Certification Practice Statement of the D-TRUST Cloud PKI

ENGLISH

DEUTSCH

Teil der Bundesdruckerei-Gruppe

Certification Practice Statement of the D-TRUST Cloud PKI

Version 3.5

Teil der Bundesdruckerei-Gruppe

Copyright Notice and License

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

This work is licensed under a 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	2017-01-01	▪ Introduction of remotely triggered signatures as a non-qualified trust service according to EN 319 411-1
2.0	2017-04-01	▪ Introduction of remote qualified signatures as a qualified trust service according to EN 319 411-2 ▪ Introduction of a qualified time-stamp service as a qualified trust service according to EN 319 421
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	▪ OrgID field in section 3.1.4 was amended according to variant 3 in section 5.1.4 of EN 319 412-1 ▪ Editorial changes
2.4	2018-10-11	▪ Table listing CA certificates in section 1.1.3 ▪ Amendments in section 7.3 ▪ Adaptation of sections 1.5.2 and 4.9 according to SC6v3 Ballot from the CAB Forum
2.5	2018-11-30	▪ This CPS complies with the requirements of Mozilla Policy 2.6.1 ▪ Full annual review of the CPS ▪ Editorial changes
2.6	2019-10-09	▪ Update according to the CAB's observation report ▪ Editorial changes
2.7	2020-03-19	▪ This CPS complies with the requirements of Mozilla Policy 2.7 ▪ Full annual review of the CPS ▪ Adjustment of the archiving period for LCP in section 5.5.2 ▪ SHA-256 fingerprints added in section 1.1.3 ▪ Editorial changes and more detailed information in sections 5.2.1, 6.6 and 7.2.2
2.8	2020-04-27	▪ Amendments to certificate chain verification in section 4.5.2 ▪ Amendments in sections 5.3.7 and 5.5.2
3.0	2020-11-10	▪ From version 3 or higher, the Cloud CPS is subordinate to the TSPS ▪ Update according to observation report
3.1	2021-06-22	▪ Introduction of the new CAs for QCP-n-qscd and BTSP in section 1.1.3 ▪ Link replaced in section 1.1.3 ▪ Full annual review of the CPS ▪ Editorial changes in section 7.1.3
3.2	2021-12-06	▪ Announcement of the go-live of the new CA for QCP-n-qscd, see section 1.1.3 ▪ Amendments in sections 7.1.2 ▪ More detailed information in sections 3.1.4 and 3.2.3

Version	Date	Description
3.3	2022-07-01	▪ Amendments and editorial changes in sections 1.1.3, 2.3, 4.3.2, 4.7, 6.2.6, 6.3.2 and 6.8 ▪ Full annual review of the CPS
3.4	2022-11-14	▪ Introduction of the QCP-l-qscd policy level
3.5	2022-12-22	▪ See section 1.1.3 for the introduction of the issuing CA for the trust service "D-Trust remote seal service (seal-me)" with policy level QCP-l-qscd.

Contents

1. Introduction 7
1.1 Overview 7
1.2 Document name and identification 11
1.3 PKI entities 11
1.4 Certificate usage 12
1.5 Policy administration 12
1.6 Definitions and acronyms 13
2. Publication and Repository Responsibility 13
2.1 Repositories 13
2.2 Publication of certificate information 13
2.3 Publication frequency 13
2.4 Repository access control 14
2.5 Access to and use of services 14
3. Identification and Authentication 14
3.1 Naming 14
3.2 Initial identity verification 16
3.3 Identification and authentication for re-keying requests 17
3.4 Identification and authentication of revocation requests 18
4. Operational Requirements 18
4.1 Certificate request and registration 18
4.2 Processing the certificate request 18
4.3 Certificate issuance 19
4.4 Certificate handover 19
4.5 Key pair and certificate usage 20
4.6 Certificate renewal 20
4.7 Certificate renewal with re-keying 20
4.8 Certificate modification 20
4.9 Certificate revocation and suspension 21
4.10 Certificate status services 22
4.11 Withdrawal from the certification service 23
4.12 Key escrow and recovery 23
5. Facility, Management and Operational Controls 23
5.1 Physical controls 23
5.2 Procedural controls 23
5.3 Personnel controls 23
5.4 Audit logging procedures 24
5.5 Records archival 24
5.6 Key change at the TSP 24
5.7 Compromise and disaster recovery at the TSP 25
5.8 Closure of the TSP or termination of services 25
6. Technical Security Controls 25
6.1 Key pair generation and installation 25
6.2 Private key protection and cryptographic module engineering controls 26
6.3 Other aspects of key pair management 27
6.4 Activation data 27
6.5 Computer security controls 28
6.6 Life cycle technical controls 28
6.7 Network security controls 28
6.8 Time stamps 28
7. Profiles of Certificates, Certificate Revocation Lists and OCSP 29
7.1 Certificate profiles 29
7.2 CRL profiles 30
7.3 OCSP profiles 30

Teil der Bundesdruckerei-Gruppe

8. Compliance Audit and Other Assessment 30
9. Other Business and Legal Matters.....30

Teil der Bundesdruckerei-Gruppe

1. Introduction

1.1 Overview

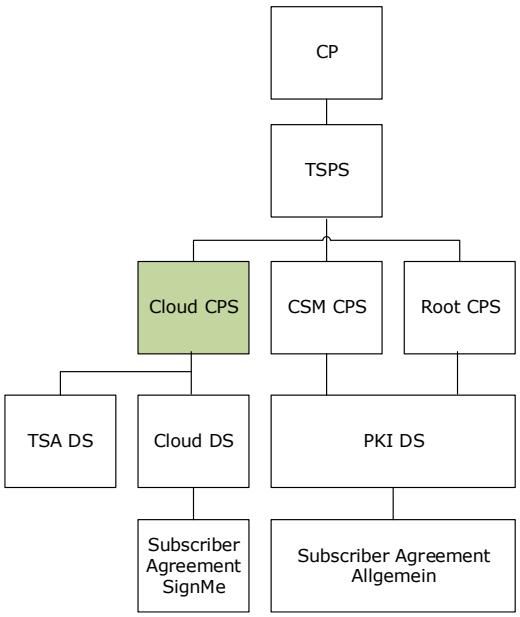
This document is the Certification Practice Statement (CPS) of the trust services operated by D-Trust GmbH which use the D-TRUST Cloud PKI. The document name is abbreviated as **Cloud CPS** and is subject to the Trust Service Practice Statement of D-TRUST (abbreviated as TSPS) and the Certificate Policy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

1.1.1 Trust service provider

These rules are laid down 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 [EN 319 412] and describes the implementation of the resultant requirements.

Unless this document distinguishes between the certification requirements or certification levels according to section 1.1.3 or unless certain certification 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.

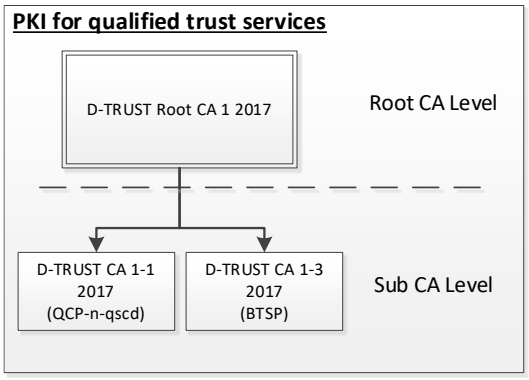
The structure of this document is based on the RFC 3647 Internet standard: *"Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework"*.

1.1.3 Properties of the PKI

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

The private keys of the EE certificates are exclusively generated and stored under the responsibility of the TSP.

Currently valid PKI hierarchy for qualified trust services[1]



[1] The "D-TRUST CA 1-21-2 2022" sub-CA is created, but is not yet operational. The publication of the sub-CA in the Federal Network Agency's Trusted List is applied, and will be put into operation after its publication.

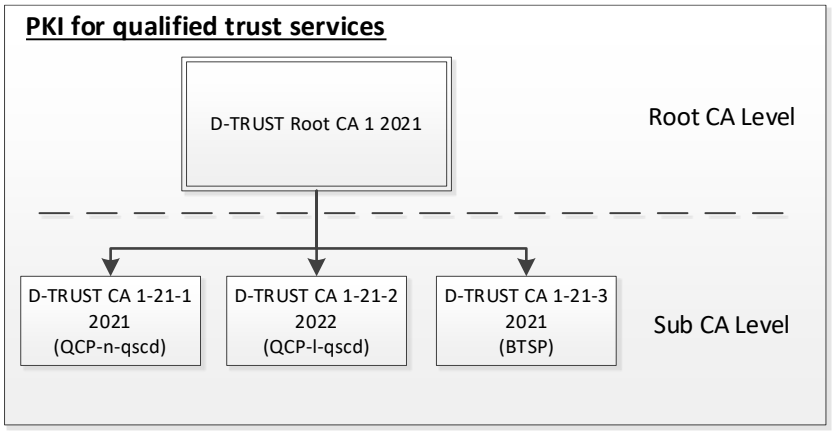


Fig. 1: PKI hierarchy for qualified trust services[2]

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

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

QCP-l-qscd – Qualified seal certificates on a qualified seal device

Depending on their features, the service certificates for time stamps can be assigned to the requirements of [EN 319 421]:

BTSP – Qualified time-stamp service

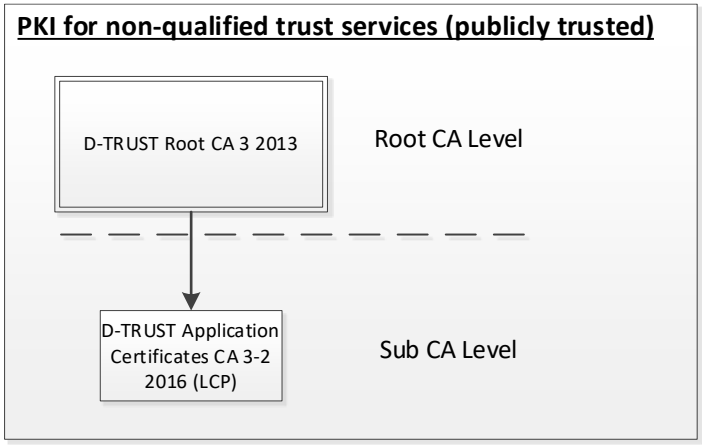


Fig. 2: PKI hierarchy for non-qualified trust services

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

LCP – Lightweight Certificate Policy

The policy levels are explained in the TSPS.

[2] The sub-CA "D-TRUST CA 1-21-1 2021" is included in the Federal Network Agency's Trusted List and has been put into operation. Certificates will only be issued from the new SubCA "D-TRUST CA 1-21-1 2021". The "D-TRUST CA 1-21-3 2021" subCA has been created but is not yet in operation. The next TSU certificate (D-TRUST qualified timestamp) will be issued from the "D-TRUST CA 1-21-3 2021". Looking to the future, the "D-TRUST Root CA 1 2021" will replace the " D-TRUST Root CA 1 2017".

CA certificates

The complete overview of all root CAs and sub-CAs with certification levels QCP-w, EVCP, OVCP, DVCP and LCP, showing which CPS 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 CA 1 2017 https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_1_2017.crt Fingerprint: SHA1: 3FE69767C9B3E938CF409D6AD6CBC33DA77EA7C8 SHA256: 4D24807B9CAD5110F40ED79D934346D7C9B0290431DC9B11A40BBB86FCF2AEF6
D-TRUST CA 1-1 2017 https://www.d-trust.net/cgi-bin/D-TRUST_CA_1-1_2017.crt Policy level: QCP-n-qscd Fingerprint: SHA1: D3BB63E49B797FEDA9527294B74B871CF63732A0 SHA256: 432DEDA662BB50C57D15F18EBCAFB7AF96388C5E8605E7568A2736E3A1F521D3 OID: 1.3.6.1.4.1.4788.2.100.1
D-TRUST CA 1-3 2017 https://www.d-trust.net/cgi-bin/D-TRUST_CA_1-3_2017.crt Policy level: BTSP Fingerprint: SHA1: 709058584B15A4BEA0272862B8DA3C47091015A8 SHA256: 5F522A439611DEC501F0468FF6A455D23DFBD08EEB33964A0C5EDE95593E1FA8 OID: 1.3.6.1.4.1.4788.2.100.3
D-TRUST Root CA 1 2021 https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_1_2021.crt Fingerprint: SHA1: 330EDD1F5AB057F473FC6FA794CBAEA342D30762 SHA256: C8337326F21230C3F844CAB299E4BFA388BF886FC31C2C236933ED2A046CAC6D
D-TRUST CA 1-21-1 2021 https://www.d-trust.net/cgi-bin/D-TRUST_CA_1-21-1_2021.crt Policy level: QCP-n-qscd Fingerprint: SHA1: 2C5681694EAF1DCDBB70F5E791252019BAA8F9C6 SHA256: C5C2E21F13A8A7CD7C4DF0F7FD30F59DF446A65D7F3A002F2CFADB02C5006409 OID: 1.3.6.1.4.1.4788.2.100.1

Teil der Bundesdruckerei-Gruppe

D-TRUST CA 1-21-2 2022 https://www.d-trust.net/cgi-bin/D-TRUST_CA_1-21-2_2022.crt Policy Level: QCP-l-qscd Fingerprint: SHA1: 969509E4B9A9076242FAD332364B3DEF76E06614 SHA256: C9194A645FEC9FF19640EC6158AB04EFCE0B0B34B3AD0BD8684A935FFA30989C OID: 1.3.6.1.4.1.4788.2.100.2 (D-Trust) OID: 0.4.0.194112.1.3 (ETSI)
D-TRUST CA 1-21-3 2021 https://www.d-trust.net/cgi-bin/D-TRUST_CA_1-21-3_2021.crt Policy level: BTSP Fingerprint: SHA1: DF0C5F927ADB377BB81BB279C2D8C0FBAF767894 SHA256: 6899A24AC929358E404CAB5EC74AE4FFD11DD3FA5C0614683D395C54DBE6F3F9 OID: 1.3.6.1.4.1.4788.2.100.3
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 3-2 2016 https://www.d-trust.net/cgi-bin/D-TRUST_Application_Certificates_CA_3-2_2016.crt Policy level: LCP Fingerprint: SHA1: 60D00D1709487115698E1D8390D6044E32BF69C3 SHA256: 7890EED59E95743C62826398129BC2F54AD414794AAC075BA67177332802B029 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 Cloud PKI
Version	3.5

1.3 PKI entities

1.3.1 Certification authorities (CAs)

These rules are documented in the TSPS.

1.3.2 Registration authorities (RAs)

These rules are documented in the TSPS.

Teil der Bundesdruckerei-Gruppe

1.3.3 Subscribers and end-entities (EEs)

These rules are documented in the TSPS.

1.3.4 Relying parties

The general rules are documented in the TSPS.

BTSP

Users of the time-stamp service according to [EN 319 421] are natural persons or legal entities who obtain and check the time-stamp service within the Cloud PKI.

1.4 Certificate usage

1.4.1 Permitted certificate usage

These rules are documented in the TSPS.

1.4.2 Forbidden certificate usage

These rules are documented in the TSPS.

1.4.3 Service certificate usage

These rules are documented in the TSPS.

1.5 Policy administration

1.5.1 Responsibility for the document

These rules are documented in the TSPS.

1.5.2 Reporting security incidents with certificates

Please contact our support unit to report security incidents:

support@d-trust.net

1.5.3 Compatibility of CPs of external CAs with this CPS

The general rules are documented in the TSPS.

QCP-n-qscd, QCP-l-qscd

Certificates or their sub-CAs and root CAs comply with the requirements of [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.

BTSP

Service certificates or their sub-CAs and root CAs comply with the requirements of [EN 319 421] and [eIDAS]. In the event of inconsistencies between this document and the regulations referred to, [eIDAS] and [EN 319 421] have priority.

1.6 Definitions and acronyms

1.6.1 Definitions and names

The general rules are documented in the CP.

BTSP	Best practices Time-Stamp Policy
TSA	Time-Stamping Authority
TSU	Time-Stamping Unit
TSA DS	TSA Disclosure Statement

1.6.2 Acronyms

Certificate Policy (CP)

Other rules are documented in the CP.

1.6.3 References

These rules are documented in the CP.

2. Publication and Repository Responsibility

2.1 Repositories

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

QCP-n-qscd, QCP-l-qscd
The status of certificates can be permanently requested via OCSP.

Other rules are documented in the CP.

2.2 Publication of certificate information

The TSP publishes the following information:

- Service certificates for time-stamp service
- EE certificates
- This CPS
- The Subscriber Agreement
- PKI user information for qualified trust services

Other rules are documented in the TSPS.

2.3 Publication frequency

LCP
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 one more year and until the end of the year.

QCP-n-qscd
EE certificates are published, i.e. they are entered in the public repository of the TSP. The subscriber must consent to publication. Published EE certificates can be retrieved until the end of their validity term plus at least ten years and until the end of the year.

QCP-l-qscd
EE certificates are not published, i.e., they are not entered in the public repository of the TSP.

In the case of publication, this takes place immediately after a certificate is issued, unless publication is not provided for by default.

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

- at least ten years (QCP-n-qscd, QCP-l-qscd, BTSP) and until the end of the year or
- at least one year and until the end of the year (LCP).

Certificate revocation lists are issued regularly and until the end of validity of the issuing CA certificate. Certificate revocation lists are issued and published immediately following revocation. Even if no certificates were revoked, the TSP ensures that a new certificate revocation list is created at 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.

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

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

2.4 Repository access control

These rules are documented in the TSPS.

2.5 Access to and use of services

These rules are documented in the CP.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of names

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

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

3.1.2 Need for telling names

The distinguished name used is unambiguous within this PKI.

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

3.1.3 Anonymity or pseudonyms of subscribers

No pseudonyms are assigned.

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 (given name)	*Given name(s)* of the natural person - BTSP: This field is not used. - QCP-n-qscd, LCP: According to the proof used for identification
SN (surname)	*Surname* of the natural person - BTSP: This field is not used. - QCP-n-qscd, LCP: According to the proof used for identification If pseudonyms are used, SN corresponds to CN.
CN (common name)	*Common name:* The following variants are used: - Natural persons without a pseudonym: "Surname, name used". - Natural persons with a pseudonym: "Pseudonym: PN" - Legal entities: Official name of the organization (company, public authority, association, etc.), if necessary, reduced to a meaningful name if the maximum number of 64 characters is exceeded.
PN	*Pseudonym*: Identical to CN.
serialNumber	*Serial number*: Name suffix number to ensure unambiguity of the name (typically the application number). Other product-specific uses of the field are possible.
O (organization)	Official name of the subscriber or name of the *organization* to which the end-entity belongs or to which he or she is otherwise affiliated (company, public authority, association, etc.) according to the proof of existence; if necessary, reduced to a meaningful name if the maximum number of 64 characters is exceeded.
OU (organization unit)	*Organization unit* (department, division or other unit) of the organization
OrgID (organization identifier)	BTSP: *Unambiguous organization number* of the organization. The number of the commercial register as well as the VAT ID number or a number assigned by D-TRUST can be entered. The number assigned by D-TRUST is based on the format according to variant 3 in section 5.1.4 of EN 319 412-1 and is made up as follows: DT:DE-1234567890 (DT: D-TRUST; DE: Germany; random number that is unambiguously assigned to the organization).
C (country)	The notation of the country to be stated corresponds to [ISO 3166] and is set up as follows: If an organization O is listed in the DistinguishedName, the organization's place of business in the register determines the entry in the certificate. If no organization O is entered, the country is listed that issued the document that was used to identify the subscriber.
E-mail	The e-mail address of the applicant (optional)
Street	Postal address *Street*
Locality	Postal address *City*
State	Postal address *(Federal) state*
PostalCode	Postal address *Postal code*

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

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

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

3.1.5 Unambiguity of names

The TSP ensures that the subscriber's and/or end-entity's ("Subject" field) name (DistinguishedName) used in EE certificates is always assigned within this PKI to the same subscriber or end-entity, respectively.

The serial number ensures the unambiguity of the certificate.

The TSP ensures the unambiguity of distinguished names in CA certificates.

3.1.6 Recognition, authentication and the role of brand names

The subscriber is liable for compliance with intellectual property rights in the application and certificate data.

3.2 Initial identity verification

3.2.1 Proof of ownership of the private key

The private key of the end-entity is exclusively generated and stored under the responsibility of the TSP.

An unambiguous authentication feature is assigned to the end-entity to ensure that the private keys can only be used by the end-entity.

3.2.2 Identification and authentication of organizations

QCP-l-qscd
The "Certification Practice Statement of the D-TRUST CSM PKI" is used for the identification and authentication of organizations. Identification takes place as part of the application to D-Trust for a qualified access certificate for the remote sealing service (QSealID P12 SMS). The company data is transferred from this certificate to the remote sealing service (re-use of identification).

3.2.3 Identification and authentication of natural persons

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

LCP
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.

	LCP	QCP-n-qscd
G SN	HR-DB / Dok-Ident / Pers-Ident / eID	Pers-Ident / eID
CN C	HR-DB / Dok-Ident / Pers-Ident / eID / Register / Non-Register	Pers-Ident / eID
O	Register / Non-Register / C confirmation / A confirmation	Register / Non-Register / C confirmation / A confirmation
OU	C confirmation/ A confirmation	C confirmation / A confirmation
STREET L State PostalCode	n.a.	n.a.
E-Mail	E-mail address	E-mail address
All other attributes	A confirmation / Dok-Ident / out-of-band mechanisms	A confirmation / Dok-Ident / out-of-band mechanisms

Documents in non-Latin characters are not accepted.

3.2.4 Non-verified information concerning the subscriber

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

3.2.5 Verification of request authorization

In the case of natural persons, the identity and, if necessary or applicable, the affiliation with the organization concerned is determined and verified and/or confirmed using procedures according to section 3.2.3. In the case of organizations, proof of their existence and the applicant's right to represent the organization in question is verified and/or confirmed according to section 3.2.2. Furthermore, at least one 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.

It is possible to issue new certificates based on identification data that is still valid.

Different procedures can be agreed to on a case-to-case basis and the TSP decides on their implementation if such procedures are not subject to certification according to [EN 319 411-1] or [EN 319 411-2].

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:

- The subject must unambiguously authenticate itself to the remote signature service. This requires logging into the remote signature portal or authentication at the interface with customer-specific credentials.
- In the case of a revocation request received in an e-mail, the sender address must correspond to the e-mail address stored as the username in the case of the remote signature service or to the e-mail address stored during registration in the case of organization certificates.
- Revocation requests can only be submitted via an online interface if the party applying for revocation can unambiguously authenticate itself to the interface using the agreed access data.

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

LCP
Revocation requests of end-entities can also 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 0.

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).

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

4.1.2 Registration process and responsibilities

The general rules are documented in the TSPS.

The QCP-n-qscd, QCP-l-qscd, LCP and BTSP policy levels referred to in section 1.1.3 are applicable in this CPS. The registration process and responsibilities for the QCP-n-qscd, QCP-l-qscd and LCP policy levels are described in the TSPS.

The procurement of time stamps (BTSP policy level) does not require a registration process. Time-stamp certificates are issued exclusively to D-Trust GmbH.

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

Pers-Ident
eID

Dok-Ident
HR-DB
C confirmation
A confirmation
out-of-band mechanisms
Register
Non-Register
E-mail address

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

4.2.2 Acceptance or rejection of certificate requests

These rules are documented in the TSPS.

4.2.3 Deadlines for processing certificate requests

These rules are documented in the TSPS.

4.3 Certificate issuance

4.3.1 Procedure of the TSP for issuing certificates

These rules are documented in the TSPS.

4.3.2 Notification of the subscriber that the certificate has been issued

No stipulation.

4.4 Certificate handover

4.4.1 Certificate handover procedure

The private key of the end-entity is exclusively generated and stored under the responsibility of the TSP. The end-entity certificates can be viewed and downloaded via an online interface.

An unambiguous authentication feature is assigned to the end-entity to ensure that the private keys can only be used by the end-entity.

QCP-n-qscd, QCP-l-qscd
Two-factor authentication is carried out.

QCP-n-qscd, QCP-l-qscd
The TSP uses qualified signature creation devices only and, as long as the issued qualified certificates are valid, monitors the status of these qualified signature creation devices within the meaning of EN 319 411-2.

The general rules are documented in the TSPS.

4.4.2 Publication of the certificate by the TSP

QCP-n-qscd
Prior consent to publication is a precondition for requesting Cloud PKI certificates, i.e. the certificates are published in D-Trust's public directory.

The status can be retrieved via OCSP after production of the certificate.

QCP-l-qscd
Certificates for legal entities are not listed in D-Trust’s public repository.

The status can be retrieved via OCSP after production of the certificate.

4.4.3 Notification of other PKI entities concerning the issuance of the certificate

Third parties authorized to request revocation according to section 4.9.2 are not notified separately. However, they have the possibility to revoke the certificates concerned via the agreed online interface.

4.5 Key pair and certificate usage

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

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

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

The remote signature system technically excludes the signature with expired certificates.

The provisions in section 1.4 apply to subscribers.

4.5.2 Public key and certificate usage by relying parties

The general rules are documented in the TSPS.

BTSP
Users of the time-stamp service can only trust the time stamp if they have checked the time stamp according to [EN 319 421] and if:

- verification of the certificate chain can be carried out successfully right through to a trusted root certificate and
- the outcome of the certificate status check via the status request service (OCSP) was positive.

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 and which has a different period of validity. The CP and CPS in effect at the time of renewal apply to the renewed certificates. 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 generally not performed for CA keys.

In the event that EE certificates for natural persons or legal entities are to be reissued while the validated identification data are still valid, the requesting end entity must unambiguously authenticate itself.

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].

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.

Third 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

The subscriber or a representative authorized by the subscriber can generally revoke a certificate via an online interface.

In the case of a revocation request received in an e-mail, the sender address must correspond to the e-mail address stored as the username or as the contact (legal entity) with the remote signature service.

Other revocation methods can be agreed to.

Revocation at a future point in time is not offered. Revocation via the online interface becomes effective immediately. Revocation requests received by e-mail are processed the next working day at the latest.

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

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

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

4.9.4 Revocation request deadlines

These rules are documented in the TSPS.

4.9.5 Time span for processing a revocation request by the TSP

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

Revocation via the online interface is carried out immediately after successful authorization of the party requesting revocation.

Revocation requests received by e-mail are processed the next working day at the latest.

4.9.6 Methods available for checking revocation information

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

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

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

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

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

QCP-n-qscd, QCP-l-qscd
Revocation entries remain in the associated certificate revocation lists after the respective certificate validity has expired.

4.9.7 Publication frequency of certificate revocation lists

See section 2.3.

4.9.8 Maximum latency time for certificate revocation lists

Certificate revocation lists are created immediately and published after 60 minutes at the latest.

4.9.9 Online availability of revocation information

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

4.9.10 Need for online verification of revocation information

These rules are documented in the TSPS.

4.9.11 Other forms for notification of revocation information

These rules are documented in the TSPS.

4.9.12 Special requirements if the private key is compromised

These rules are documented in the TSPS.

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

Private EE keys of the Cloud PKI are generally and exclusively generated and stored by the TSP. A specific procedure for key escrow is not offered.

5. Facility, Management and Operational Controls

The descriptions in this section refer to the time-stamp service and the CAs operated by D-Trust GmbH in accordance with [EN 319 421] or [EN 319 411-1] and [EN 319 411-2], respectively.

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 319 421] or [EN 319 411-1] and [EN 319 411-2], respectively.

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

The TSP operates a time-stamp service in accordance with [eIDAS] (see section 6.8).

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.

EE keys are generated and stored by the TSP. The 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].

QCP-n-qscd, QCP-l-qscd
The TSP uses qualified signature creation devices only and, as long as the qualified certificates issued are valid, monitors the status of the corresponding qualified signature creation device within the meaning of [EN 319 411-2].

6.1.2 Private key delivery to subscribers

The private EE keys are not delivered to the subscriber.

The EE key remains in the secured area of the TSP as long as it is used.

6.1.3 Public key delivery to the TSP

The TSP does not accept any public keys from external bodies.

6.1.4 CA public key delivery to relying parties

The CA public key is contained in certificate. This certificate is available to the subscriber for download. The CA and service certificates are available from the public directory.

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 referred to 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.

The service, CA and EE keys are protected by HSMs and/or service cards that comply with the existing requirements.

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

The cryptographic module on which the service, CA and EE keys are stored is located in the secure environment of the trust service provider. Two authorized persons are needed to activate the respective private key and to access the private EE keys.

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.

Service keys stored on a smart card are not secured. Availability is ensured by providing several service keys on redundant smart cards.

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

The general rules are documented in the TSPS.

Private EE keys can be transferred from the cryptographic module only by the trust service provider. The key will never leave the module in a non-encrypted form.

6.2.7 Storage of private keys in cryptographic modules

The general rules are documented in the TSPS.

EE keys are encrypted with the help of an HSM according to ETSI TS 119 431-1 and contained 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 the end-entity using the authentication features.

6.2.9 Deactivation of private keys

The general rules are documented in the TSPS.

QCP-n-qscd, QCP-l-qscd, LCP
EE keys of the Cloud PKI are deactivated as soon as they have been used once.

6.2.10 Destruction of private keys

The general rules are documented in the TSPS.

Service keys stored on smart cards are deleted by destroying the card.

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 term of validity of the service and CA keys and certificates is variable and shown in the certificate. The maximum possible validity period totals 30 years.

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

LCP
63 months.

QCP-n-qscd, QCP-l-qscd
EE certificates are issued with a maximum period of validity of 24 months.

6.4 Activation data

6.4.1 Activation data generation and installation

The general rules are documented in the TSPS.

The authentication feature is generated by the subscriber and closely linked to the subscriber within the scope of identification.

QCP-n-qscd
The second authentication factor is generated by the TSP and transferred to the end-entity via a separate channel.

QCP-l-qscd
The second factor for authentication (QSealID p12 SMS) is requested from the TSP by the subject and generated by the TSP and transmitted to the subject on a separate channel.

6.4.2 Protection of activation data

The general rules are documented in the TSPS.

The subscriber is responsible for protecting his or her authentication features.

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

The TSP operates a time-stamp service in accordance with [eIDAS], [EN 319 421] and [EN 319 422].

The time-stamp service has a redundant structure and its availability in the productive environment is 99.5%. The service is monitored 24/7.

The time stamp can be addressed via an online interface according to RFC 3161 (Internet X.509 Public Key Infrastructure Time-Stamp Protocol [TSP]).

A client certificate is required for authentication which must be separately applied for at the TSP. Users of the time-stamp service are subject to the requirements of [EN 319 421].

A TSU has only one active time stamp signature key. The validity of the TSU key ends two years before the corresponding certificate expires. The validity of the TSU key is laid down in the public certificate. Once the validity of the keys has expired, they are no longer used for the time stamp signature.

Events in the time-stamp service (change in time stamp key/certificate, synchronization of the time, loss of the time source, etc.) are logged.

Specific requirements and implementations are marked in this document with the certification level "BTSP". Furthermore, only subsections 3.1 and 3.2 of section 3 of this document are applicable.

The system time of the time stamp is synchronized daily with the German DCF77 time signal and reliable time servers (NTP) on the Internet. In the case of major deviations or expired service certificates, a manipulation protection will prevent the issuing of faulty time stamps to ensure accuracy with a maximum deviation of less than one second. Leap seconds are corrected by analyzing

the DCF77 signal. The systems used for the time provision are operated in the secured environment of the computer center.

Time stamps are not issued if the system time deviates more than one second from the official time, if the service certificate is not valid, if synchronization of the time can no longer be guaranteed or in the case of suspected compromising.

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

EE certificates can include the following non-critical extensions:

Extension	OID	Parameter
additionalInformation	1.3.36.8.3.15	This number can be assigned by D-Trust. It is used for internal referencing of data records of the applicant.

Further rules are documented in the TSPS.

7.1.3 Algorithm OIDs

The following encryption algorithm is currently used in CA and EE certificates:

- rsaEncryption with OID 1.2.840.113549.1.1.1
- id-RSASSA-PSS with OID 1.2.840.113549.1.1.10

The following curve is used for ECC keys in EE certificates:

- secp521r1 with OID: 1.3.132.0.35

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

- sha256 with RSA encryption with OID 1.2.840.113549.1.1.11
- sha384 with RSA encryption with OID 1.2.840.113549.1.1.12
- sha512 with RSA encryption with OID 1.2.840.113549.1.1.13
- ecdsa-with-SHA256 with OID 1.2.840.10045.4.3.2
- ecdsa-with-SHA384 with OID 1.2.840.10045.4.3.3
- ecdsa-with-SHA512 with OID 1.2.840.10045.4.3.4

SHA1 is not used.

7.1.4 Name formats

These rules are documented in the TSPS.

7.1.5 Name constraints

These rules are documented in the TSPS.

7.1.6 Certificate Policy Object Identifier

These rules are documented in the TSPS.

7.1.7 Use of the "PolicyConstraints" extension

These rules are documented in the TSPS.

7.1.8 Syntax and semantics of "PolicyQualifiers"

These rules are documented in the TSPS.

7.1.9 Processing the semantics of the critical "CertificatePolicies" extension

These rules are documented in the TSPS.

7.2 CRL profiles

7.2.1 Version number(s)

These rules are documented in the TSPS.

7.2.2 Extensions of certificate revocation lists and certificate revocation list entries

These rules are documented in the TSPS.

7.3 OCSP profiles

These rules are documented in the TSPS.

7.3.1 Version number(s)

These rules are documented in the TSPS.

7.3.2 OCSP extensions

These rules are documented in the TSPS.

8. Compliance Audit and Other Assessment

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 and also the General Terms and Conditions [AGB].

Certification Practice Statement der D-TRUST Cloud PKI

Version 3.5

Teil der Bundesdruckerei-Gruppe

Copyright UND NUTZUNGSLIZENZ

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

This work is licensed under a 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	01.01.2017	▪ Einführung von fernausgelösten Signaturen als nicht-qualifizierter Vertrauensdienst gemäß EN 319 411-1
2.0	01.04.2017	▪ Einführung von fernausgelösten qualifizierten Signaturen als qualifizierter Vertrauensdienst gemäß EN 319 411-2 ▪ Einführung eines qualifizierte Zeitstempeldienstes als qualifizierter Vertrauensdienst gemäß EN 319 421
2.1	01.10.2017	▪ Editorische Änderungen sowie 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	▪ Feld OrgID in Abschnitt 3.1.4 wurde gemäß Variante 3 aus Kapitel 5.1.4 der EN 319 412-1 ergänzt ▪ Redaktionelle Anpassungen
2.4	11.10.2018	▪ Tabellarische Darstellung der CA Zertifikate in Abschnitt 1.1.3 ▪ Ergänzungen in Kapitel 7.3 ▪ Anpassungen der Abschnitte 1.5.2 und 4.9 gemäß Ballot SC6v3 aus dem CAB-Forum
2.5	30.11.2018	▪ Dieses CPS entspricht den Anforderungen der Mozilla Policy 2.6.1 ▪ Jährliches Review des gesamten CPS ▪ Redaktionelle Anpassungen
2.6	09.10.2019	▪ Update nach observation report vom CAB ▪ Editorische Änderungen
2.7	19.03.2020	▪ Dieses CPS entspricht den Anforderungen der Mozilla Policy 2.7 ▪ Jährliches Review des gesamten CPS ▪ Anpassung der Aufbewahrungsfrist für LCP in Abschnitt 5.5.2 ▪ Ergänzung des SHA-256 Fingerprints in Abschnitt 1.1.3 ▪ Editorische Änderungen sowie Konkretisierung der Abschnitte 5.2.1, 6.6, 7.2.2
2.8	27.04.2020	▪ Ergänzungen zur Verifikation der Zertifikatskette in Abschnitt 4.5.2 ▪ Ergänzungen in den Abschnitten 5.3.7 und 5.5.2
3.0	10.11.2020	▪ Das Cloud CPS ist ab Version 3.0 der TSPS untergeordnet. ▪ Update nach observation report
3.1	22.06.2021	▪ Bekanntmachung der neuen CAs für QCP-n-qscd und BTSP in Abschnitt 1.1.3 ▪ Austausch des Links in Abschnitt 1.1.3 ▪ Jährliches Review des gesamten CPS ▪ Editorische Änderungen in Abschnitt 7.1.3
3.2	06.12.2021	▪ Mitteilung der Inbetriebnahme der neuen CA für QCP-n-qscd, siehe Abschnitt 1.1.3 ▪ Ergänzungen in Abschnitt 7.1.2

Teil der Bundesdruckerei-Gruppe

Version	Datum	Beschreibung
		▪ Konkretisierungen in Abschnitt 3.1.4 und 3.2.3
3.3	01.07.2022	▪ Ergänzungen und Konkretisierungen in den Abschnitten 1.1.3, 2.3, 4.3.2, 4.7, 6.2.6, 6.3.2 und 6.8 ▪ Jährliches Review des gesamten CPS
3.4	14.11.2022	▪ Einführung des Policy Levels QCP-l-qscd
3.5	22.12.2022	▪ Bekanntmachung der ausstellenden CA für den Vertrauensdienst „D-Trust remote seal service (seal-me)" mit dem Policy Level QCP-l-qscd, siehe Abschnitt 1.1.3.

Teil der Bundesdruckerei-Gruppe

Inhaltsverzeichnis

1. Einleitung 7
1.1 Überblick 7
1.2 Name und Kennzeichnung des Dokuments 11
1.3 PKI-Teilnehmer 11
1.4 Verwendung von Zertifikaten 12
1.5 Administration der Policy 12
1.6 Begriffe und Abkürzungen 12
2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen 13
2.1 Verzeichnisse 13
2.2 Veröffentlichung von Informationen zu Zertifikaten 13
2.3 Häufigkeit von Veröffentlichungen 13
2.4 Zugriffskontrollen auf Verzeichnisse 14
2.5 Zugang und Nutzung von Diensten 14
3. Identifizierung und Authentifizierung 14
3.1 Namensregeln 14
3.2 Initiale Überprüfung der Identität 16
3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying) 17
3.4 Identifizierung und Authentifizierung von Sperranträgen 18
4. Betriebsanforderungen 18
4.1 Zertifikatsantrag und Registrierung 18
4.2 Verarbeitung des Zertifikatsantrags 18
4.3 Ausstellung von Zertifikaten 19
4.4 Zertifikatsübergabe 19
4.5 Verwendung des Schlüsselpaars und des Zertifikats 20
4.6 Zertifikatserneuerung (certificate renewal) 20
4.7 Zertifikatserneuerung mit Schlüsselerneuerung 20
4.8 Zertifikatsänderung 21
4.9 Widerruf und Suspendierung von Zertifikaten 21
4.10 Statusabfragedienst für Zertifikate 22
4.11 Austritt aus dem Zertifizierungsdienst 23
4.12 Schlüsselhinterlegung und –wiederherstellung 23
5. Nicht-technische Sicherheitsmaßnahmen 23
5.1 Bauliche Sicherheitsmaßnahmen 23
5.2 Verfahrensvorschriften 23
5.3 Eingesetztes Personal 23
5.4 Überwachungsmaßnahmen 24
5.5 Archivierung von Aufzeichnungen 24
5.6 Schlüsselwechsel beim TSP 24
5.7 Kompromittierung und Geschäftsweiterführung beim TSP 25
5.8 Schließung des TSP bzw. die Beendigung der Dienste 25
6. Technische Sicherheitsmaßnahmen 25
6.1 Erzeugung und Installation von Schlüsselpaaren 25
6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module 26
6.3 Andere Aspekte des Managements von Schlüsselpaaren 27
6.4 Aktivierungsdaten 27
6.5 Sicherheitsmaßnahmen in den Rechneranlagen 28
6.6 Technische Maßnahmen während des Life Cycles 28
6.7 Sicherheitsmaßnahmen für Netze 28
6.8 Zeitstempel 28
7. Profile von Zertifikaten, Sperrlisten und OCSP 29
7.1 Zertifikatsprofile 29
7.2 Sperrlistenprofile 30

Teil der Bundesdruckerei-Gruppe

7.3 Profile des Statusabfragedienstes (OCSP) 30
8. Überprüfungen und andere Bewertungen 30
9. Sonstige finanzielle und rechtliche Regelungen 30

Teil der Bundesdruckerei-Gruppe

1. Einleitung

1.1 Überblick

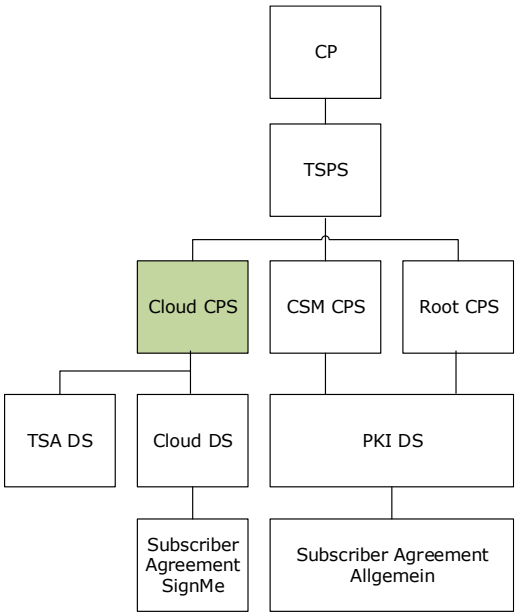
Dieses Dokument ist das Certification Practice Statement (CPS) der von D-Trust GmbH betriebenen Vertrauensdienste, die die D-TRUST Cloud PKI nutzen. Der Dokumentenname wird mit **Cloud CPS** abgekürzt verwendet und unterliegt dem Trust Service Practice Statement der D-TRUST (abgekürzt TSPS) und der Zertifikatsrichtlinie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

1.1.1 Vertrauensdiensteanbieter

Diese Regelungen sind in der CP festgehalten.

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 (Trust Service Practice Statement der D-TRUST) und die [EN 319 411-1] bzw. [EN 319 411-2] und [EN 319 421]. Es beschreibt die Umsetzung der daraus resultierenden Anforderungen.

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

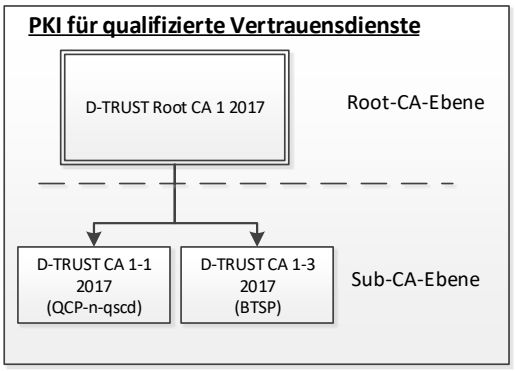
Die Struktur dieses Dokumentes folgt dem Internet-Standard RFC 3647 "*Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*".

1.1.3 Eigenschaften der PKI

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

Die privaten Schlüssel der EE-Zertifikate werden ausschließlich im Verantwortungsbereich des TSP erzeugt und gehalten.

Aktuell gültige PKI-Hierarchie für qualifizierte Vertrauensdienste[1]



[1] Die SubCA „D-TRUST CA 1-21-2 2022" ist erstellt, jedoch noch nicht in Betrieb. Die Aufnahme der SubCA in der Trusted List des BNetzA ist beantragt und wird nach ihrer Veröffentlichung in Betrieb genommen.

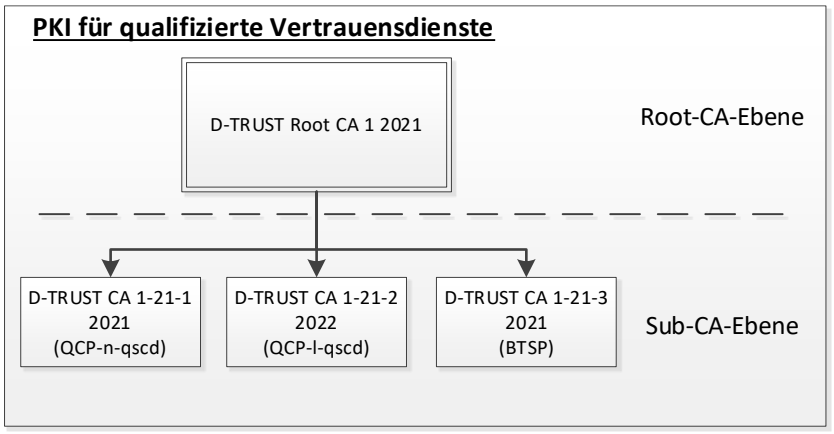


Abbildung 1: PKI-Hierarchie für qualifizierte Vertrauensdienste[2]

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

QCP-n-qscd – Qualifizierte Personenzertifikate auf qualifizierter Signaturerstellungseinheit

QCP-l-qscd – Qualifizierte Siegelzertifikate auf qualifizierter Siegelerstellungseinheit

Die Dienstezertifikate für Zeitstempel lassen sich in ihrer Ausprägung den Anforderungen der [EN 319 421] zuordnen:

BTSP – Qualifizierter Zeitstempeldienst

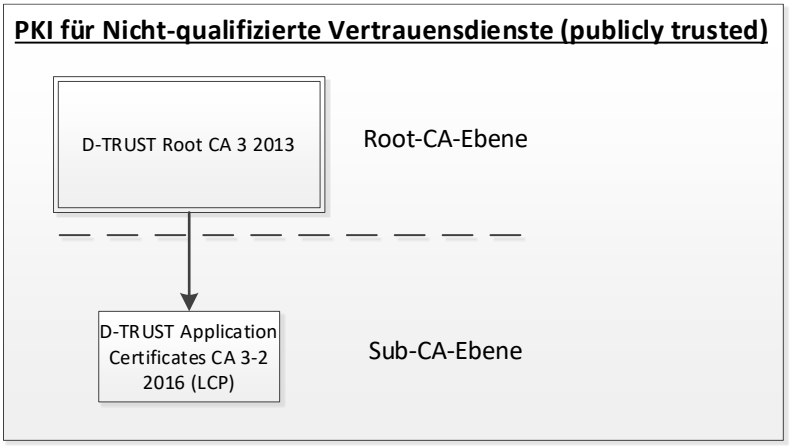


Abbildung 2: PKI-Hierarchie für nicht-qualifizierte Vertrauensdienste

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

LCP – Lightweight Certificate Policy

Die Policy Level werden im TSPS erläutert.

[2] Die SubCA „D-TRUST CA 1-21-1 2021" ist in der Trusted List der BNetzA aufgelistet und wurde in Betrieb genommen. Zertifikate werden nur noch aus der neuen SubCA „D-TRUST CA 1-21-1 2021" ausgestellt. Die SubCA „D-TRUST CA 1-21-3 2021" ist erstellt jedoch noch nicht in Betrieb. Das nächste TSU-Zertifikat (D-TRUST qualified Timestamp) wird aus der „D-TRUST CA 1-21-3 2021" ausgestellt. Perspektivisch wird die „D-TRUST Root CA 1 2021" die „D-TRUST Root CA 1 2017" ersetzen.

CA-Zertifikate

Die Gesamtübersicht aller RootCAs und SubCAs mit den Zertifizierungsstufen QCP-w, EVCP, OVCP, DVCP und LCP aus der hervorgeht welches CPS 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 CA 1 2017 https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_1_2017.crt Fingerprint: SHA1: 3FE69767C9B3E938CF409D6AD6CBC33DA77EA7C8 SHA256: 4D24807B9CAD5110F40ED79D934346D7C9B0290431DC9B11A40BBB86FCF2AEF6
D-TRUST CA 1-1 2017 http://www.d-trust.net/cgi-bin/D-TRUST_CA_1-1_2017.crt Policy Level: QCP-n-qscd Fingerprint: SHA1: D3BB63E49B797FEDA9527294B74B871CF63732A0 SHA256: 432DEDA662BB50C57D15F18EBCAFB7AF96388C5E8605E7568A2736E3A1F521D3 OID: 1.3.6.1.4.1.4788.2.100.1
D-TRUST CA 1-3 2017 https://www.d-trust.net/cgi-bin/D-TRUST_CA_1-3_2017.crt Policy Level: BTSP Fingerprint: SHA1: 709058584B15A4BEA0272862B8DA3C47091015A8 SHA256: 5F522A439611DEC501F0468FF6A455D23DFBD08EEB33964A0C5EDE95593E1FA8 OID: 1.3.6.1.4.1.4788.2.100.3
D-TRUST Root CA 1 2021 https://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_1_2021.crt Fingerprint: SHA1: 330EDD1F5AB057F473FC6FA794CBAEA342D30762 SHA256: C8337326F21230C3F844CAB299E4BFA388BF886FC31C2C236933ED2A046CAC6D
D-TRUST CA 1-21-1 2021 https://www.d-trust.net/cgi-bin/D-TRUST_CA_1-21-1_2021.crt Policy Level: QCP-n-qscd Fingerprint: SHA1: 2C5681694EAF1DCDBB70F5E791252019BAA8F9C6 SHA256: C5C2E21F13A8A7CD7C4DF0F7FD30F59DF446A65D7F3A002F2CFADB02C5006409 OID: 1.3.6.1.4.1.4788.2.100.1

Teil der Bundesdruckerei-Gruppe

D-TRUST CA 1-21-2 2022 https://www.d-trust.net/cgi-bin/D-TRUST_CA_1-21-2_2022.crt Policy Level: QCP-l-qscd Fingerprint: SHA1: 969509E4B9A9076242FAD332364B3DEF76E06614 SHA256: C9194A645FEC9FF19640EC6158AB04EFCE0B0B34B3AD0BD8684A935FFA30989C OID: 1.3.6.1.4.1.4788.2.100.2 (D-Trust) OID: 0.4.0.194112.1.3 (ETSI)
D-TRUST CA 1-21-3 2021 https://www.d-trust.net/cgi-bin/D-TRUST_CA_1-21-3_2021.crt Policy Level: BTSP Fingerprint: SHA1: DF0C5F927ADB377BB81BB279C2D8C0FBAF767894 SHA256: 6899A24AC929358E404CAB5EC74AE4FFD11DD3FA5C0614683D395C54DBE6F3F9 OID: 1.3.6.1.4.1.4788.2.100.3
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 3-2 2016 https://www.d-trust.net/cgi-bin/D-TRUST_Application_Certificates_CA_3-2_2016.crt Policy Level: LCP Fingerprint: SHA1: 60D00D1709487115698E1D8390D6044E32BF69C3 SHA256: 7890EED59E95743C62826398129BC2F54AD414794AAC075BA67177332802B029 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 Cloud PKI
Version	3.5

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)

Die allgemeinen Regelungen sind in dem TSPS dokumentiert.

BTSP

Nutzer des Zeitstempeldienstes gemäß [EN 319 421] sind natürliche oder juristische Personen, die den Zeitstempeldienst im Rahmen der Cloud PKI erhalten und prüfen.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

Diese Regelungen sind im TSPS dokumentiert.

1.4.2 Verbotene Verwendungen von Zertifikaten

Diese Regelungen sind im TSPS dokumentiert.

1.4.3 Verwendung von Dienstezertifikaten

Diese Regelungen sind im TSPS dokumentiert.

1.5 Administration der Policy

1.5.1 Zuständigkeit für das Dokument

Diese Regelungen sind im TSPS dokumentiert.

1.5.2 Meldung von Sicherheitsvorfällen mit Zertifikaten

Zur Meldung von Sicherheitsvorfällen kontaktieren Sie bitte unseren Support:

support@d-trust.net

1.5.3 Verträglichkeit von CPs fremder CAs mit diesem CPS

Die allgemeinen Regelungen sind im TSPS dokumentiert.

QCP-n-qscd, QCP-l-qscd

Zertifikate, bzw. deren Sub- sowie Root-CAs kommen den Anforderungen aus [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].

BTSP

Dienstezertifikate, bzw. deren Sub- sowie Root-CAs kommen den Anforderungen aus [EN 319 421] und [eIDAS] nach. Im Falle von Inkonsistenzen zwischen diesem Dokument und den genannten Richtlinien, gelten vorrangig [eIDAS] und [EN 319 421].

1.6 Begriffe und Abkürzungen

1.6.1 Begriffe und Namen

Die allgemeinen Regelungen sind in der CP dokumentiert.

BTSP	Best practices Time-Stamp Policy
TSA	Time-Stamping Authority
TSU	Time-Stamping Unit
TSA DS	TSA Disclosure statement

1.6.2 Abkürzungen

Certificate Policy (CP)	Zertifikatsrichtlinie.

Die weiteren Regelungen sind in der CP dokumentiert.

1.6.3 Referenzen

Diese Regelungen sind in der CP dokumentiert.

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

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

QCP-n-qscd, QCP-l-qscd
Der Status der Zertifikate kann mittels OCSP-Abfrage dauerhaft abgerufen werden.

Die weiteren Regelungen sind in der CP dokumentiert.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Der TSP veröffentlicht folgende Informationen:

- Dienstezertifikate für den Zeitstempeldienst,
- EE-Zertifikate,
- dieses CPS,
- die Verpflichtungserklärung,
- die PKI-Nutzerinformation für qualifizierte Vertrauensdienste.

Die weiteren Regelungen sind im TSPS dokumentiert.

2.3 Häufigkeit von Veröffentlichungen

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

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

QCP-l-qscd
EE-Zertifikate werden nicht veröffentlicht, d.h. sie werden nicht in das öffentliche Verzeichnis des TSP aufgenommen.

Im Falle der Veröffentlichung findet diese sofort nach Ausstellung eines Zertifikats statt, es sei denn die Veröffentlichung ist per Default nicht vorgesehen.

CA- und Dienstezertifikate werden nach ihrer Erstellung veröffentlicht und

- mindestens 10 Jahre (QCP-n-qscd, QCP-l-qscd, BTSP) und bis zum Jahresende bzw.
- mindestens 1 Jahr und bis zum Jahresende (LCP)

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 erstellt und veröffentlicht. Auch wenn kein Widerruf von Zertifikaten erfolgt, stellt der TSP sicher, dass alle 12 Stunden eine neue Sperrliste ausgestellt wird. Die Sperrlisten werden mindestens ein Jahr nach Ablauf der Gültigkeit der CA vorgehalten.

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

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.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.

Eine eindeutige Zuordnung des Zertifikats zum Zertifikatsnehmer (bei Zertifikaten für natürliche Personen auch zum Endanwender) ist gegeben. Bei alternativen Namen (*subjectAltName*) gibt es, 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 nicht vergeben.

3.1.4 Regeln für die Interpretation verschiedener Namensformen

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

DN-Bestandteil	Interpretation
G (given name)	*Vorname(n)* der natürlichen Person - BTSP: Feld wird nicht verwendet - QCP-n-qscd, LCP: gemäß dem zur Identifizierung verwendeten Nachweis
SN (surname)	*Familienname* der natürlichen Person - BTSP: Feld wird nicht verwendet - QCP-n-qscd, LCP: gemäß dem zur Identifizierung verwendeten Nachweis Bei der Verwendung von Pseudonymen entspricht der SN dem CN.
CN (common name)	*Gebräuchlicher Name:* Folgende Varianten werden verwendet: - Natürlichen Personen ohne Pseudonym: „Familienname, Rufname". - Natürliche Personen mit Pseudonym: „Pseudonym: PN". - Juristischen Personen: offizielle Bezeichnung der Organisation (Firma, Behörde, Verein etc.), ggf. sinnvolle Abkürzung bei Überschreiten der Zeichenbegrenzung von 64 Zeichen.
PN	*Pseudonym*: ist identisch zu CN.
serialNumber	*Seriennummer*: Namenszusatznummer, welche die Eindeutigkeit des Namens sicherstellt (i.d.R. die Antragsnummer). Produktspezifisch kann das Feld anderweitig verwendet werden.
O (organization)	Offizielle Bezeichnung des Zertifikatsnehmers oder Bezeichnung der *Organisation*, der der Endanwender angehört oder damit sonst verbunden ist (Firma, Behörde, Verein etc.) entsprechend Existenznachweis, ggf. sinnvolle Abkürzung bei Überschreiten der Zeichenbegrenzung von 64 Zeichen.
OU (organization unit)	*Organisationseinheit* (Abteilung, Bereich oder andere Unterteilung) der Organisation.
OrgID (organization identifier)	BTSP: *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).
C (country)	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.
E-Mail	Die E-Mail Adresse des Antragstellers (optional)
Street	Postalische Adresse *Straße*
Locality	Postalische Adresse *Ort*
State	Postalische Adresse *(Bundes-)Land*
PostalCode	Postalische Adresse *Postleitzahl*

QCP-n-qscd

Qualifizierte Zertifikate für natürliche Personen enthalten mindestens die subject-DN-Bestandteile „commonName", „countryName", „serialNumber" sowie „GivenName" und „Surname".

BTSP, QCP-l-qscd

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

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

3.1.5 Eindeutigkeit von Namen

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

Die Eindeutigkeit des Zertifikats wird mittels der Seriennummer erzielt.

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

3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen

Der Zertifikatsnehmer haftet für die Einhaltung geistiger Eigentumsrechte in den Antrags- und Zertifikatsdaten.

3.2 Initiale Überprüfung der Identität

3.2.1 Nachweis für den Besitz des privaten Schlüssels

Der private Schlüssel des Endanwenders wird ausschließlich im Verantwortungsbereich des TSP erzeugt und gehalten.

Dem Endanwender wird ein eindeutiges Authentifizierungsmerkmal zugeordnet, so dass sichergestellt wird, dass die privaten Schlüssel ausschließlich durch den Endanwender verwendet werden können.

3.2.2 Identifizierung und Authentifizierung von Organisationen

QCP-l-qscd

Für die Identifizierung und Authentifizierung von Organisationen findet das „Certification Practice Statement der D-TRUST CSM PKI" Anwendung. Die Identifizierung findet im Rahmen der Antragstellung bei D-Trust für ein qualifiziertes Zugangszertifikat zum Fernsiegeldienst (QSealID P12 SMS) statt. Die Unternehmensdaten werden aus diesem Zertifikat zum Fernsiegeldienst übernommen (Nachnutzung der Identifizierung).

3.2.3 Identifizierung und Authentifizierung natürlicher Personen

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

LCP

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.

Teil der Bundesdruckerei-Gruppe

	LCP	QCP-n-qscd
G SN	HR-DB / Dok-Ident / Pers-Ident / eID	Pers-Ident / eID
CN C	HR-DB / Dok-Ident / Pers-Ident / eID / Register / Non- Register	Pers-Ident / eID
O	Register / Non-Register / Z-Bestätigung/ A-Bestätigung	Register / Non-Register / Z-Bestätigung/ A-Bestätigung
OU	Z-Bestätigung/ A-Bestätigung	Z-Bestätigung/ A-Bestätigung
STREET L State PostalCode	n.a.	n.a.
E-Mail	E-Mail	E-Mail
Alle weiteren Attribute	A-Bestätigung / Dok-Ident / out-of-band mechanisms	A-Bestätigung / Dok-Ident / out-of-band mechanisms

Nachweise in nicht lateinischer Schrift werden nicht akzeptiert.

3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

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

3.2.5 Prüfung der Berechtigung zur Antragstellung

Bei natürlichen Personen werden Identitätsnachweis und ggf. die Organisationszugehörigkeit mittels der Verfahren gemäß Abschnitt 3.2.3 ermittelt und geprüft bzw. bestätigt. Bei Organisationen wird der Existenznachweis sowie die Vertretungsberechtigung des Antragstellers nach Abschnitt 3.2.2 geprüft bzw. bestätigt. Weiterhin wird mindestens ein 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.

Die Ausstellung neuer Zertifikate auf Basis noch gültiger Identifikationsdaten ist möglich.

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

Schlüsselerneuerung auf Basis eines widerrufenen Zertifikats wird nicht angeboten.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Sperrberechtigung wird wie folgt geprüft:

- Der Endanwender muss sich gegenüber dem Fernsignaturdienst eindeutig authentifizieren. Dazu ist die Anmeldung im Fernsignaturportal oder eine Authentifizierung an der Schnittstelle mit den kundenindividuellen Credentials notwendig.
- Bei einem Sperrantrag, der in einer E-Mail eingeht, muss die Absenderadresse der beim Fernsignaturdienst als Benutzernamen oder im Falle von Organisationszertifikaten, der bei der Registrierung hinterlegten Mailadresse entsprechen.
- Sperranträge können nur dann über eine Online-Schnittstelle eingereicht werden, wenn sich der Sperrantragsteller gegenüber der Schnittstelle mit den vereinbarten Zugangsdaten eindeutig authentifizieren kann.

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

LCP
Sperranträge eines Endanwenders können auch an den technischen Ansprechpartner der RA gerichtet werden. 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.

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-n-qscd, QCP-l-qscd, LCP und BTSP Anwendung. Der Registrierungsprozess und die Zuständigkeiten für die Policy Level QCP-n-qscd, QCP-l-qscd und LCP werden in der TSPS beschrieben.

Der Bezug von Zeitstempeln (Policy Level BTSP) erfordert keinen Registrierungsprozess. Zeitstempelzertifikate werden ausschließlich auf die D-Trust GmbH ausgestellt.

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Die allgemeinen Regelungen sind im TSPS dokumentiert.

Im Rahmen des Cloud 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
HR-DB
Z-Bestätigung
A-Bestätigung
out-of-band-Mechanismen
Register
Non-Register
E-Mail-Adresse

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

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Diese Regelungen sind im TSPS dokumentiert.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Diese Regelungen sind im TSPS dokumentiert.

4.3 Ausstellung von Zertifikaten

4.3.1 Vorgehen des TSP bei der Ausstellung von Zertifikaten

Diese Regelungen sind im TSPS dokumentiert.

4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausstellung des Zertifikats

Keine Vorgaben.

4.4 Zertifikatsübergabe

4.4.1 Verhalten bei der Zertifikatsübergabe

Der private Schlüssel des Endanwenders wird ausschließlich im Verantwortungsbereich des TSP erzeugt und gehalten. Die Endanwenderzertifikate können über eine Online-Schnittstelle eingesehen und heruntergeladen werden.

Dem Endanwender wird ein eindeutiges Authentifizierungsmerkmal zugeordnet, so dass sichergestellt wird, dass die privaten Schlüssel ausschließlich durch den Endanwender verwendet werden können.

QCP-n-qscd, QCP-l-qscd
Es wird eine Zwei-Faktor-Authentisierung durchgesetzt.

QCP-n-qscd, QCP-l-qscd
Der TSP verwendet ausschließlich qualifizierte Signaturerstellungseinheiten und überwacht während der Gültigkeit der ausgegebenen qualifizierten Zertifikate den Status dieser qualifizierten Signaturerstellungseinheiten im Sinne EN 319 411-2.

Die allgemeinen Regelungen sind im TSPS dokumentiert.

4.4.2 Veröffentlichung des Zertifikats durch den TSP

QCP-n-qscd
Die Zustimmung zur Veröffentlichung ist Voraussetzung für die Beantragung von Zertifikaten der Cloud PKI, d.h. die Zertifikate werden in das öffentliche Verzeichnis der D-Trust aufgenommen.

Der Status ist nach der Erstellung des Zertifikats über OCSP abrufbar.

Teil der Bundesdruckerei-Gruppe

QCP-l-qscd
Zertifikate für juristische Personen werden nicht in das öffentliche Verzeichnis der D-Trust aufgenommen.

Der Status ist nach der Erstellung des Zertifikats über OCSP abrufbar.

4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats

Sperrberechtigte Dritte nach Abschnitt 4.9.2 werden nicht gesondert benachrichtigt, haben aber die Möglichkeit die entsprechenden Zertifikate über die vereinbarte Online-Schnittstelle zu widerrufen.

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 stehen.

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

Das Fernsignatursystem schließt technisch die Signatur mit abgelaufenen Zertifikaten aus.

Für Zertifikatsnehmer gelten die Bestimmungen aus Abschnitt 1.4.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Die allgemeinen Regelungen sind im TSPS dokumentiert.

BTSP
Nutzer des Zeitstempeldienstes können auf den Zeitstempel nur vertrauen, wenn sie den Zeitstempel gemäß [EN 319 421] geprüft haben sowie:

- die Verifikation der Zertifikatskette bis zu einem vertrauenswürdigen Root-Zertifikat erfolgreich durchgeführt und
- der Status der Zertifikate über den Statusabfragedienst (OCSP) positiv geprüft werden konnte.

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 und dessen Gültigkeits-zeitraum verändert wird. Für die erneuerten Zertifikate gilt die zum Zeitpunkt der Erneuerung aktuelle CP und CPS. Haben sich grundsätzliche Änderungen an den Nutzungsbedingungen ergeben, wird der Zertifikatsnehmer darüber informiert. Der Zertifikatsnehmer bestätigt die neuen Bedingungen.

Bei CA-Schlüsseln wird generell keine Zertifikatserneuerung durchgeführt.

Sollen EE-Zertifikate für natürliche oder juristische Personen während der Gültigkeit der validierten Identifizierungsdaten neu ausgestellt werden, muss sich der beantragende Endanwender eindeutig authentifizieren.

Abweichende Verfahren können kundenindividuell vereinbart werden, deren Umsetzung im Ermessen des TSP liegen, wenn sie keiner Zertifizierung nach [EN 319 411-1] unterliegen.

4.8 Zertifikatsänderung

Diese Regelungen sind im TSPS dokumentiert.

4.9 Widerruf und Suspendierung von Zertifikaten

4.9.1 Bedingungen für einen Widerruf von Zertifikaten

Diese Regelungen sind im TSPS dokumentiert.

Sperrberechtigte müssen sich gemäß Abschnitt 3.4 authentifizieren.

4.9.2 Berechtigung zum Widerruf

Diese Regelungen sind im TSPS dokumentiert.

4.9.3 Verfahren für einen Sperrantrag

Der Widerruf eines Zertifikats kann grundsätzlich über eine Online-Schnittstelle durch den Zertifikatsnehmer bzw. seinen autorisierten Vertretern durchgeführt werden.

Bei einem Sperrantrag, der in einer E-Mail eingeht, muss die Absenderadresse der beim Fernsignaturdienst als Benutzernamen, bzw. als Kontakt (juristische Person) hinterlegten Mailadresse entsprechen.

Andere Sperrverfahren können vereinbart werden.

Ein Widerruf in der Zukunft wird nicht angeboten. Der Widerruf über die Online-Schnittstelle wird sofort wirksam. Per E-Mail eintreffende Sperranträge werden spätestens am folgenden Arbeitstag bearbeitet.

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.

Nach erfolgtem Widerruf des Zertifikats wird der Zertifikatsnehmer bzw. der Endanwender über den Widerruf informiert.

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

Die Authentifizierung der Sperrberechtigten erfolgt gemäß Abschnitt 3.4.

4.9.4 Fristen für einen Sperrantrag

Diese Regelungen sind im TSPS dokumentiert.

4.9.5 Zeitspanne für die Bearbeitung des Sperrantrags durch den TSP

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

Die Sperrung über eine Online-Schnittstelle erfolgt umgehend nach erfolgreicher Autorisierung des Sperrantragstellers.

Per E-Mail eintreffende Sperranträge werden spätestens am folgenden Arbeitstag bearbeitet.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Aktuelle Sperrinformationen sind in Sperrlisten vorgehalten, die über das Protokoll LDAP 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-n-qscd, QCP-l-qscd
Sperreinträge verbleiben nach Ablauf der jeweiligen Zertifikatsgültigkeit in den zugehörigen Sperrlisten.

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Siehe Abschnitt 2.3.

4.9.8 Maximale Latenzzeit für Sperrlisten

Sperrlisten werden unmittelbar erstellt und nach spätestens 60 Minuten veröffentlicht.

4.9.9 Online-Verfügbarkeit von Sperrinformationen

Zur Onlineprüfung steht ein OCSP-Dienst zur Verfügung. Die Erreichbarkeit dieses Dienstes wird in Form eines URL in den Zertifikaten angegeben.

4.9.10 Notwendigkeit zur Online-Prüfung von Sperrinformationen

Diese Regelungen sind im TSPS dokumentiert.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Diese Regelungen sind im TSPS dokumentiert.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Diese Regelungen sind im TSPS dokumentiert.

4.9.13 Bedingungen für eine Suspendierung

Diese Regelungen sind im TSPS dokumentiert.

4.10 Statusabfragedienst für Zertifikate

4.10.1 Funktionsweise des Statusabfragedienstes

Diese Regelungen sind im TSPS dokumentiert.

4.10.2 Verfügbarkeit des Statusabfragedienstes

Diese Regelungen sind im TSPS dokumentiert.

4.10.3 Optionale Leistungen

Diese Regelungen sind im TSPS dokumentiert.

4.11 Austritt aus dem Zertifizierungsdienst

Diese Regelungen sind im TSPS dokumentiert.

4.12 Schlüsselhinterlegung und –wiederherstellung

Private EE-Schlüssel der Cloud PKI werden grundsätzlich und ausschließlich vom TSP erstellt und gehalten. Ein gesondertes Verfahren für die Hinterlegung des Schlüssels wird nicht angeboten.

5. Nicht-technische Sicherheitsmaßnahmen

Die Beschreibungen dieses Kapitels beziehen sich auf den Zeitstempeldienst und die CAs, die bei der D-Trust GmbH gemäß [EN 319 421] bzw. [EN 319 411-1] und [EN 319 411-2] betrieben werden.

Die weiteren Regelungen sind im TSPS dokumentiert.

5.1 Bauliche Sicherheitsmaßnahmen

Diese Regelungen sind im TSPS dokumentiert.

5.2 Verfahrensvorschriften

5.2.1 Rollenkonzept- und Berechtigungskonzept

Diese Regelungen sind im TSPS dokumentiert.

5.2.2 Mehraugenprinzip

Diese Regelungen sind im TSPS dokumentiert.

5.2.3 Identifikation und Authentifizierung für einzelne Rollen

Diese Regelungen sind im TSPS dokumentiert.

5.2.4 Rollenausschlüsse

Diese Regelungen sind im TSPS dokumentiert.

5.3 Eingesetztes Personal

Der TSP erfüllt die Anforderungen an das Personal aus [EN 319 421] bzw. [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.

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

Der TSP betreibt einen Zeitstempeldienst gemäß [eIDAS] (siehe Abschnitt 6.8).

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 Geschäftsfortführung

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.

EE-Schlüssel werden vom TSP erzeugt und gehalten. Die Schlüssel werden 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].

QCP-n-qscd, QCP-l-qscd
Der TSP verwendet ausschließlich qualifizierte Signaturerstellungseinheiten und überwacht während der Gültigkeit der ausgegebenen qualifizierten Zertifikate den Status der entsprechenden qualifizierten Signaturerstellungseinheit im Sinne [EN 319 411-2].

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Die privaten EE-Schlüssel werden nicht an den Zertifikatsnehmer ausgeliefert.

Der EE-Schlüssel verbleibt auch während der Nutzung im gesicherten Bereich des TSP.

6.1.3 Lieferung öffentlicher Schlüssel an den TSP

Der TSP nimmt keine öffentlichen Schlüssel von externen Stellen an.

6.1.4 Lieferung öffentlicher CA-Schlüssel an Zertifikatsnutzer

Der öffentliche Schlüssel der CA ist im Zertifikat enthalten. Dieses Zertifikat wird dem Zertifikatsnehmer zum Download angeboten. Die CA- und Dienstezertifikate können aus dem öffentlichen Verzeichnis bezogen werden.

6.1.5 Schlüssellängen

Diese Regelungen sind im TSPS dokumentiert.

Teil der Bundesdruckerei-Gruppe

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.

Zur Sicherung der Dienste-, CA- und EE- Schlüssel werden HSMs bzw. Dienstekarten eingesetzt, die den jeweils bestehenden Anforderungen entsprechen.

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

Das kryptographische Modul, auf dem jeweils die Dienste-, CA- und EE-Schlüssel aufbewahrt werden, befindet sich in der sicheren Umgebung des Trustcenters. Die Aktivierung des jeweiligen privaten Schlüssels sowie ggf. Zugriff auf private EE-Schlüssel erfordert zwei autorisierte Personen.

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.

Diensteschlüssel auf einer Smartcard werden nicht gesichert. Die Verfügbarkeit wird durch die Bereitstellung mehrerer Diensteschlüssel auf redundanten Smartcards sichergestellt.

6.2.5 Archivierung privater Schlüssel

Diese Regelungen sind im TSPS dokumentiert.

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Die allgemeinen Regelungen sind im TSPS dokumentiert.

Ein Transfer privater EE-Schlüssel aus dem kryptographischen Modul kann ausschließlich durch den Trust Service Provider erfolgen. Der Schlüssel verlässt das Modul nie im Klartext.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Die allgemeinen Regelungen sind im TSPS dokumentiert.

EE-Schlüssel liegen mit Hilfe eines HSM gemäß ETSI TS 119 431-1 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 Verwendung der Authentifizierungsmerkmale durch den Endanwender aktiviert.

6.2.9 Deaktivieren privater Schlüssel

Die allgemeinen Regelungen sind im TSPS dokumentiert.

QCP-n-qscd, QCP-l-qscd, LCP
EE-Schlüssel der Cloud PKI werden nach der einmaligen Verwendung deaktiviert.

6.2.10 Zerstörung privater Schlüssel

Die allgemeinen Regelungen sind im TSPS dokumentiert.

Diensteschlüssel auf Smartcards werden durch Zerstörung der Karte vernichtet.

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 Gültigkeitsdauer der Dienste-, CA-Schlüssel und Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximal mögliche Gültigkeitsdauer beträgt 30 Jahre.

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

LCP
63 Monate.

QCP-n-qscd, QCP-l-qscd
EE-Zertifikate werden mit einer maximalen Gültigkeit von 24 Monaten ausgestellt.

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation von Aktivierungsdaten

Die allgemeinen Regelungen sind im TSPS dokumentiert.

Das Authentifizierungsmerkmal wird vom Zertifikatsnehmer erzeugt und im Rahmen der Identifizierung mit dem Zertifikatsnehmer fest verbunden.

QCP-n-qscd
Der zweite Faktor zur Authentifizierung wird vom TSP erzeugt und auf einem separaten Kanal an den Endanwender übertragen.

QCP-l-qscd
Der zweite Faktor zur Authentifizierung (QSealID p12 SMS) wird vom Endanwender beim TSP beantragt und vom TSP erzeugt und auf einem separaten Kanal an den Endanwender übertragen.

6.4.2 Schutz von Aktivierungsdaten

Die allgemeinen Regelungen sind im TSPS dokumentiert.

Der Zertifikatsnehmer ist selbst für den Schutz seiner Authentifizierungsmerkmale verantwortlich.

Teil der Bundesdruckerei-Gruppe

6.4.3 Andere Aspekte von Aktivierungsdaten

Keine Vorgaben.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Diese Regelungen sind im TSPS dokumentiert.

6.5.2 Beurteilung von Computersicherheit

Diese Regelungen sind im TSPS dokumentiert.

6.5.3 Monitoring

Diese Regelungen sind im TSPS dokumentiert.

6.6 Technische Maßnahmen während des Life Cycles

Diese Regelungen sind im TSPS dokumentiert.

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

Diese Regelungen sind im TSPS dokumentiert.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Diese Regelungen sind im TSPS dokumentiert.

6.6.3 Sicherheitsmaßnahmen während des Life Cycles

Diese Regelungen sind im TSPS dokumentiert.

6.7 Sicherheitsmaßnahmen für Netze

Diese Regelungen sind im TSPS dokumentiert.

6.8 Zeitstempel

Der TSP betreibt einen qualifizierten Zeitstempeldienst gemäß [eIDAS], [EN 319 421] und [EN 319 422].

Der Zeitstempeldienst ist redundant aufgebaut und seine Verfügbarkeit in der Produktivumgebung beträgt 99,5%. Der Dienst wird mit einem Monitoring des Services 24x7 überwacht.

Der Zeitstempel kann über eine Online-Schnittstelle gemäß RFC 3161 (Internet X.509 Public Key Infrastructure Time-Stamp Protocol [TSP]) angesprochen werden.

Hierzu wird zur Authentifizierung ein Client-Zertifikat benötigt, welches beim TSP gesondert beantragt werden muss. Die Nutzer des Zeitstempeldienstes unterliegen den Verpflichtungen aus [EN 319 421].

Eine TSU hat nur einen aktiven Zeitstempel-Signaturschlüssel. Die Gültigkeit des TSU-Schlüssels endet zwei Jahre vor Ablauf des zugehörigen Zertifikats. Die Gültigkeit des TSU-Schlüssels ist im öffentlichen Zertifikat festgelegt. Nach Ablauf der Gültigkeit der Schlüssel werden diese nicht mehr für die Signatur des Zeitstempels verwendet.

Ereignisse im Zeitstempeldienst (Änderung des Zeitstempel-Schlüssel/Zertifikate, Synchronisation der Uhrzeit, Verlust der Zeitquelle et cetera) werden geloggt.

Teil der Bundesdruckerei-Gruppe

In diesem Dokument werden spezielle Anforderungen und Umsetzungen mit dem Zertifizierungslevel „BTSP" gekennzeichnet. Des Weiteren sind aus dem Abschnitt 3 dieses Dokumentes nur die Unterkapitel 3.1 und 3.2 anwendbar.

Die Systemzeit des Zeitstempels wird über DCF77 und verlässliche Zeitserver (NTP) im Internet täglich gegen die offizielle Zeit synchronisiert. Bei größeren Abweichungen oder abgelaufenen Dienstezertifikaten wirkt ein Manipulationsschutz, um die Ausstellung von fehlerhaften Zeitstempeln zu verhindern, so dass eine Genauigkeit mit einer maximalen Abweichung unter einer Sekunde gewährleistet werden kann. Schaltsekunden werden durch die Auswertung des DCF77 Signals korrigiert. Die Systeme zur Bereitstellung der Zeiten werden in der gesicherten Umgebung des Rechenzentrums betrieben.

Es werden keine Zeitstempel ausgestellt, wenn die Systemzeit über eine Sekunde offiziellen Zeit abweicht, das Dienstezertifikat nicht gültig ist, die Synchronisation der Zeit nicht mehr gewährleistet werden kann oder der Verdacht auf Kompromittierung besteht.

7. Profile von Zertifikaten, Sperrlisten und OCSP

7.1 Zertifikatsprofile

7.1.1 Versionsnummern

Diese Regelungen sind im TSPS dokumentiert.

7.1.2 Zertifikatserweiterungen

EE-Zertifikate können folgende unkritische Erweiterungen enthalten:

Erweiterung	OID	Parameter
additionalInformation	1.3.36.8.3.15	Diese Nummer kann von D-Trust vergeben werden. Sie dient zur internen Referenzierung von Datensätzen des Antragstellers.

Die weiteren Regelungen sind im TSPS dokumentiert.

7.1.3 Algorithmen-OIDs

In den CA- und EE-Zertifikaten werden in der subjectPublicKeyInfo derzeit folgende Algorithmen verwendet:

- rsaEncryption mit OID 1.2.840.113549.1.1.1
- id-RSASSA-PSS mit OID 1.2.840.113549.1.1.10

Für ECC-Schlüssel wird in den EE-Zertifikaten folgende Kurve verwendet:

- secp521r1 mit OID: 1.3.132.0.35

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

- sha256 WithRSAEncryption mit OID 1.2.840.113549.1.1.11
- sha384 WithRSAEncryption mit OID 1.2.840.113549.1.1.12
- sha512WithRSAEncryption mit OID 1.2.840.113549.1.1.13
- ecdsa-with-SHA256 mit OID 1.2.840.10045.4.3.2
- ecdsa-with-SHA384 mit OID 1.2.840.10045.4.3.3

Teil der Bundesdruckerei-Gruppe

- ecdsa-with-SHA512 mit OID 1.2.840.10045.4.3.4

SHA1 wird nicht verwendet.

7.1.4 Namensformate

Diese Regelungen sind im TSPS dokumentiert.

7.1.5 Name Constraints

Diese Regelungen sind im TSPS dokumentiert.

7.1.6 Certificate Policy Object Identifier

Diese Regelungen sind im TSPS dokumentiert.

7.1.7 Nutzung der Erweiterung „PolicyConstraints"

Diese Regelungen sind im TSPS dokumentiert.

7.1.8 Syntax und Semantik von „PolicyQualifiers"

Diese Regelungen sind im TSPS dokumentiert.

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung CertificatePolicies

Diese Regelungen sind im TSPS dokumentiert.

7.2 Sperrlistenprofile

7.2.1 Versionsnummer(n)

Diese Regelungen sind im TSPS dokumentiert.

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

Diese Regelungen sind im TSPS dokumentiert.

7.3 Profile des Statusabfragedienstes (OCSP)

Diese Regelungen sind im TSPS dokumentiert.

7.3.1 Versionsnummer(n)

Diese Regelungen sind im TSPS dokumentiert.

7.3.2 OCSP-Erweiterungen

Diese Regelungen sind im TSPS dokumentiert.

8. Überprüfungen und andere Bewertungen

Diese Regelungen sind im TSPS dokumentiert.

9. Sonstige finanzielle und rechtliche Regelungen

Bezüglich der entsprechenden Regelungen wird auf Kapitel 9 in der CP sowie ergänzend die [AGB] verwiesen.