP angeboten. Dem Subscriber steht es frei, Schlüssel im eigenen Verantwortungsbereich zu hinterlegen.

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel

Schlüsselhinterlegung wird nicht vom TSP angeboten.

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Schlüsselhinterlegung wird nicht vom TSP angeboten.

5. Nicht-technische Sicherheitsmaßnahmen

Die 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.

Teil der Bundesdruckerei-Gruppe

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 von Risiken

Diese Regelungen sind im TSPS dokumentiert.

Teil der Bundesdruckerei-Gruppe

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.

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

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP

Der Zertifikatsnehmer darf eine Zertifikatsanfrage nur mit einem neuen, selbst erzeugten Schlüsselpaar stellen. Dies gilt insbesondere für EE-Server-Zertifikatsanfragen. Wenn der TSP feststellt, dass das neue Zertifikat mit dem gleichen Schlüsselpaar angefragt wird und/oder zur Zertifikatsanfrage ein Schlüsselpaar verwendet wird bei der eine oder mehrere der Bedingungen aus Abschnitt 6.1.1.3 [BRG] zutreffen, wird die Zertifikatsanfrage abgelehnt.

V-PKI

Der Zertifikatsnehmer darf eine Zertifikatsanfrage nur mit einem neuen, selbst erzeugten Schlüsselpaar stellen und ist bei Projekten der Bundesregierung verpflichtet bei der Erzeugung von EE-Schlüsseln diese nach den Vorgaben aus BSI [TR-02102-1] kryptographisch sicher zu erzeugen.

Werden EE-Schlüssel vom TSP erzeugt, werden diese mit Hilfe eines HSMs in der sicheren Umgebung des Trustcenters erzeugt und entsprechen den Vorgaben aus [EN 319 411-1] und [EN 319 411-2].

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

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP, V-PKI

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.

Teil der Bundesdruckerei-Gruppe

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.

V-PKI

Für die Schlüsselgenerierung und Speicherung wird das HSM „Utimaco CP5 SE 500" Version 5.1.0.0 verwendet.

NCP, LCP

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

6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m)

Das HSM, auf dem die CA-Schlüssel aufbewahrt werden, befindet sich in der sicheren Umgebung des Trustcenters. Die Aktivierung des privaten Schlüssels erfordert zwei autorisierte Personen.

Ein Zugriff auf private EE-Schlüssel besteht nur im Fall von Schlüsselhinterlegung gemäß Abschnitt 6.2.3.

6.2.3 Hinterlegung privater Schlüssel (key escrow)

Private EE-Schlüssel werden vom TSP nicht hinterlegt.

6.2.4 Backup privater Schlüssel

Die allgemeinen Regelungen sind im TSPS dokumentiert.

Für private EE-Schlüssel wird kein Backup angeboten, eine Sicherung erfolgt nur im Rahmen der Hinterlegung (key escrow), wenn diese produktspezifisch verfügbar ist oder vereinbart wurde.

6.2.5 Archivierung privater Schlüssel

Diese Regelungen sind im TSPS dokumentiert.

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Diese Regelungen sind im TSPS dokumentiert.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Die allgemeinen Regelungen sind im TSPS dokumentiert.

EE-Schlüssel liegen bis zur Auslieferung verschlüsselt in einer Datenbank des TSP vor.

6.2.8 Aktivierung privater Schlüssel

Die allgemeinen Regelungen sind im TSPS dokumentiert.

Private EE-Schlüssel werden durch Eingabe des Geheimnisses aktiviert.

6.2.9 Deaktivieren privater Schlüssel

Die allgemeinen Regelungen sind im TSPS dokumentiert.

Die jeweilige Anwendung deaktiviert den privaten EE-Schlüssel, spätestens aber durch das Deaktivieren oder Löschen des Soft-PSEs.

6.2.10 Zerstörung privater Schlüssel

Die allgemeinen Regelungen sind im TSPS dokumentiert.

Schlüssel, die im Bereich des TSPs erstellt wurden, werden nach Auslieferung automatisch gelöscht.

6.2.11 Beurteilung kryptographischer Module

Diese Regelungen sind im TSPS dokumentiert.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Diese Regelungen sind im TSPS dokumentiert.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die allgemeinen Regelungen sind im TSPS dokumentiert.

Die Gültigkeitsdauer der EE-Schlüssel und Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximal mögliche Gültigkeitsdauer beträgt:

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP

Bis einschließlich 31.08.2020 werden TLS-Zertifikate mit folgender Gültigkeitsdauer ausgestellt:

Max. 825 Tage

Seit 01.09.2020 werden TLS-Zertifikate mit folgender Gültigkeitsdauer ausgestellt:

Max. 398 Tage

In 2022 wurde die maximale Gültigkeitsdauer um einen Tag reduziert. TLS-Zertifikate werden nun mit folgender Gültigkeitsdauer ausgestellt:

Max. 397 Tage

Teil der Bundesdruckerei-Gruppe

QEVCP-w und QNCP-w mit der Ausprägung PSD2

Qualifizierte Webseitenzertifikate mit der Ausprägung PSD2 werden mit folgender Gültigkeitsdauer ausgestellt:

Max. 397 Tage

V-PKI

Max. 27 Monate

NCP, LCP

Max. 63 Monate

QCP-l

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

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.

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

NCP, LCP

Erzeugt der TSP die EE-Schlüssel, wird entweder die PIN in einem PIN-Brief an den Zertifikatsnehmer versandt bzw. übergeben oder dem Zertifikatsnehmer über eine gesicherte TLS-Verbindung bzw. Onlineschnittstelle zur Verfügung gestellt.

NCP, LCP, V-PKI

Der Zertifikatsnehmer ist für die sichere Zustellung der PIN an den Endanwender verantwortlich, wenn Zertifikatsnehmer und Endanwender voneinander abweichen.

6.4.2 Schutz von Aktivierungsdaten

Die allgemeinen Regelungen sind im TSPS dokumentiert.

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

6.4.3 Andere Aspekte von Aktivierungsdaten

Keine Vorgaben.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Diese Regelungen sind im TSPS dokumentiert.

6.5.2 Beurteilung von Computersicherheit

Diese Regelungen sind im TSPS dokumentiert.

Teil der Bundesdruckerei-Gruppe

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 der 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, DVCP)

Teil der Bundesdruckerei-Gruppe

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

- secp384r1 mit OID 1.3.132.0.34
- secp521r1 mit OID: 1.3.132.0.35[12]
- secp256r1 mit OID: 1.2.840.10045.3.1.7

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

- sha512 WithRSAEncryption mit OID 1.2.840.113549.1.1.13
- sha256 WithRSAEncryption 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.

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP
Die Vorgaben aus Abschnitt 7.1.3.2 [BRG] werden eingehalten.

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 von CertificatePolicies

Diese Regelungen sind im TSPS dokumentiert.

[12] Diese Kurve wird nicht verwendet für EVCP, OVCP, DVCP, LCP und NCP.

Teil der Bundesdruckerei-Gruppe

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.

Teil der Bundesdruckerei-Gruppe