# D-TRUST Trust Service Practice Statement (TSPS)

ENGLISH

DEUTSCH

# D-TRUST Trust Service Practice Statement (TSPS)

Version 1.7

# Copyright Notice and License

**Trust Service Practice Statement for D-Trust GmbH**
**©2023 D-Trust GmbH**



Please direct any inquiries regarding any other form of use of this TSPS 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 TSPS.
Please note that only the German version of this TSPS is authoritative.

# Document History

| Version | Date | Description |
|---|---|---|
| 1.0 | 2020-11-10 | ▪ Initial version<br>▪ Version 1.0 of the TSPS is the superior Practice Statement for the following CPS documents:<br>CSM CPS, Root CPS and Cloud CPS<br>▪ Update according to observation report<br>▪ Changes pursuant to CAB/F SC35 (Cleanups and Clarifications) in sections 4.2.2, 4.9.1, 6.1.5 and 6.1.6 |
| 1.1 | 2021-04-23 | ▪ Detailed description of validation methods in section 4.2.1<br>▪ Specification of the requirements for reporting a compromised private key in section 4.9.12<br>▪ Full annual review of the TSPS<br>▪ Amendments in sections 4.2.2, 4.9.1, 4.9.2, 5.4.2, 5.5.1, 5.5.2, 6.1.5, 6.1.6, 6.6.3, 7.1.1, 7.2, 7.2.2, 7.3, 8 |
| 1.2 | 2021-07-02 | ▪ Introduction of qualified seal certificates without QSCD for the EU digital vaccination certificate, see section 7.1.2<br>▪ Update in the context of the BR Self Assessment<br>▪ Editorial changes and additions in sections 2.2, 4.1.2, 4.2.1, 4.2.2, 4.9.1, 5.3.1, 5.7.3, 6.1.6, 6.7, 7.1.1, 7.1.2, 7.1.4, 7.2, 7.3, 8 |
| 1.3 | 2021-10-14 | ▪ Amendments in section 1.3.2, 4.2.1 (Domain), 5.2.2, 5.3.3, 7.1.2 and 8 |
| 1.4 | 2022-04-14 | ▪ Informative introduction of the NCP policy level<br>▪ Amendments in sections 2.4, 4.2.1, 4.10.2 and 6.3.2<br>▪ Changes in section 4.2.2 due to Ballot SC50<br>▪ Inclusion of the online ID function eID in the IDENT procedures under PersIdent in section 4.2.1<br>▪ Renaming of the QCP-w policy level to QEVCP-w and introduction of the QNCP-w policy level<br>▪ Full annual review of the TSPS |
| 1.5 | 2022-11-14 | ▪ Concretisations in sections 1.1.3, 1.4.1, 1.4.2, 4.2.1, 4.9.1, 4.9.12, 4.10.1, 5.5.1, 5.5.2, 6.1.5, 6.1.6, 6.2.11, 6.5.1, 6.6.1, 6.6.3, 7.1.2 and 8 |
| 1.6 | 2023-02-16 | ▪ Amendments in section 4.5.2<br>▪ Editorial changes |
| 1.7 | 2023-06-21 | ▪ Amendments and concretisations in sections 4.2.1, 7.1.2 and 7.2<br>▪ Full annual review of the TSPS |

Contents

# 1. Introduction

This document is the Trust Service Practice Statement (TSPS) for the trust services operated by D-Trust GmbH.

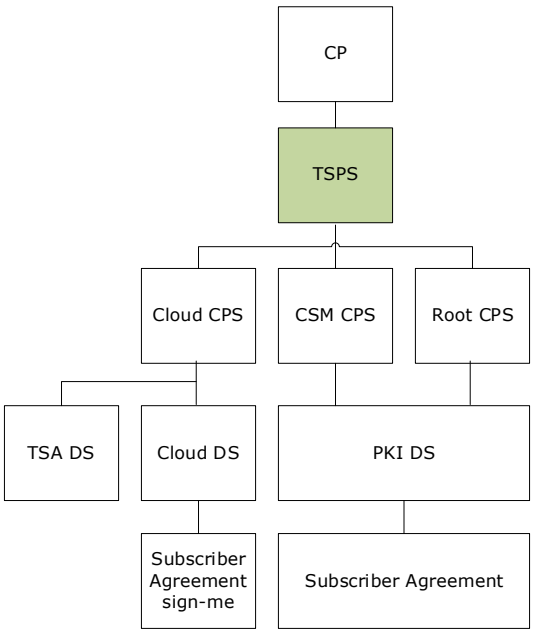
## 1.1 Overview

### 1.1.1 Trust service provider (TSP)

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. At present, the three CPSs named are subject to the TSPS. Others will be gradually added.




**References are shown as follows:**

**These rules are laid down in the CP.**
The rules in this section are not documented in the TSPS or in the respective CPS, but can be found exclusively in the CP.

**These rules are documented in the respective CPS.**
The rules in this section are not documented in the TSPS or in the CP, but can be found exclusively in the respective CPS.

**The specific rules are documented in the respective CPS.**
The rules applicable to all trust services can be found in this TSPS. Rules that are applicable to only a certain trust service can be found in the respective CPS. Rules from the TSPS and the corresponding CPS must be considered.

This TSPS refers to the CP (Certificate Policy) of D-Trust GmbH with OID 1.3.6.1.4.1.4788.2.200.1.

This TSPS and the respective CPS define procedures within the scope of trust services throughout the entire life of CA and end-entity certificates (EE certificates). Minimum measures are defined that must be fulfilled by all PKI entities.

The CP from D-Trust GmbH, the TSPS and the respective CPS are legally binding in as far as this is permitted under German and/or European law. They contain provisions regarding obligations, warranty and liability for the PKI entities. As regards warranties or representations, this TSPS and the respective CPS contain only those warranties or representations expressly granted for this area.

Knowledge of the certification procedures and rules described in this TSPS and of the legal framework enables relying parties to build trust in the components of the PKI and in the PKI entities and to decide to what extent the trust and security level established by the PKI is appropriate for respective application.

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"*.

The specific rules are documented in the respective CPS.

### 1.1.3 Properties of the PKI

D-Trust GmbH defines a separate D-Trust Policy OID for each product, which is additionally included in the pertinent certificates. The D-Trust Policy OIDs are documented in section 1.1.3 of the CP of D-Trust GmbH.

Explanation of the policy levels of qualified trust services:

**QEVCP-w**[1]
EE certificates with QEVCP-w level are qualified TLS certificates according to [EN 319 411-2]; this can be recognized by the QEVCP-w OID in the EE certificates. EE certificates are not issued on smart cards.

Qualified website certificates from D-TRUST CA 2-2 EV 2016 always also meet the requirements for TLS certificates pursuant to EVCP level according to [EN 319 411-1] and [EVGL]; this can be recognized by the EVCP OID in the EE certificates.

**QNCP-w**
EE certificates with QNCP-w level are qualified TLS certificates according to [EN 319 411-2]; this can be recognized by the QNCP-w OID in the EE certificates. EE certificates are not issued on smart cards.

**QCP-l**
EE certificates with QCP-l level are qualified certificates according to [EN 319 411-2]; this can be recognized by the QCP-l OID in the EE certificates. EE certificates are not issued on smart cards.

**QCP-l-qscd**
EE certificates with QCP-l-qscd level are qualified certificates according to [EN 319 411-2]; this can be recognized by the QCP-l-qscd OID in the EE certificates. These EE certificates are issued on smart cards.

[1] The QCP-w policy level has been renamed QEVCP-w in analogy to ETSI EN 319 411-2.

**QCP-n-qscd**
EE certificates with QCP-n-qscd level are qualified certificates according to [EN 319 411-2]; this can be recognized by the QCP-n-qscd OID in the EE certificates. These EE certificates are issued on smart cards.

**BTSP**
BTSP-level certificates are qualified service certificates for the time-stamp service according to [EN 319 421]; this can be recognized by the BTSP OID in the service certificates.

Explanation of the policy level of non-qualified (publicly trusted) trust services:

**EVCP**
EE certificates with EVCP level are TLS certificates. The fact that they are EV certificates can be recognized by the EV OID (as described in section 1.1.3 of the CP/CPS) in the EE certificates. EV certificates are not issued on smart cards.

**OVCP**
EE certificates with OVCP level include TLS certificates and machine certificates that show the name of an organization. OV certificates are not issued on smart cards.

**DVCP**
EE certificates with DVCP level include TLS certificates in which the subject (end-entity) is identified via the domain name. DV certificates are not issued on smart cards.

**NCP**
NCP-level EE certificates are personal certificates or organization certificates. The name of an organization can be optionally included as an attribute in these personal certificates. NCP certificates are not issued on smart cards.

The NCP policy level is included in the documentation for information purposes. In the future, LCP level products will be migrated to NCP level. The respective policy level can be recognized by the OID in EE certificates.

**LCP**
LCP-level EE certificates are simple personal certificates or organization certificates. The name of an organization can be optionally included as an attribute in these personal certificates. LCP certificates are not issued on smart cards.

**V-PKI**
EE certificates with V-PKI certification level (administration PKI) are simple personal certificates or function certificates. V-PKI certificates are made available via an online interface and are not issued on smart cards.

Products with non-qualified policy levels (such as EVCP+, NCP+), which require use of a secure signature creation device, are currently not offered, however, subscribers are free to use an SSCD to create and store their private keys.

The specific rules are documented in the respective CPS.

## 1.2 Document name and identification

| | |
|---|---|
| Document name: | D-TRUST Trust Service Practice Statement (TSPS) |
| Version | 1.7 |

## 1.3 PKI entities

### 1.3.1 Certification authorities (CAs)

Certification authorities (CAs) are operated by the trust service provider (TSP) and issue certificates and revocation lists.

The following types of certificates are possible, depending on the PKI:

- Personal certificates for natural persons (EE certificate)
- Seal certificates for legal entities (EE certificate)
- Group certificates for groups of people (EE certificate)
- Service certificates for legal entities (EE certificate)
- Certificates for web servers, devices or machines (EE certificate)
- Certification authorities (lower-level CA certificates of the TSP)

Root authorities issue certificates exclusively with the extension basicConstraints: cA=TRUE (CA certificate). Lower-level CAs issue EE certificates and/or further CA certificates. The name of the certification authority is shown in the "issuer" field of the certificates issued and in the CRLs.

### 1.3.2 Registration authorities (RAs)

The RA identifies and authenticates subscribers or end-entities (subjects), and it collects and checks requests for different certification services.

The concrete tasks and obligations of the RA as the representative of the TSP and/or CA are defined and finally set forth in the respective agreement with the RA. The RA is unambiguously identified by the TSP in this context.

Registration authorities that are not operated by D-Trust are subject to the same requirements.

RA operator activities, both internal and external, take place on security-critical systems used for certificate issuance and are protected by enforced multi-factor authentication (see also section 5.2.2).

TLS certificate requests are processed exclusively by D-Trust's internal RA. Domain validation is therefore carried out exclusively by D-Trust itself and is generally neither delegated nor outsourced to third parties (e.g. to an external RA).

The domain check within the scope of the email verification method in section 4.2.1 for S/MIME certificates is also carried out exclusively by D-Trust itself.

### 1.3.3 Subscribers

Subscribers are natural persons or legal entities who apply for and hold EE certificates. The subscriber can be identical to the end-entity *(subject)* whose name appears in the certificate.

End-entities (EE, *subjects*) use the private end-entity keys (EE keys). The identity of the end-entity is linked to the certificate and the related key pair. The end-entity can be identical to the subscriber. Depending on the PKI, end-entities can be:

- Natural persons
- Legal entities
- Groups of people or teams
- Devices or machines

- Functions that are performed by staff of an organization
- IT processes

The subscriber is responsible for the key and certificate when the key material was generated by the subscriber or as soon as the trust service provider (TSP) passes it on to the subscriber. Moreover, additional obligations exist under [EN 319 411-1] and/or [EN 319 411-2] or BSI [TR-03145-1]. As soon as the application is submitted at the very latest, subscribers are provided with the CP, this TSPS, the CPS and the Subscriber Agreement, informing them of these obligations which they are obliged to adhere to.

**QCP-n-qscd**
The subscriber and end-entity must be identical in the case of qualified signature certificates.

**QEVCP-w, QNCP-w, QCP-l, QCP-l-qscd, EVCP, DVCP, OVCP, NCP, LCP, V-PKI**
In the event that the subscriber and the end-entity are not identical, the subscriber and the end-entity are responsible for adherence to the Subscriber Agreement.

**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, QCP-l, QCP-l-qscd**
Seal and TLS certificates are issued exclusively to legal entities.

**BTSP**
Service certificates for issuing qualified time stamps are issued exclusively for D-Trust GmbH. Only a certificate is used for the qualified time stamp.[2]
Users of the time-stamp service according to [EN 319 421] are natural persons or legal entities who obtain the time-stamp service within the Cloud PKI from the trust service provider (TSP).

### 1.3.4 Relying parties

Relying parties are natural persons or legal entities who use the certificates of this PKI and have access to the services of the TSP.

The specific rules are documented in the respective CPS.

## 1.4 Certificate usage

### 1.4.1 Permitted certificate usage

CA certificates are used exclusively and in line with their extension (BasicConstraints, PathLengthConstraint) for issuing CA or EE certificates and CRLs.

EE certificates can be used for applications that are compatible with the types of usage shown in the certificate (keyUsage).

Relying parties are responsible for their own actions. Relying parties are responsible for assessing whether TSPS and CPS meet with the requirements of an application and whether use of the particular certificate is suitable for a given purpose.

The rules of the CP of D-Trust GmbH also apply.

### 1.4.2 Forbidden certificate usage

Types of use (keyUsage) other than those listed in the certificate are not permitted.

The rules of the CP of D-Trust GmbH also apply.

[2]See repository: www.d-trust.net/repository

**V-PKI**
Within the scope of the V-PKI, the provisions of the CP V-PKI BSI are additionally applicable.

### 1.4.3 Service certificate usage

The TSP uses service certificates to perform trust services in accordance with [eIDAS]. Service certificates are issued by the TSP itself and for its own use. They are subject to the requirements of the respective type of certification.

The types of use include:

- CA certificates for CA and certificate creation
- Signing status information[3]
- Signing time stamps[4]

## 1.5 Policy administration

### 1.5.1 Responsibility for the document

This TSPS and the subordinate CPS documents are maintained by D-Trust GmbH. The representative of management is responsible for document release.

This TSPS and the subordinate CPS documents are reviewed at least once a year by the TSP and updated as required. Changes are indicated by a new version number in the respective updated document and are promptly republished in D-Trust's repository after the current version has been released by management. If employees or external parties (such as customers, exIdent offices, resellers) are affected by such changes, they will be informed in advance or, if necessary, appropriately trained to implement the changes.

The contact data of the TSP is documented in section 1.5.1 of the CP.

### 1.5.2 Reporting security incidents with certificates

These rules are documented in the CP.

### 1.5.3 Compatibility of CPs of external CAs with this CPS

Both in CA and in EE certificates, further CPs can be referenced via policy OIDs which do not contradict this TSPS or the respective CPS. The reference of a policy OID in the certificate extensions serves as confirmation of compatibility of the certification practices with the referenced CP (for instance, NCP 0.4.0.2042.1.1 according to [EN 319 411-1]).

The specific rules are documented in the respective CPS.

## 1.6 Definitions and acronyms

### 1.6.1 Definitions and names

The general rules are documented in the CP.

The specific rules are documented in the respective CPS.

[3] OCSP information is signed using special OCSP service certificates.

[4] Time stamps are signed using special service certificates.

1.6.2 Acronyms

Certificate Policy (CP)

| | |
|---|---|
| IDN | Internationalized Domain Name |

General rules are laid down in the CP.

1.6.3 References

General rules are laid down in the CP.

## 2. Publication and Repository Responsibility

2.1 Repositories

The general rules for repositories are documented in the CP.

The specific rules are documented in the respective CPS.

2.2 Publication of certificate information

The TSP publishes the following information:

- CA certificates
- CP of D-Trust GmbH
- This TSPS
- Certificate revocation lists (CRLs) and online certificate status protocol (OCSP)
- EE demo certificates

The specific rules are documented in the respective CPS.

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

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

2.3 Publication frequency

These rules are documented in the respective CPS.

2.4 Repository access control

Certificates, revocation lists, the TSPS, the CPS and CPs can be publicly retrieved 24/7 at no cost. The repository service offers at least 98.5% availability. The TSP ensures that in the event of a malfunction, downtime is limited to a maximum of four hours.

Read only access is unrestricted. Changes in repository and web contents are carried out exclusively by the TSP.

The relevant parts of other non-public documents can be made available on request for inspection against proof of a legitimate interest.

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

These rules are documented in the respective CPS.

### 3.1.2 Need for telling names

These rules are documented in the respective CPS.

### 3.1.3 Anonymity or pseudonyms of subscribers

These rules are documented in the respective CPS.

### 3.1.4 Rules for the interpretation of different name forms

These rules are documented in the respective CPS.

### 3.1.5 Unambiguity of names

These rules are documented in the respective CPS.

### 3.1.6 Recognition, authentication and the role of brand names

These rules are documented in the respective CPS.

## 3.2 Initial identity verification

### 3.2.1 Proof of ownership of the private key

These rules are documented in the respective CPS.

### 3.2.2 Identification and authentication of organizations

These rules are documented in the respective CPS.

### 3.2.3 Identification and authentication of natural persons

These rules are documented in the respective CPS.

### 3.2.4 Non-verified subscriber information

These rules are documented in the respective CPS.

### 3.2.5 Verification of request authorization

These rules are documented in the respective CPS.

### 3.2.6 Criteria for interoperation

See section 1.5.3.

## 3.3 Identification and authentication for re-keying requests

These rules are documented in the respective CPS.

## 3.4 Identification and authentication for revocation requests

These rules are documented in the respective CPS.

# 4. Certificate Life Cycle Operational Requirements

## 4.1 Certificate request and registration

### 4.1.1 Request authorization

CA certificates are exclusively issued to legal entities.
The specific rules are documented in the respective CPS.

### 4.1.2 Registration process and responsibilities

The TSP warrants compliance with the registration process. Sub-tasks can be carried out by partners or external providers under a corresponding agreement if such partners or external providers fulfil the requirements of the CP, TSPS and the CPS.

Depending on the application path and policy level, certain documents must be agreed to which then become part of the agreement and therefore legally binding. A related overview can be found in the repository:

https://www.d-trust.net/files/dokumente/pdf/terms-and-conditions_product-service_1.pdf

To send the registration data, communication between the external registration authorities and the internal registration authority at the TSP end is encrypted and authenticated via an TLS connection.

Depending on the policy level, the TSP determines the registration process as follows:

**QEVCP-w, QNCP-w, EVCP, QCP-l, QCP-l-qscd**

Prior to completing the registration process, the subscriber receives the CP, TSPS, CPS and a Subscriber Agreement and undertakes to abide by the terms and conditions thereof. The documents are published. The Subscriber Agreement complies with the requirements of [EN 319 411-1] and [EN 319 411-2]. The application also includes, if necessary, the subscriber's consent to the certificates being published. The Subscriber Agreement corresponds to the requirements of [BRG] and [EVGL]. Proof is kept electronically or in printed form.

**QCP-n-qscd**

Prior to completing the registration process, the subscriber receives the CP, TSPS, CPS and a Subscriber Agreement and undertakes to abide by the terms and conditions thereof. The documents are published. The Subscriber Agreement complies with the requirements of [EN 319 411-1] and [EN 319 411-2]. The application also includes the subscriber's consent to the certificates being published or not. The Subscriber Agreement corresponds to the requirements of [BRG] and [EVGL]. Proof is kept electronically or in printed form.

**OVCP, DVCP**

Prior to completing the registration process, the subscriber receives the CP, TSPS, CPS and a Subscriber Agreement and undertakes to abide by the terms and conditions thereof. The documents are published. The Subscriber Agreement complies with the requirements of [EN 319 411-1]. The application also includes the subscriber's consent to the certificates being published. The Subscriber Agreement corresponds to the requirements of [BRG]. Proof is kept electronically or in printed form.

**NCP, LCP**

The subscriber receives the CP, TSPS, CPS and a Subscriber Agreement and undertakes to abide by the terms and conditions thereof. The documents are published. The Subscriber Agreement complies with the requirements of [EN 319 411-1]. The application also includes the subscriber's consent to the certificates being published. If the subscriber is not the end-

entity, the subscriber must prove that the obligations under this document and the Subscriber Agreement have been transferred to the end-entity.

**V-PKI**

The subscriber receives the CP, TSPS, CPS and a Subscriber Agreement and undertakes to abide by the terms and conditions thereof. The CPS is published. If the subscriber is not the end-entity, the subscriber must prove that the obligations under this document and the Subscriber Agreement have been transferred to the end-entity.
The subscriber must ensure that the private keys from the V-PKI are passed onto and used by authorized end-entities only.

The specific rules are documented in the respective CPS.

## 4.2 Processing the certificate request

### 4.2.1 Performing identification and authentication processes

The customer must be identified before the certification and trust services of D-Trust GmbH can be used. The registration process and an identification method permitted for the selected product must be completed and all the required evidence must be furnished.

Natural persons or organizations can be authenticated and further certificate-relevant data verified before or after submission of the application, but must be completed before certificates are issued and key material, if any, and PINs are handed over.

Natural persons must be unambiguously identified. In addition to the full name, other attributes, such as place and date of birth or other applicable individual parameters, must be used to prevent natural persons from being mistaken. If legal entities are named in the certificate or if legal entities are subscribers, their complete name and legal status as well as any relevant register information must be verified.

Identification of natural person is carried out according to section 3.2.3. of the respective CPS.

**EVCP**

A natural person may act in the role of contract signer on behalf of the requester if they can adequately demonstrate that they have been authorized to represent the legal entity. The contract signer can authorize one or more natural persons to assume the role of certificate approver (primary operator). This authorization must be proven and will be verified. In this case, the TSP verifies the name and title of the contract signer and the certificate approver. The certificate approver can authorize one or more natural persons to assume the role of certificate requester.
The requirements of section 11.8 [EVGL] are met.

The TSP checks the following data on the HADDEX sanctions list:

- The name of the applicant, the contract signer, the certificate approver or
- the applicant's jurisdiction of incorporation, registration or
- place of business.

If an entry is found on this list, cooperation will not take place.

To check the certificate request signature according to section 11.9 [EVGL] and depending on the order and distribution process, the following methods are used to securely identify the signer's name and title (function at the organization):

1. Use of a correspondingly secure login method that identified the signer prior to signing and

2. use of a digital signature that was created with reference to a correspondingly verified certificate.

In the event that methods 1 or 2 cannot be used, the applicant can be contacted using one of the verified communication methods according to section 4 [EVGL], requesting that the contract signer or the certificate requester confirm that they signed the certificate request.

D-Trust has implemented a process for identifying high-risk certificate requests and for extended processing of these certificate requests in order to prevent misuse.

The TSP defines the following IDENT procedures for determining the identity of a natural person:

**PersIdent**
Using a valid ID document, the natural person must prove his or her identity in person before an RA (e.g. the TSP itself, a contractually obliged organization or authority) or an authorized identification partner who fulfils the requirements of the TSPS and the CPS.

Acceptable documents are ID cards or passports of nationals of a Member State of the European Union or of a country of the European Economic Area as well as documents offering an equivalent degree of safety. Identification information is archived as proof.

If the RA of the TSP or the external registration and/or identification office of the TSP is unable to carry out the personal identification of the subscriber or subject itself, then the accredited identification procedures from other partners can be used as an alternative.

**eID**
Natural persons with their place of residence in Germany authenticate themselves using a valid, official electronic ID function according to Article 9 of the eIDAS Regulation. Accepted documents are German ID cards or electronic residence permits issued by the Federal Republic of Germany with an electronic ID function. Identification information is archived as proof.

**NotarIdent**
Using a valid ID document, the natural person or authorized representative of a legal entity must identify themselves in person before a notary who fulfils the requirements of the TSPS and the CPS. The TSP only accepts identification by notaries who are listed in the accepted public notary registers in the respective EU Member States. Acceptable documents are ID cards or passports of nationals of a Member State of the European Union or of a country of the European Economic Area, as well as documents offering an equivalent degree of safety. The notary is obliged to respect the relevant data protection requirements. Documents used as proof are filed.

**BotschaftsIdent**
Using a valid ID document, natural persons or authorized representatives of a legal entity can identify themselves in person before a consular officer at a Germany embassy. Acceptable documents are ID cards or passports of nationals of a Member State of the European Union or of a country of the European Economic Area, as well as documents offering an equivalent degree of safety. Identification by a consular officer is confirmed by an official seal. Documents used as proof are filed.

**Dok-Ident**
The contents to be verified are compared to the application data on the basis of copies (printed copies or electronically scanned documents or fax transmissions). An out-of-band mechanism by phone is used for random queries in order to verify the correctness of contents. Permissible documents are those specified for the Pers-Ident procedure, as well as EU driving licences that have a statutory expiry date, extracts from commercial or equivalent registers which are not older than six months, doctorate or habilitation certificates as well as documents of an equivalent importance. Documents used as proof are filed.

**HR-DB**
The TSP enters into an agreement with an organization (subscriber) and stipulates that only valid data is to be transmitted which meets with the requirements of the CP. As part of standard personnel processes, the personal identification of an employee is carried out at least once.

An authorized employee or official of an organization forwards extracts from the organization's human resources database and/or requests generated on the basis of such data to the TSP via a secure communication channel. The organization is obliged to respect the relevant data protection requirements. The TSP trusts in the correctness and unambiguity of the data transmitted. At the time the tokens are handed over at the latest, the subscriber informs the end-entity of the latter's obligations under the Subscriber Agreement. The following items are filed:

- electronic or printed copies of the data transmitted,
- confirmation/proof of the forwarder as the organization's "authorized employee" or "authorized official", respectively,
- proof that such data was made available by an authorized employee as well as proof that the subscriber has consented to the Subscriber Agreement.

When it comes to the identification and authentication of organizations and domains as well as other certificate-relevant attributes, the following procedures are used to check the application in order to identify credentials:

**C confirmation**
An authorized signatory of the organization confirms certificate-relevant information. This is carried out in writing, with the possibility of electronically signed confirmation being also accepted. The authorization to sign must be proven either with proof of the organization's existence or in another suitable manner. Documents used as proof are filed.

**A confirmation**
Authorized employees or officials within an organization or trusted third parties (for instance, partners of the TSP or government bodies) confirm certain certificate-relevant information which they are authorized to confirm. This is carried out in writing, with the possibility of electronically signed confirmation being also accepted. Documents used as proof are filed.

**Out-of-band mechanisms**
The TSP uses out-of-band mechanisms in order to check the correctness of application data using communication channels and verification methods which the subscriber is unable to influence. Documents used as proof are documented and filed electronically or in printed form.

Proof of existence of organizations or natural persons can, for instance, be provided to the TSP in the form of a bank transfer, direct debit or payment by credit card. The TSP trusts the bank whose customer is either the organization or the natural person. The following methods are also permissible on the part of the TSP:

a. Verification by telephone using telephone numbers obtained from a public telephone directory.

b. Verification via an e-mail address, provided that this e-mail address was obtained from the QGIS or QIIS registers.

In order to identify natural persons, the TSP can send a letter "by registered mail with acknowledgement of receipt" to the subscriber whose signature on the receipt is then compared to the signature on the stored evidence documents or in the application documents.

The end-entity's affiliation with an organization can also be verified by way of a verification letter sent "by registered mail with acknowledgement of receipt" to the organization to the attention of the end-entity. The signature on the registered letter is compared to the signature on the stored proof documents or in the application documents. Affiliation with an organization, e-mail address, contents of extensions as well as any further certificate-relevant data can also be confirmed in the form of an enquiry by telephone to be made by the TSP using a public telephone directory.

**Register**
The application data is compared (or captured) manually or automatically to copies of extracts from printed or electronic registers. Acceptable registers are registers of government bodies, so-called Qualified Government Information Sources (QGISs), such as registration courts, German Federal Central Tax Office, the Federal Financial Supervisory Authority, professional associations under public law, the German Patent and Trade Mark Office or equivalent organizations and registers organized under private law, so-called Qualified Independent Information Sources (QIISs), such as D-U-N-S, comparable business databases, government bodies organized under private law. Register entries are only accepted as valid if they do not include attributes of the "invalid", "inactive" or equivalent types.

**Register check as part of PSD2**
As part of PDS2 and pursuant to section 5 of [TS 119 495], the register check also includes a check of the PSD2-specific information issued by the National Competent Authority (NCA) which is shown in the certificate:

For QEVCP-w, QNCP-w, QCP-l and QCP-l-qscd with PSD2 extension, the role of the payment service provider (PSP) is additionally checked and included in the certificate. A payment service provider is assigned one or more roles (RolesOfPSP) by the National Competent Authority (NCA):

i) Account servicing payment service provider;
OID: id-psd2-role-psp-as { 0.4.0.19495.1.1 }
Role: PSP_AS

ii) Payment initiation service provider;
OID: id-psd2-role-psp-pi { 0.4.0.19495.1.2 }
Role: PSP_PI

iii) Account information service provider;
OID: id-psd2-role-psp-ai { 0.4.0.19495.1.3 }
Role: PSP_AI

iv) Payment service provider issuing card-based payment instruments
OID: id-psd2-role-psp-ic { 0.4.0.19495.1.4 }
Role: PSP_IC

For QEVCP-w, QNCP-w, QCP-l and QCP-l-qscd with PSD2 extension, the National Competent Authorities (NCAs) will continue to be described by a name "NCAName" and an identifier "NCAId". The European Banking Authority (EBA) has provided a list of valid values for "NCAName" and "NCAId" which are published in [TS 119 495], Annex D.

Documents used as proof are filed.

**Non-Register**
Government bodies/institutions under public law confirm certificate-relevant information with their official seal and signature. Furthermore, government bodies can also be authenticated on the basis of legal legitimation. Documents used as proof are filed.

**Check within the scope of the administration PKI (V-PKI)**
Applicants/contract partners are reported to BSI. As soon as BSI has confirmed the applicant/contract partner, they are then connected to the CSM and are permitted to obtain certificates from the V-PKI.

**Public bodies**
The TSP enters into an agreement with public bodies and stipulates that only data is to be transmitted which meets with the requirements of the CP. An authorized employee or official of this public body forwards to the TSP personal data and/or application forms created on the basis of such data via a secure communication channel. The public body is obliged to respect the relevant data protection requirements. Moreover, the same procedures as those of HR-DB apply.

**Verification via domain**

**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP (TLS certificates)**
Control over a domain used in a DNS name must be clearly demonstrated by the registered organization. In this case, the domain is exclusively validated by the TSP itself using the domain validation methods supported by D-Trust according to the Baseline Requirements and the methods required or recommended by Mozilla (see section 1.3.2).

D-Trust uses the following domain validation methods according to [BRG]:

- 3.2.2.4.2 E-mail, fax, SMS, or postal mail to domain contact: With this method, a random value is transmitted exclusively by e-mail. The *Whois* protocol is not used to determine the e-mail address as a domain contact. If receipt of th random value is correctly proven to the TSP, the domain is considered validated.
- 3.2.2.4.4 Constructed e-mail to domain Contact: With this method, a random value is transmitted exclusively by e-mail. This e-mail is structured as follows: local part according to [BRG] section 3.2.2.4.4, followed by an @ sign and followed by the ADN. If receipt of the random value is correctly proven to the TSP, the domain is considered validated.
- 3.2.2.4.7 DNS change: With this method, a random value is sent by e-mail or a random value is displayed in the CSM application platform. The secret must be stored in the CNAME, TXT or CAA-RR of the ADN or of the ADN provided with a prefix label starting with an underscore. If the random value is correctly provided to the TSP in this way, the domain is considered validated.
- 3.2.2.4.13 E-mail to DNS CAA contact: With this method, a random value is transmitted exclusively by e-mail. The e-mail is sent to the DNS CAA contact. The CAA Resource Record Set required for this is determined using the search algorithm defined in RFC 8659,
  section 3. If the random value is correctly proven to the TSP, the domain is considered validated.
- 3.2.2.4.14 E-mail to DNS TXT contact: With this method, a random value is transmitted exclusively by e-mail. The e-mail is sent to the DNS TXT record e-mail contact of the ADN for validation of the FQDN. If the random value is correctly proven to the TSP, the domain is considered validated.
- 3.2.2.4.18 Agreed-Upon change to website v2: With this method, a random value is sent by e-mail or a random value is displayed in the CSM application platform. If the random value according to [BRG], section is proven in the manner described in section 3.2.2.4.18, the domain is considered validated.

D-Trust documents for each validated domain or FQDN the verification method used, including the BRG/SBR version number used at the time. The records are archived.

**OVCP, DVCP**

The domain validation methods mentioned are also suitable for validating Wildcard Domain Names. In addition, the requested domain will be checked against a "public suffix list" to prevent the issuance of a wildcard certificate for a registerable portion of a Country Code Top-Level Domain Namespace.
Method 3.2.2.4.18 used for domain validation of wildcard TLS certificates will be discontinued by 30 November 2021 at the latest.

**QEVCP-w, QNCP-w, EVCP**

No wildcard TLS certificates are issued for this policy level.

**QEVCP-w, QNCP-w, EVCP**

In the case of TLS certificates with QEVCP-w, QNCP-w and EVCP level, the domain name is additionally checked against blacklists of known phishing domains and other blocklists.

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

Domain names not subject to a registration obligation, domains of the top-level domain ".int" as well as top-level domains in general and onion certificates are not permitted.

In order to prevent attacks, such as the "homographic spoofing of Internationalized Domain Names (IDNs)", D-Trust has IDNs individually checked by validation specialists. The release is carried out according to the four-eyes principle. If there are any concerns, the issuance of certificates will be refused.

If e-mail addresses are used as part of domain validation, the e-mail addresses must be used in the TSP validation process as found in the approved sources.

The results of the enquiry are filed.

**Control over the mailbox**

**NCP, LCP**

Control of a mailbox (P.O. box) must be demonstrated by the organization registered in the certificate request using one of the following methods:

- **Via domain**

  Domain verification is carried out in the same way as in the previous section "Verification via domain" for TLS certificates.

- **Via e-mail**

  The TSP sends an e-mail with a secret to the e-mail address to be confirmed, receipt of which must be confirmed within 24 hours (challenge response/secret exchange). Once validation has been completed, the associated certificate must be issued within 30 days.

**QCP-n-qscd**

E-mail addresses from natural persons are not checked.

The results of the enquiry are filed.

**IP addresses**

IP addresses are not validated and are not permitted.

**CAA**

CAA stands for Certification Authority Authorization. This Resource Record (according to RFC6844) determines which CA is authorized to issue TLS certificates for the Internet domain.

When it receives the application and immediately before activating the certificate, D-Trust checks Fully Qualified Domain Names (FQDNs) for a corresponding CAA entry in the "issue"

and "issuewild" field. Validated domains can be used for certificate generation if the CAA entry is empty or if the domain holder entered D-Trust as the CA (d-trust.net, dtrust.de, d-trust.de, dtrust.net).

D-Trust cannot issue TLS certificates if a different CA is stated in the “issue” or “issuewild” field of the CAA Resource Record.

### 4.2.2 Acceptance or rejection of certificate requests

The four-eyes principle is used, as a minimum, when checking the certificate contents and the related proof.

In the event that any inconsistency occurs during identity verification or during validation of the data in the certificate application or of the proof documents that cannot be fully resolved, the application will be rejected.

Other reasons for rejection include:

- Suspected violation of third-party name rights
- Non-adherence to deadlines for proof of data
- Payment arrears of the applicant in relation to the TSP
- Circumstances that give rise to the suspicion that issuing a certificate could or would bring the operator of the CA into disrepute (e.g. due to suspected phishing or other fraudulent or malicious use)
- If the requirements of sections 6.1.5 and 6.1.6 of the TSPS are not met when generating the key pair
- If there is a clear indication that the specific method for generating the private key was incorrect
- If the TSP is aware that the method used by the requester to generate their private keys could be compromised
- If the TSP is aware that the requester's private key was previously compromised, e.g. according to provisions of section 4.9.1.1 [BRG], or
- If the TSP is aware, based on the public key, that the requester has used a weak method to calculate the private key, e.g. a Debian weak key

The TSP is entitled to reject certificate applications without giving reasons.

When the TSP receives PKCS#10 or other certificate requests, the contents thereof are checked by the TSP for correctness.

**NCP, LCP, QCP-n-qscd, QCP-l-qscd, QCP-l**
Certain certificate contents (for instance, O or OU) can be determined by agreement.

If the TSP receives certificate data in advance via a client-enabled online interface, the certificate data can be checked in advance. When the actual certificate request is forwarded after checking by the TSP, certificates can be issued immediately.

The request is not deemed to be unconditionally accepted until the TSP has made a positive decision regarding the certificate request and the certificate requested has been handed over.

### 4.2.3 Deadlines for processing certificate requests

There are no rules regarding the deadlines for processing certificate requests.

## 4.3 Certificate issuance

### 4.3.1 Procedure of the TSP for issuing certificates

Digital certificates are produced in the high-security area of the trust service provider. The technical events for creating certificates are logged and/or recorded in auditable form.

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

When a certificate is created, it is ensured that the correct time is used.

The TSP either files the complete request documentation in accordance with section 5.5 in auditable form, or the TSP concludes agreements with partners pursuant to which the complete application documents and/or requests have to be filed in a secure manner until the period according to section 5.5.2 expires. This application documentation can be assigned to the certificate created at any time.

The specific rules are documented in the respective CPS.

### 4.3.2 Notification of the subscriber that the certificate was issued

The subscriber does not receive separate notification after the certificate has been issued.

The specific rules are documented in the respective CPS.

## 4.4 Certificate handover

### 4.4.1 Certificate handover procedure

The specific rules are documented in the respective CPS.

The subscriber is obliged to check that the certificate contents are correct before using the certificate.

In the event that the subscriber detects errors in the certificates or during their use, the subscriber must communicate this to the TSP without delay. The certificates will then be revoked.

Incorrect data in the certificate is only deemed to be a contractual defect within the meaning of the law in as far as the TSP performs a check of the data affected by such defect according to this CPS. Otherwise the relevant rules for remedial measures according to the applicable General Terms and Conditions [AGB] are applicable to defects and their existence.

Acceptance by the customer does not take place as the delivery constitutes a service rather than a work within the meaning of German civil law.

### 4.4.2 Publication of the certificate by the TSP

These rules are documented in the respective CPS.

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

These rules are documented in the respective CPS.

## 4.5 Key pair and certificate usage

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

These rules are documented in the respective CPS.

### 4.5.2 Public key and certificate usage by relying parties

The certificates issued by D-Trust can be used by all relying parties. However, they can only be relied upon if:

1) the certificates are used in line with the types of use shown there (key use, extended key use, restricting extensions, if applicable).

2) all other precautionary measures determined in agreements or otherwise were taken[5] and if any restrictions in the certificate as well as any application-specific measures were taken by the relying party and found to be compatible.

3) the verification of the certificate-chain is carried out successfully right through to the trusted root certificate. This is done, to validate the trust status of the PKI (e.g. EU Trusted List according to eIDAS[6] or roots stores of software providers).

4) it is verified that the certificate is not listed as revoked on the associated Certificate Revocation List (CRL), or the status of the certificates is checked via the Online Certificate Status Protocol (OCSP) and the outcome is positive[7].

If the check mechanism from point 3 did not work, the existence and validity of a certificate can be checked via the Online Certificate Status Protocol (OCSP).

The specific rules are documented in the respective CPS.

## 4.6 Certificate renewal

These rules are documented in the respective CPS.

## 4.7 Certificate renewal with re-keying

As a rule, any changes to the information, which should be taken into consideration when renewing the certificate, must be notified to D-Trust GmbH no later than six weeks prior to expiration of the certificate.

The specific rules are documented in the respective CPS.

## 4.8 Certificate modification

Certificate modification is not offered.

## 4.9 Certificate revocation and suspension

### 4.9.1 Conditions for certificate revocation

The procedures of the TSP fulfil the requirements of [EN 319 411-1].

**QEVCP-w, EVCP**
The procedures of the TSP additionally fulfil the requirements of [EN 319 411-2] and [EVGL].

**QCP-l, QNCP-w**
The procedures of the TSP additionally fulfil the requirements of [EN 319 411-2].

Subscribers, third parties concerned, or other third parties are called upon to immediately request revocation if they suspect that private keys have been compromised or that any content data of the certificate is no longer correct (for instance, termination of the subscriber's affiliation with an organization).

[5] https://www.d-trust.net/en/support/repository

[6] Regulation (EU) No 910/2014

[7] Positively verified means that a third party can determine via the OCSP status query that D-Trust has issued the requested certificate. See section 7.3.

If the subscriber applies for revocation, this will be executed immediately. If a third party concerned or any other third party applies for revocation, a risk assessment is carried out prior to revocation. The subscriber is informed in advance about the consequences of revocation. However, the deadlines laid down in section 4.9 [BRG] must be observed if the certificate is subject to these guidelines.

A certificate is revoked, for instance, under the following circumstances:

- if requested by the subscriber and/or the third party concerned (for instance, the organization named in the certificate),
- if the certificate was issued on the basis of incorrect data,
- if the original certificate request was not authorized and the authorization is not granted retroactively,
- if the TSP becomes aware that the private CA or EE key has been communicated to an unauthorized person or organization that is not affiliated with the subscriber,
- if the private key of the subscriber associated with the public key in the certificate has been compromised,
- if it can be proven to the TSP that the associated private key can be calculated based on the public key in the certificate,
- if it can be proven to the TSP that the domain authorization or validation via the FQDN in the certificate cannot be trusted,
- if the TSP determines that the certificate has not been issued in accordance with the applicable CP; TSPS, CPS and [BRG] or that the sub-CA does not meet the requirements of the applicable CP, TSPS, CPS or [BRG],
- if the TSP determines that the requester has breached the Subscriber Agreement or the applicable CP, TSPS, CPS or [BRG],
- if certificate contents that were valid at the time the request was submitted become invalid during the validity period, e.g. due to a change in name or loss of organizational affiliation,
- if the TSP discontinues its activities and if such activities are not continued by another TSP.

**Qualified certificates with PSD2 extension**
In the case of qualified website authentication certificates (QWACs) with PSD2 extension, the National Competent Authorities (NCAs), as the issuer of the PSD2-specific information, are authorized to initiate revocation if the information in section 4.2.1 (Register) published by these authorities has been changed and this can affect the validity of the certificate.

Revocation of a qualified website authentication certificate (QWAC) with PSD2 extension is additionally carried out pursuant to section 6.2.6 [TS 119 495] under the following conditions:

- the authorization of payment service provider (PSP) has been revoked,
- any role of the payment service provider (PSP) included in the certificate has been revoked.

Irrespective of the foregoing, the TSP is entitled to revoke certificates if:

- D-Trust as the trust service provider (TSP) is obliged by law to revoke the certificate,
- the private key of the issuing or of a higher-level CA has been compromised,

- the certificate of the issuing or of a higher-level CA has been revoked,
- weaknesses are detected in the encryption algorithm used which pose serious risks for the permitted applications during the certificate life cycle,
- the hardware and software used show security shortcomings which pose serious risks for the permitted applications during the certificate life cycle,
- unambiguous assignment of the key pair to the subscriber is no longer ensured,
- a certificate was obtained on the basis of false data,
- there are reasonable grounds to suspect that a certificate is being misused,
- the customer is in default with payment after two reminders, or has violated the applicable General Terms and Conditions [AGB],
- the contract was terminated or expired in any other manner,
  - the CA is transferred to another TSP without the relevant revocation information of the issued EE certificates being transferred too.

**NCP, LCP**

Certificates that are capable of signing or encrypting e-mails and contain an e-mail address are also subject to the revocation reasons listed in Mozilla Root Store Policy 2.7, Chapter 6.2. Depending on the reason for revocation, the certificate must be revoked within 24 hours or can be revoked within five days.

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

The deadlines set out in section 4.9 of [BRG] are complied with. A certificate of a subscriber or of an issuing CA is revoked if at least one of the revocation reasons from section 4.9 of [BRG] applies.

Pursuant to [BRG], the TSP offers PKI entities and third parties an additional 24x7 service for TLS certificates and for their issuing or higher-level CA. This service can be used in cases of suspicion to report that a private key has been compromised, a public key misused as well as fraud or technical non-conformities.

Security incidents with D-Trust certificates can be described and reported according to section 1.5.2 of the CP.

Revocations are marked with the time of revocation. Retroactive revocation is not possible. Furthermore, revocation cannot be reversed.

Parties authorized to request revocation must identify themselves according to section 3.4 of the applicable CPS. Revocation requests that cannot be authenticated are neither accepted nor executed.

### 4.9.2 Authorization to revoke

The TSP is generally authorized to revoke certificates.

Subscribers are always authorized to revoke their certificates if they can authenticate themselves to the TSP.

If a certificate contains information regarding the subscriber's power to be represented by a third party, such third party is also authorized to request revocation of the certificate concerned.

If a certificate contains official, professional or other information about a person (e.g. "tax advisor"), then the third party who consented to the inclusion of such information in the certificate, or the body responsible for the official, professional or other information about the person, may also demand its revocation if the power of representation or the conditions

for the official, professional or other information about the person should cease to exist after inclusion in the certificate.

Additional third parties authorized to request revocation can be specified and will then always be authorized to request revocation of these certificates.

Any person who is able to state the correct revocation password to the TSP is deemed to be authorized to request revocation.

**EVCP, OVCP, DVCP, QEVCP-w, QNCP-w**
In principle, any other third party can submit a certificate problem report in accordance with CP 1.5.2. In justified cases, the TSP revokes the certificate in accordance with section 4.9 of [BRG].

4.9.3 Revocation request procedure

General information regarding certificate revocation can be retrieved via the following website:

https://www.d-trust.net/en/support/revocation

The specific rules are documented in the respective CPS.

4.9.4 Revocation request deadlines

The end-entity or subscriber is solely responsible for ensuring that they or a person authorized to request revocation on their behalf immediately request revocation as soon as reasons for revocation of the respective certificate become known.

4.9.5 Time span for processing a revocation request by the TSP

These rules are documented in the respective CPS.

4.9.6 Methods available for checking revocation information

These rules are documented in the respective CPS.

4.9.7 Publication frequency of certificate revocation lists

These rules are documented in section 2.3 of the respective CPS.

4.9.8 Maximum latency time for certificate revocation lists

These rules are documented in the respective CPS.

4.9.9 Online availability of revocation information

These rules are documented in the respective CPS.

4.9.10 Need for online verification of revocation information

There is no obligation for online validation of revocation information.

4.9.11 Other forms for notification of revocation information

No stipulation.

4.9.12 Special requirements if the private key is compromised

D-Trust revokes a certificate due to a compromised private key if key compromise can be proven using one of the following methods:

- Transmission of the compromised private key or

- Signing of a CSR with the common name entry "Proof of Key Compromise for D-TRUST" by the compromised private key

D-Trust provides a Certificate Problem Report for reporting a key compromise with TLS certificates. In the case of all other certificates, the report is sent to an e-mail address. This is described in the section 1.5.2 of the CP and must be used.

If a key compromise is successfully proven, D-Trust will revoke the certificate according to the specifications in section 4.9. of [BRG].

#### 4.9.13 Conditions for suspension

Certificate suspension is not offered.

## 4.10 Certificate status query service

#### 4.10.1 How the certificate status query service works

The certificate status query service is available via the OCSP protocol. The availability of the service is indicated as a URL in the certificates.

The formats and protocols of the services are described in sections 7.2 and 7.3 of the respective CPS.

The system time of the OCSP responder is synchronized daily using the DCF77 time signal and reliable time servers (NTP) on the Internet.

#### 4.10.2 Availability of the certificate status query service

The status check service is available 24 hours a day, 7 days a week and has an availability of 99.95%. The TSP ensures that in the event of a malfunction, downtime is limited to a maximum of four hours.

The requirements of section 4.10.2 of [BRG] are met.

#### 4.10.3 Optional services

No stipulation.

## 4.11 Withdrawal from the certification service

The validity of the certificate ends on the expiry date shown in the certificate. The request to revoke a certificate by a subscriber or third party authorized to request revocation leads to revocation by the TSP. The TSP's main contractual duties are thereby completely fulfilled.

If revocation lists are offered within a trust service, as soon as the trust service is discontinued a last CRL with the entry "99991231235959Z" will be created in the *nextUpdate* field and published.

If a trust service offers an OCSP information service, OCSP information is usually signed with an OCSP signer certificate from the respective PKI of the EE certificate. If this is no longer possible (revoked, expired), an OCSP signer certificate from a CA with identical security (identical level, e.g. eIDAS or Basic) is used.

## 4.12 Key escrow and recovery

These rules are documented in the respective CPS.

#### 4.12.1 Conditions and procedures for escrow and recovery of private keys

These rules are documented in the respective CPS.

4.12.2 Conditions and procedures for escrow and recovery of session keys

These rules are documented in the respective CPS.

# 5. Facility, Management and Operational Controls

The specific rules are documented in the respective CPS.

D-Trust operates an Information Security Management System (ISMS) in accordance with ISO/IEC 27001. Operation of the TSP is subject to this ISMS. An Information Security Policy regulates the binding requirements for operation. This was approved by the management of D-Trust GmbH and communicated to all employees of the TSP. The Security Policy is reviewed and updated each year, and also on an event basis.

If changes due to processes or operations lead to an update of the Security Policy, the resulting changes for TSP operation must be approved by management. The updated and approved Security Policy must be communicated promptly by the managers to all the employees concerned. Compliance with the Security Policy is mandatory for employees. At least once a year, employees receive instruction in existing and updated security rules.

With the exception of a few identification services, no other TSP activities are outsourced to external service providers. Where applicable, necessary aspects of the Security Policy will also become mandatory for service providers.

## 5.1 Physical controls

An infrastructure security concept documents the physical controls in detail. The implementation of this concept has been audited by a recognized conformity assessment body. D-Trust GmbH has received accreditation for the security area of the TSP, confirming that this area meets all high-protection requirements of the Trusted Site Infrastructure catalogue, TSI V3.2 Level 3 (according to the catalogue of audit criteria for a "Trusted Site Infrastructure" issued by TÜV Informationstechnik GmbH). The audit for re-accreditation is repeated every two years.

## 5.2 Procedural controls

### 5.2.1 Roles and authorization concept

Documentation includes a role and authorization concept where TSP management assigns employees to one or more roles with these employees then receiving corresponding authorizations in a managed process. The authorizations of the individual roles are limited to those authorizations which these roles need to fulfil their tasks. The assignment of authorizations is revised by security management on a regular basis, and authorizations are cancelled immediately when no longer needed.

Roles with security responsibility for TSP operation, known as "Trusted Roles" (including the tasks of security officer, system administrator, system operator, system auditor, registration officer, revocation officer and validation specialist) are defined in D-Trust's authorization concepts. These roles may only be assumed by competent and reliable employees. Employees who are assigned these roles receive separate instruction and must actively confirm their acceptance of such roles.

Job descriptions are created for the respective roles. These define the tasks as well as the minimum level of qualification and experience required for each role. An employee can perform one or more roles on condition that these roles are not mutually exclusive. Employees must also prove that they have the qualifications and experience required for these roles.

Employees receive regular training to ensure that they can perform their roles and assume the related responsibilities. Information security management regularly initiates awareness-

raising activities to ensure that the applicable security rules are adhered to. Employees can attend training courses in order to qualify for further roles.

The requirements for the roles are documented in the job descriptions and can be viewed by employees at any time.

In the case of mutually exclusive roles, an employee can assume only one such role (four-eyes principle). A risk assessment is carried out on a regular basis.

Employees working in the area of certification and revocation services act independent and are free from commercial and financial constraints that could influence their decisions and acts. The organizational structure of the TSP considers and supports employees in the independence of their decisions.

#### 5.2.2 Four-eyes principle

The four-eyes principle is the minimum requirement for particularly security-critical operations. This is ensured by technical and organizational measures, such as access authorization and verification of knowledge.

When validating subject data (especially TLS certificates), it is ensured that an experienced validation specialist is called upon and works according to the four-eyes principle.

Security-critical systems used for certificate issuance are generally protected by multi-factor authentication.

#### 5.2.3 Identification and authentication for individual roles

Before being allowed to access any security-critical applications, the employee concerned must have been successfully authenticated. Only authorized and identified employees may access security-critical areas. Event logs enable the identification of employees who performed past actions; these employees are accountable for their acts.

#### 5.2.4 Role exclusions

The role concept includes various role exclusions in order to prevent any conflict of interests, ensure the four-eyes principle and avoid any harmful behaviour.

### 5.3 Personnel controls

These rules are documented in the respective CPS.

#### 5.3.1 Qualifications, experience and clearance requirements

The TSP ensures that persons employed in the area of the certification service have the knowledge, experience and skills necessary for this activity. This includes, among others, the requirements of [BRG] and [EVGL].

The identity, reliability and professional qualifications of employees are verified before they commence work. Regular and demand-driven training ensures competency in the respective fields of activity as well as general information security. Training and proficiency checks are documented.

Line managers, in particular, are selected according to special criteria. They must demonstrate that they have knowledge of security procedures for staff with security responsibility and that they have sufficient experience of information security and risk assessment in relation to the trust service provided. Evidence can be provided in the form of certificates and CVs. If the required qualification cannot be proven sufficiently, it must be acquired through appropriate training before the employee can take over management functions.

#### 5.3.2 Background checks

Individuals who work in security-relevant areas of the TSP are also regularly required to present clearance certificates.

#### 5.3.3 Training

The TSP trains certification service personnel. The aim is for each staff member to be thoroughly familiar with the verification tasks and for all staff members to implement the instructions in the same manner in order to detect and prevent common threats to the information verification process (including phishing and other social engineering tactics). Training covers the requirements from the company's own certification practices as well as external applicable requirements (e.g. BRG, ETSI, BSI).

Employees who fail to attend mandatory training may be excluded from security-relevant activities.

The TSP also operates an ISMS certified according to ISO 27001 that provides employees with security-relevant rules and/or rules of conduct.

#### 5.3.4 Frequency of training and information

The TSP trains certification service personnel at the beginning of their employment, annually and as required.

#### 5.3.5 Job rotation frequency and sequence

Role changes are documented. The corresponding employees are trained.

#### 5.3.6 Sanctions for unauthorized actions

The TSP does not employ any unreliable persons in the certification service.

Violations by employees of the policies or processes of TSP operations are analyzed and evaluated. If the relationship of trust cannot be ensured, these employees are excluded from security-relevant activities.

#### 5.3.7 Independent contractor requirements

External personnel working in the field of trust services fulfil the requirements laid down in section 5.3 of this TSPS and are subject to the sanctions laid down in section 5.3.6 of this TSPS.

#### 5.3.8 Documentation supplied to personnel

Comprehensive process instructions and procedures for all activities define the relevant employee roles and rights as well as the corresponding manual and automated checks. The technical security infrastructure of D-Trust GmbH ensures that deviations from these defined processes are not possible.

### 5.4 Audit logging procedures

#### 5.4.1 Monitoring access

Video surveillance and tracking are used to monitor access.

Visitors must be reported in name at least 24 hours before arrival and must be accompanied by a TSP member of staff at all times.

### 5.4.2 Risk monitoring

Relevant assets are correctly identified, and any changes to these assets are checked or, if applicable, released by the TSP staff commissioned by management. Based on this, risks are then identified, analyzed, assessed, handled and monitored.

A risk analysis is carried out at least once a year. This provides a comprehensive analysis of threats to the TSP's operations and defines requirements and counter-measures. Furthermore, an analysis of the residual risks shows the appropriateness of the residual risk and, if reasonable, this is accepted by management.

## 5.5 Records archival

### 5.5.1 Types of records archived

A distinction is made between electronic and printed documents.

Documents archived are the complete application documents, documents concerning procedures (CP, TSPS, CPS), certificates, revocation documentation, electronic files and reports/logs regarding the certificate life cycle. Events are recorded, including related time information. If applicable, this also includes the corresponding system reports/logs that were generated as part of the stated events.

**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP**
The events specified in section 5.4.1 of [GL-BRG] are, as a minimum, logged in an auditable form.

The TSP ensures that unauthorized modification of the data archived by it is not possible during the archiving periods.

Furthermore, security-relevant events are suitably recorded. The system time is synchronized daily using the DCF77 time signal and reliable time servers (NTP) on the Internet.

### 5.5.2 Retention period for archive

The traceability of the identification procedure used as the basis for issuing a certificate is a quality feature of the certificate. Application and verification documents as well as data concerning the certificate life cycle and the certificates themselves are created and archived according to the statutory storage periods or those specified in certifications and depending on the specific product[8].

**QCP-n-qscd, QCP-l-qscd, QCP-l**
In the case of qualified signature and seal certificates, the provisions of section 16 (4) of the Trust Services Act (VDG) on permanent archival apply to certificates, identification data, including contact data. This corresponds to the entire duration of operations by the trust service provider (TSP).

Before discontinuing its operations, the TSP is required to hand over the data to the Federal Network Agency or another qualified TSP.

**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP**
According to section 5.5.2 of [BRG], archiving certificate verification data, such as application data, identification data, revocation data and the certificates themselves, is subject to a retention period of seven years after the certificate has lost its validity.

[8] If, in addition to the non-qualified certificates of the Root PKI, the token also contains other qualified end-entity certificates, the archival periods of such certificates will then apply.

For the audit logs defined in section 5.4.3. of [BRG], a retention period of at least two years is applicable.

**NCP, LCP, V-PKI**

As part of archiving certificate verification data, for instance, application data, identification data, revocation data and the certificates themselves, the data is stored for a period of at least seven years after the certificate has lost its validity.

Audit logs must be stored for a period of at least two years.

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

Before operation is discontinued, the archived data is transferred to another (qualified) trust service provider (TSP) or to Bundesdruckerei. Bundesdruckerei has warranted to the TSP compliance with the minimum requirements regarding retention periods.

Certificates and registration data are archived and tracked by the TSP or by contractually bound partners or external providers that meet the requirements of the CP, TSPS and CPS, so that this archived data can be used in case of a necessary backup. The requirements of TR-03145-1 section 6.10 should be observed.

The period begins after expiration of the term of validity of the certificate that was issued last on the basis of these documents.

Event logs of IT systems are stored for at least six months. Video recordings of persons and recordings of administrative activities are stored for a period of 90 days.

The system time for the archival system is synchronized daily using the DCF77 time signal and reliable time servers (NTP) on the Internet.

### 5.5.3 Archive protection

The archive of the trust service provider (TSP) is located in secure rooms and is subject to the role and access concept of the TSP.

### 5.5.4 Archive data backup

Confidentiality and integrity of data are maintained. Documentation is set up immediately so that subsequent changes are discovered. Both European and German data protection requirements are adhered to.

### 5.5.5 Requirements for time stamping of records

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

### 5.5.6 Archiving (internally/externally)

Archiving is carried out internally at the TSP as well as externally in rooms affording equivalent protection.

### 5.5.7 Procedure for obtaining and verifying archive information

The process of obtaining and verifying archive information is subject to the role concept of the trust service provider (TSP).

## 5.6 Key change at the TSP

In due time before a CA or sub-CA expires, new CA or sub-CA keys are generated, and new CA or sub-CAs set up and published. This also applies to service certificates if these are relevant.

## 5.7 Compromise and disaster recovery at the TSP

### 5.7.1 Incident and compromise handling procedures

The TSP has a contingency concept and a restart plan which are known to the roles involved and which can be implemented by these roles when necessary. Responsibilities are clearly distributed and are known.

Should a system recovery be necessary, the responsibilities and corresponding "Trusted Roles" are laid down in D-Trust's authorization concept and are known to the respective employees. See section 5.2.1.

### 5.7.2 Recovery after resources have been compromised

Recovery procedures have been defined for restoring the operating capability of the TSP. Backups are made on a daily basis and after changes. Backups are stored in a different fire zone. The recovery of critical CA systems is regularly tested in emergency drills.

### 5.7.3 Compromising of the private CA key

In the event of compromising or communication of uncertainty of algorithms or associated parameters, the TSP will initiate the following:

- The CA certificates concerned as well as their certificates already issued and not yet expired will be revoked.
- The subscribers involved will be informed about the incident and its effects.
- The respective supervisory body and in the case of publicly trusted CA certificates the Certificate Consumer members of the CA Browser/Forum will be informed and the incident published on the websites of the TSP together with a statement that any certificates that were issued by this CA are no longer valid and that the revocation status can be verified.

The analysis of the reasons for the compromise will be used, if possible, to take suitable measures in order to prevent future cases of compromise. Taking the reasons for the compromise into consideration, new CA signature keys will be generated and new CA certificates issued.

### 5.7.4 Disaster recovery options

In an emergency, the TSP decides, depending on the type of incident, whether a recovery of the backup of the CA described in section 6.2.4 is to be carried out or whether the procedure described in section 5.7.3 is to be adopted in the case of compromise. Following this, an attempt is made to return to normal operations with all of the necessary services for a subscriber being restored.

## 5.8 Closure of the TSP or termination of services

D-Trust has a continuously updated termination plan.

When the services of CAs are terminated, the TSP informs all subscribers and terminates all access possibilities for the TSP's subcontractors with regard to the CAs concerned. All certificates issued by the CAs concerned which are still valid are revoked. The private CA keys concerned are destroyed.

In the event of scheduled discontinuation of its operations, the TSP will inform all end-entities, subscribers and third parties in advance.

The repository service and request documents as well as the repository (CP, CPS, TSPS and CA certificates) will be handed over to Bundesdruckerei GmbH and continued there under equivalent conditions. Continuation of the repository service until the end of the term of validity of the EE certificates is warranted and will be handed over either to another TSP or to Bundesdruckerei GmbH.

Bundesdruckerei has warranted to the TSP compliance with these minimum requirements.

On termination of operations, all functionalities of the CAs concerned will be discontinued.

**QCP-n-qscd, QCP-l-qscd, QCP-l**
The certificate database together with the revocation information and the repository (CP, TSPS, CPS and CA certificates) are transferred to the Federal Network Agency in accordance with sec. 16 (1) VDG.

## 6. Technical Security Controls

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

### 6.1 Key pair generation and installation

#### 6.1.1 Generation of key pairs

CA keys and keys for service certificates are generated in a "FIPS 140-2 Level 3" OR a CC-evaluated (according to Protection Profile EN 419 211-5) hardware security module (HSM). The HSM is located in the high-security area of the trust service provider. The key ceremony takes place according to defined procedures. Depending on the CA, the key ceremony is performed by trusted roles in the presence of the security officer and, if necessary, under the supervision of an independent third party. The activities during the key ceremony are checked and recorded using a checklist. During key generation, the enforcement of the role concept and thus the 4-eyes principle is enforced by the voluntary entry of the activation data for signature generation of the CA certificate. Whenever CA keys are generated, an independent auditor is present if necessary or, following key generation, the auditor can use a video recording in order to verify that the key generation process was carried out correctly. Furthermore, the creation of CA keys and, if applicable, service certificates will be documented for:

- Products within the **Root CPS and CSM CPS:** according to [EN 319 411-1] or [EN 319 411-2],
- Products within the **Cloud CPS:** according to [EN 319 421] or [EN 319 411-1] or [EN 319 411-2]

The specific rules are documented in the respective CPS.

#### 6.1.2 Private key delivery to subscribers

These rules are documented in the respective CPS.

#### 6.1.3 Public key delivery to the TSP

These rules are documented in the respective CPS.

#### 6.1.4 CA public key delivery to relying parties

These rules are documented in the respective CPS.

#### 6.1.5 Key lengths

RSA keys with a key length of at least 2048 bits are currently used for CA and service certificates.

ECC keys with 384 bits are used for the new root CAs and sub-CAs with policy levels DVCP, QCP-n and QCP-l.

RSA keys with a key length of at least 2048 bits and ECC keys with a key length of at least 256 bits are currently used for EE certificates.

**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP**
The RSA key lengths used can be divided by modulus 8.

The signature and encryption algorithms are referred to in section 7.1.3.

### 6.1.6 Determining the key parameters and quality control

This TSPS explains the respective definitions for the following policy levels:

- **OVCP, DVCP, NCP, LCP:** Service, CA and EE certificates are issued on the basis of keys that comply with [ETSI-ALG], [EN 319 411-1] and [BRG] in their latest applicable version in as far as compatibility in the use environment is ensured.
- **QEVCP-w, EVCP:** CA and EE certificates are exclusively issued on the basis of keys that comply with [ETSI-ALG], [EN 319 411-1], [EN 319 411-2], [BRG] and [EVGL] in their latest applicable version.
- **QNCP-w:** CA and EE certificates are exclusively issued on the basis of keys that comply with [ETSI-ALG], [EN 319 411-1], [EN 319 411-2], and [BRG] in their latest applicable version.
- **QCP-l, QCP-l-qscd, QCP-n-qscd:** EE certificates are exclusively issued on the basis of keys that comply with [ETSI-ALG], [EN 319 411-1] and [EN 319 411-2] in their latest applicable version.
- **V-PKI:** EE certificates are issued on the basis of keys that were generated for federal government projects according to cryptographic specifications from BSI [TR-02102-2].

**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP**
For ECDSA key pairs, the TSP ensures that the key represents a valid point on the NIST P-256, NIST P-384, or NIST P-521 elliptic curve.

The signature and encryption algorithms are referred to in section 7.1.3.

### 6.1.7 Key usage purposes

Private root CA keys are exclusively used to sign CA certificates, service certificates and certificate revocation lists. All other private CA keys are used to sign CA certificates, service certificates, EE certificates and certificate revocation lists (see 7.1.2).

The EE keys may only be used for the types of use stated in the certificate. The types of use are defined in the *keyUsage* and *extKeyUsage* fields in the certificate and may be restricted by further extensions (see section 7.1.2).

Private keys of service certificates for time stamps are used exclusively within the scope of the time-stamp service.

## 6.2 Private key protection and cryptographic module engineering controls

### 6.2.1 Cryptographic module standards and controls

Throughout their entire life cycle (including delivery and storage), the modules are protected against manipulation by suitable technical and organizational controls.

The CA keys are protected by an HSM that was evaluated according to FIPS 140-2 Level 3 OR according to Common Criteria (pursuant to Protection Profile EN 419 211-5).

The specific rules are documented in the respective CPS.

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

These rules are documented in the respective CPS.

### 6.2.3 Private key escrow

These rules are documented in the respective CPS.

### 6.2.4 Private key backup

A backup of the private CA keys exists. A CA key backup must be carried out at the HSM by two persons authorized for this activity and takes place in the secure environment of the trust service provider. The backup system is subject to the same requirements and backup measures as the productive system. Recovery of private keys also requires two authorized persons. Further copies of the private CA keys do not exist.

The specific rules are documented in the respective CPS.

### 6.2.5 Private key archival

Private CA and EE keys are not archived.

### 6.2.6 Transfer of private keys to or from cryptographic modules

Transfers of private CA keys to or from the HSM are limited to backup and recovery purposes. Adherence to the 4-eyes principle is compulsory. Private CA keys exported to/imported from another HSM are protected by encryption.

The specific rules are documented in the respective CPS.

### 6.2.7 Storage of private keys in cryptographic modules

The private keys for CA and service certificates are contained in encrypted form in the HSM.

The specific rules are documented in the respective CPS.

### 6.2.8 Activation of private keys

The private CA and service keys can only be activated according to the 4-eyes principle, by the authorized roles and for the permitted types of use (*keyCertSign, cRLSign*).

The specific rules are documented in the respective CPS.

### 6.2.9 Deactivation of private keys

The private keys for CA and service certificates are deactivated by termination of the connection between the HSM and the application by the Trusted Roles provided for this purpose.

The specific rules are documented in the respective CPS.

### 6.2.10 Destruction of private keys

When the scheduled useful life of the private CA keys expires, these keys are deleted by the Trusted Roles provided for this purpose. Useful life is determined in accordance with ETSI ALGO Paper TS 119 312 and SOG-IS. This is accomplished by deleting the private key on the HSM and simultaneous deleting of the backups on data media. When the HSM is shut down, the private keys in the device are deleted.

When the files containing the private EE key are deleted, the private key is then also destroyed.

The specific rules are documented in the respective CPS.

#### 6.2.11 Assessment of cryptographic modules

The TSP operates suitable hardware-based and software-based key generators according to [EN 319 421] or [EN 319 411-1] and [EN 319 411-2] and in the case of federal government projects according to BSI [TR-02102-1] in order to warrant the key quality.

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

The list of QSCDs in Germany is made publicly available by a regulatory authority, i.e., the Federal Network Agency (BNetzA, Bundesnetzagentur).

D-Trust monitors the validity period of the QSCDs used. It is ensured that no certificates are issued that have a validity period that is longer than the validity period of the QSCD or, alternatively, it is ensured that the certificates are revoked when the validity of the QSCD expires.

### 6.3 Other aspects of key pair management

#### 6.3.1 Archiving of public keys

Public service, CA and EE keys are archived in the form of the certificates generated.

#### 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.

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

Issuing CAs do not issue EE certificates that are valid for longer than the CA certificate itself.

The specific rules are documented in the respective CPS.

### 6.4 Activation data

#### 6.4.1 Activation data generation and installation

The activation data of the service and CA keys is requested by the smart card or HSM. Adherence to the 4-eyes principle is compulsory.

The specific rules are documented in the respective CPS.

#### 6.4.2 Protection of activation data

The activation data of the service and CA keys is made up of two secrets with one authorized employee each knowing one of these. Only authorized employees can access the activation data.

The specific rules are documented in the respective CPS.

#### 6.4.3 Other aspects of activation data

These rules are documented in the respective CPS.

### 6.5 Computer security controls

#### 6.5.1 Specific technical security requirements in the computer systems

The computers, networks and other components used by the TSP ensure in their given configuration that only those actions can be carried out which are not in conflict with the CP of D-Trust GmbH and

- for products within the **CSM CPS:** the CSM CPS, [EN 319 411-1] or [EN 319 411-2] and, in the case of EV certificates, [EVGL],

- for products within the **Root CPS:** the Root CPS, [EN 319 411-1] or [EN 319 411-2] and, in the case of EV certificates, [EVGL],
- for products within the **Cloud CPS:** the Cloud CPS, [EN 319 421], [EN 319 411-1] or [EN 319 411-2],
- for products within the **Device CPS:** the Device CPS, [TR-03145-1],
- for products within the **E.ON CPS:** the E.ON CPS and [EN 319 411-1] or
- for products within the **Uniper CPS:** the Uniper CPS and [EN 319 411-1]

The TSP's computer security for exposed systems is ensured, amongst other things, by multi-level security systems providing perimetric virus protection, end-point protection and integrity-protecting tools.

It is ensured that security-relevant software updates are installed at the appropriate point in time on the relevant systems. Evaluation and, if necessary, elimination of identified vulnerabilities takes place within 48 hours. If it is not possible to resolve the problem within 48 hours, the assessment will include a concrete action plan. Any deviations are suitably documented by the TSP and, if necessary, addressed in the TSP's risk management.

Subscribers and relying parties must use trusted computers and software.

The system time of the relevant CA systems is ensured by a radio clock with a redundant connection.

All systems required for operation (status service, revocation service, certificate management) are redundant systems with at least one active/passive cluster (hot standby).

**LCP, NCP**

When reapplying for certificates with keys generated by the TSP, redundant systems are used that have at least one backup server (cold standby).

### 6.5.2 Assessment of computer security

The computers, networks and other components used for the CA keys are checked, inspected and audited by recognized conformity assessment bodies and are suitably monitored in accordance with [EN 319 401].

### 6.5.3 Monitoring

The relevant systems are continuously monitored in order to ensure their availability. Each failure is recorded, documented, classified according to its severity and prioritized. The handling of critical notifications is part of the incident management process. Notifications on security-relevant events are sent to a central place and assessed according to their criticality.

In the event of prolonged disruptions where a service is no longer available, the parties affected will be informed every 24 hours on the current status of trouble-shooting.

## 6.6 Life cycle technical controls

Productive server systems receive security-relevant configurations via central management systems. Services that are not urgently required are deactivated. The configurations are checked every 15 minutes. Any deviations from the central security guidelines are immediately corrected in the configurations.

The requirements of section 5 of [BRG] are already adequately considered during the planning of all systems operated by the TSP or on behalf of the TSP.

### 6.6.1 Security controls during development

Security requirements are already analyzed during the draft design phase for all system development projects carried out by or on behalf of the TSP. The results are defined as requirements for development.

D-Trust's test environment for development, testing and staging systems is separate from its production systems.

### 6.6.2 Security controls in conjunction with computer management

Administration of computers, networks and other components is strictly limited to personnel authorized according to the role concept. Log files are regularly analyzed with a view to rule violations, attempted attacks and other incidents. Audit logging procedures begin when a device is set into operation and end when it is disposed of.

### 6.6.3 Life cycle security controls

Any devices used are operated in accordance with their manufacturers' instructions. Prior to being set into operation, they are meticulously checked and inspected. They are only set into operation if it is clear that they have not been manipulated. In the case of suspected manipulation of a component, any action planned will not be carried out and the incident will be reported. In order to enable an immediate and co-ordinated response to any security-relevant incidents, the TSP defines clear-cut escalation rules for the individual roles.

Capacity requirements and utilization as well as the suitability of the systems involved are monitored and adapted as required. Devices or data media will be taken out of service and disposed of in such a manner that any misuse of functionalities or data is ruled out. Changes in systems, software or processes are subject to a documented change management process. Security-critical modifications are checked by the Information Security Officer. After expiration of the term of validity of CAs, the private keys are destroyed.

Electronic data or printed reports are used to document all relevant events which influence the life cycle of the CA, of the certificates issued and of the keys generated, and such electronic data or printed reports are stored on long-lived media in an auditable form. The company's media are safely protected against damage, theft, loss or compromising depending on their respective classification within the scope of the TSP's documentation guideline.

Penetration tests are carried out at least once a year by an independent and competent body. Furthermore, vulnerability scans are initiated at least once every three months. The results of the penetration test report are archived internally.

## 6.7 Network security controls

A network concept is implemented at the CAs that ensures that the relevant CA systems are operated in particularly well-protected network zones. The network architecture of the TSP features a multi-level concept of network security zones. The root CAs are operated in the network security zone with the highest security requirements.

In order to protect the processes of the TSP, firewalls and intrusion detection/prevention mechanisms are used that allow expressly permitted connections only. D-Trust operates network segments with different protection requirements and separates networks for employees and Internet-related uses from server networks. The systems are subject to regular inspection and revision, the employees in charge are accountable. Anomalies are reported by technical systems and organizational processes and addressed by a defined incident handling procedure as well as related processes.

Redundancy ensures the availability of the Internet connection. There are two permanent connections to the provider on two different routes. If the provider's access point fails, the system automatically switches to the second connection.

Cryptographic mechanisms are used to protect data traffic with a high protection demand outside the networks protected by the TSP for which integrity or confidentiality must be ensured.

The physical security of the networks operated and used by the TSP is ensured and adapted to the structural conditions and any changes therein.

D-Trust complies with the specific requirements of [NetSec-CAB].

### 6.8 Time stamps

The TSP operates a time-stamp service.

The specific rules are documented in the Cloud CPS.

## 7. Profiles of Certificates, Certificate Revocation Lists and OCSP

### 7.1 Certificate profiles

#### 7.1.1 Version numbers

Certificates are issued in X.509v3 format and in accordance with EN 319 412-2, -3 or -4, respectively.

The certificate serial number is randomly generated using a cryptographically secure pseudo-random number generator (CSPRNG) and contains an entropy of 128 bits.

#### 7.1.2 Certificate extension

The selection of the extension is largely product-dependent.

CA certificates contain the following *critical* extensions ("mandatory field"):

| Extension | OID | Parameter |
|---|---|---|
| *keyUsage* | 2.5.29.15 | *keyCertSign, cRLSign* |
| *basicConstraints* | 2.5.29.19 | *Ca=TRUE, (pathLenConstraint)* |

CA certificates can include the following *non-critical* extensions ("optional"):

| Extension | OID | Parameter |
|---|---|---|
| *extKeyUsage*[9,10] | 2.5.29.37 | According to [RFC 5280], [RFC 6818]<br>**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP:**<br>For sub-CA certificates, the extension "extKeyUsage" is used according to the subordinate EE certificate profiles. |

[9] Not used in root CA certificates.

[10] Used exclusively for QEVCP-w, QNCP-w, EVCP, OVCP and DVCP.

| | | |
|---|---|---|
| | | The anyExtendedKeyUsage KeyPurposeId is generally not used. |
| *authorityKeyIdentifier*[9] | 2.5.29.35 | 160-bit SHA-1 hash of the issuer key |
| *subjectKeyIdentifier* | 2.5.29.14 | 160-bit SHA-1 hash of the subject public key |
| *cRLDistributionPoints* | 2.5.29.31 | Address(es) of the CRL issuing authority/authorities |
| *authorityInfoAccess*[9] | 1.3.6.1.5.5.7.1.1 | *accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation {…} accessMethod=caIssuers {1.3.6.1.5.5.7.48.2}, accessLocation {…}* |
| *certificatePolicies*[9] | 2.5.29.32 | OIDs of the CPs supported |
| *subjectAltName*[9] | 2.5.29.17 | Alternative holder's name |

Further extensions can be added; they must comply with [X.509], [RFC 5280], [RFC 6818], [ETSI EN 319 412] and [ETSI-ALG] or they must be described in a referenced document.

EE certificates contain the following *critical* extensions:

| Extension | OID | Parameter |
|---|---|---|
| *keyUsage* | 2.5.29.15 | Possible are:<br>*digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, decipherOnly*<br>and combinations thereof |

EE certificates can include the following non-critical extensions:

| Extension | OID | Parameter |
|---|---|---|
| *extKeyUsage* | 2.5.29.37 | According to [RFC 5280], [RFC 6818][11]<br>**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP:**<br>only "id-kp-serverAuth" and "id-kp-clientAuth" are allowed |
| *authorityKeyIdentifier* | 2.5.29.35 | 160-bit SHA-1 hash of the issuer key |
| *subjectKeyIdentifier* | 2.5.29.14 | 160-bit SHA-1 hash of the subject public key |
| *cRLDistributionPoints* | 2.5.29.31 | CRL issuing authority as ldap address |

[11] Special case within the framework of the EU digital vaccination certificate deviating from this.

| Extension | OID | Parameter |
|---|---|---|
| *authorityInfoAccess* | 1.3.6.1.5.5.7.1.1 | *accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation {…}*[12]<br>*accessMethod= caIssuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}* |
| *certificatePolicies* | 2.5.29.32 | OIDs of the CPs supported<br>*cpsURI* |
| *subjectAltName* | 2.5.29.17 | Alternative holder's name<br>If an e-mail address is specified, it must be entered as *RFC822Name*. |
| *qcStatements* | *1.3.6.1.5.5.7.1.3* | **QEVCP-w and QNCP-w:**<br>esi4-qcStatement-1 {0 4 0 1862 1 1};<br>esi4-qcStatement-5 {0 4 0 1862 1 5};<br>esi4-qcStatement-6 {0 4 0 1862 1 6};<br>id-etsi-qct-web {0 4 0 1862 1 6 3};<br><br>**QCP-l:**<br>esi4-qcStatement-1 {0 4 0 1862 1 1};<br>esi4-qcStatement-5 {0 4 0 1862 1 5};<br>esi4-qcStatement-6 {0 4 0 1862 1 6};<br>id-etsi-qct-eseal {0 4 0 1862 1 6 2} ;<br><br>**QCP-l-qscd:**<br>esi4-qcStatement-1 {0 4 0 1862 1 1};<br>esi4-qcStatement-4 {0 4 0 1862 1 4};<br>esi4-qcStatement-5 {0 4 0 1862 1 5};<br>esi4-qcStatement-6 {0 4 0 1862 1 6};<br>id-etsi-qct-eseal {0 4 0 1862 1 6 2} ;<br><br>**QCP-n-qscd:**<br>esi4-qcStatement-1 {0 4 0 1862 1 1};<br>esi4-qcStatement-2 {0 4 0 1862 1 2};<br>esi4-qcStatement-4 {0 4 0 1862 1 4};<br>esi4-qcStatement-5 {0 4 0 1862 1 5};<br>esi4-qcStatement-6 {0 4 0 1862 1 6};<br>id-etsi-qct-esign {0 4 0 1862 1 6 1} ;<br><br>**BTSP:**<br>esi4-qtstStatement-1 {0 4 0 19422 1 1};<br><br>**In the case of certificates with PSD2 extension and QEVCP-w, QNCP-w and QCP-l, the following applies:**<br>etsi-psd2-qcStatement {0 4 0 19495 2}<br><br>together with<br>PSD2QcType ::= SEQUENCE {<br>rolesOfPSP |

[12] If the status of a certificate is provided via online certificate status protocol (OCSP), this is carried out via the http protocol.

| Extension | OID | Parameter |
|---|---|---|
| | | nCAName<br>nCAId }<br>The validation of the PSD2-specific attributes is described in section 4.2.1. |

Further extensions can be added; they must comply with [X.509], [RFC 5280], [RFC 6818], [ETSI EN 319 412] and [ETSI-ALG] or they must be described in a referenced document.

The specific rules are documented in the respective CPS.

**QEVCP-w, EVCP,OVCP, DVCP**
A Precertificate, as described in RFC 6962, is not considered a "certificate" in the true sense of the word, which meets the requirements of RFC 5280.

**QCP-n-qscd, QCP-l-qscd**
The list of QSCDs in Germany is made publicly available on the website of the Federal Network Agency (BNetzA). D-Trust monitors the QSCD certification status of the QSCDs it uses. If the QSCD certification status of the QSCDs used is shorter than the regular certificate validity periods, customers will be informed in advance and the certificates will be issued with a shorter certificate validity period from the critical point in time.

However, if a certificate is mistakenly issued on a QSCD with a certificate expiry date that is valid beyond the valid QSCD certification status, the subject/ subscriber will be informed in advance and the certificate will be revoked no later than by the expiry date of the QSCD.

If the TSP becomes aware of changes that affect the validity of the certificate, for instance, because the supervisory body has withdrawn the QSCD certification status, all affected certificates with "esi4-qcStatement-4" according to ETSI EN 319 412-5 and which are affected by this change of the affected QSCD certification status will be revoked. The subjects concerned and, if applicable, subscribers will be informed of this.

**QCP-l for the EU digital vaccination certificate**
Seal certificates used within the framework of the EU digital vaccination certificate can contain the following OID entries in the extendedKeyUsage (extKeyUsage) field:

- OID 1.3.6.1.4.1.0.1847.2021.1.1 for Test Issuers
- OID 1.3.6.1.4.1.0.1847.2021.1.2 for Vacination Issuers
- OID 1.3.6.1.4.1.0.1847.2021.1.3 for Recovery Issuers

### 7.1.3 Algorithm OIDs

SHA1 is not used.

The specific rules are documented in the respective CPS.

### 7.1.4 Name formats

In the *subject* (here: name of the subject/end-entity) and *issuer* (name of the issuer) fields, names are assigned according to [X.500] or [X.509] as DistinguishedName. The attributes described in section 3.1.4 can be assigned. Coding is carried out as UTF8 string or PrintableString for the C (Country) attribute.

The *SubjectAltName* (alternative subject name) and *IssuerAltName* (alternative issuer name) fields can contain names according to [RFC 5280], [RFC 6818] (coded as IA5String).

**QEVCP-w, QNCP-w, EVCP,OVCP, DVCP**
The requirements of section 7.1.4 of [BRG] are met.

**QEVCP-w, EVCP**
The specifications from section 9.2 [EVGL] apply and supersede the specifications from section 7.1.4 [BRG].

7.1.5 Name constraints

"NameConstraints" is not used.

7.1.6 Certificate Policy Object Identifier

"CertificatePolicies" can contain the OID of CPs supported.

Further rules are documented in section 1.1.3 of the CP.

7.1.7 Use of the "PolicyConstraints" extension

"PolicyConstraints" is not used.

7.1.8 Syntax and semantics of "Policy Qualifiers"

"PolicyQualifiers" can be used.

7.1.9 Processing the semantics of the critical "CertificatePolicies" extension

In service, CA and EE certificates, the *CertificatePolicies* extension is not critical. Subscribers and relying parties are free to decide whether this extension is evaluated.

7.2 CRL profiles

The difference between the nextUpdate field and the thisUpdate field does not exceed ten days.

**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP**
**CA certificates**
For revoked CA certificates, D-Trust states the reason for revocation in the reasonCode entry in the CRL. If an entry is required, D-Trust uses one of the following CRLReasons according to RFC 5280, section 5.3.1, which best matches the revocation reason:

- keyCompromise (1),
- cACompromise (2),
- affiliationChanged (3),
- superseded (4) or
- cessationOfOperation (5).

**Subscriber certificates**
The subscriber must select a revocation reason. If the subscriber selects unspecified (0), the reasonCode entry in the CRL remains empty. D-Trust uses one of the following CRLReasons according to RFC 5280, sectoin 5.3.1:

- unspecified (0)
- keyCompromise (1),
- affiliationChanged (3),
- superseded (4) or
- cessationOfOperation (5)

The TSP subsequently enters the following revocation reason as a CRL reason if the subscriber violates the agreed terms and conditions:

- privilegeWithdrawn (9).

If there is evidence that a key has been compromised, but the subscriber failed to document this correctly in the CRLReason, the TSP will then set this value to "keyCompromise". If the TSP determines that the certificate private key was compromised before the revocation date specified

in the CRL entry for that certificate, the TSP will then correct the revocation date. This backdating is an exception and does not usually apply.

### 7.2.1 Version number(s)

Certificate revocation lists v2 according to [RFC 5280], [RFC 6818] are generated. Delta CRLs are not foreseen.

### 7.2.2 Extensions of certificate revocation lists and certificate revocation list entries

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

Certificate revocation lists can contain the following non-critical extensions:

| Extension | OID | Parameter |
|---|---|---|
| *cRLNumber* | 2.5.29.20 | Number of the certificate revocation list |
| *authorityKeyIdentifier* | 2.5.29.35 | 160-bit SHA-1 hash of the issuer key |
| *expiredCertsOnCRL* | 2.5.29.60 | The extension is used only for **QCP-n-qscd, QCP-l-qscd, QCP-l, QEVCP-w, QNCP-w** |
| *reasonCode* | 2.5.29.21 | If this field is shown, then a CRLReason is used according to section 7.2. |

## 7.3 OCSP profiles

In addition to RFC 6960, the OCSP responder also supports positive information. ("Certificate is authentic and valid").

The OCSP responder delivers the following replies:

- "good"[13] if the responder identifies the certificate as valid,
- "unknown"[14] if the responder cannot identify the status of the certificate and
- "revoked" if the responder identifies the certificate as revoked.

If the "nextUpdate" field is not set, the OCSP responder indicates according to section 4.2.2.1 of RFC 6960 that the latest revocation information is always available.

**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP**
The "nextUpdate" field is set. The difference between the nextUpdate field and the thisUpdate field does not exceed 24 hours.

If the OCSP information is provided for a revoked CA certificate, then this contains the entry revocationReason within the RevokedInfo of the CertStatus according to RFC 6960. The content of the entry is based on the specifications from section 7.2.

Information regarding certificates is provided at least until the expiry date of the certificate.

### 7.3.1 Version number(s)

OCSP v1 according to [RFC 6960] is used.

[13] If a certificate is not issued, the OCSP responder returns "unknown" as the status information.

[14] The OCSP responder does not monitor requests identified as "unknown". These are currently discarded.

### 7.3.2 OCSP extensions

The OCSP responder supports the extension shown below for queries:

| Extension | Parameter |
|---|---|
| *retrieveIfAllowed* | If set, the certificate is delivered in the response (optional). |

The OCSP responder uses the extensions shown below in the responses:

| Extension | Parameter |
|---|---|
| *archiveCutOff* | Period of time for which the OCSP responder makes the status information available after issuance of the certificate. |
| *certHash* | In the case of the "good" or "revoked" status, the SHA-1 hash value of the certificate is entered. |
| *certInDirSince* | Time of publication of the certificate in the central repository service. |
| *requestedCertificate* | Contains the certificate if *RetrieveIfAllowed* was set. |

All extensions are non-critical. Further non-critical extensions can be contained.

## 8. Compliance Audit and Other Assessments

Revisions, revision objects and processes are described in detail in D-Trust GmbH's documentation. The role concept documents the qualification and position of the internal auditor.

An independent conformity assessment body recurrently checks TSP's documentation and operational procedures in annual audits consecutively over the entire period. Relevant parts of these documents can be inspected against proof of a legitimate interest.

With a view to certificates, the CP, TSPS and CPS meet the requirements for:

- Products within the **Root CPS and CSM CPS:** according to [EN 319 411-1] or [EN 319 411-2] or BSI [TR-03145-1] including the requirements of [BRG] and [NetSec-CAB]
- Products within the **Cloud CPS:** according to [EN 319 421], [EN 319 411-1] or [EN 319 411-2] including the requirements of [BRG] and [NetSec-CAB]

A regular assessment by a competent independent third party proves conformity for:

- Products within the Root CPS and CSM CPS: according to [EN 319 411-1] or [EN 319 411-2] which includes normative references to [ETSI EN 319 401]
- Products within the Cloud CPS: according to [EN 319 421], [EN 319 411-1] or [EN 319 411-2] which includes normative references to [ETSI EN 319 401]

The TSP does not issue certificates with a policy OID reference according to the above specified standards of the respective CPS until after a successfully completed audit by an independent external conformity assessment body. Regular monitoring audits are carried out. When procedures and processes are found to be no longer in conformity with the current guidelines of the above specified standards of the respective CPS, the TSP discontinues issuance of the above-mentioned certificates until conformity with the guidelines is restored and has been audited accordingly. This audit takes place annually. Critical modifications are also audited and released during the course of the year by the conformity assessment body.

Regular internal audits are additionally carried out. Every quarter, within the framework of "self audits", randomly selected samples of at least three percent of the certificates (but at least one certificate) issued by D-Trust during such period in accordance with the requirements of the [BRG] and [EVGL] are audited and documented internally for quality assurance purposes.

**EVCP, OVCP, DVCP**

In the event of any discrepancies with a view to applicable national law, [BRG] and [EVGL], D-Trust will inform the CA/Browser Forum of such fact, the circumstances and the applicable national law.

## 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].

# D-TRUST Trust Service Practice Statement (TSPS)

Version 1.7

# Copyright UND NUTZUNGSLIZENZ

**Trust Service Practice Statement der D-Trust GmbH**
**©2023 D-Trust GmbH**



Anfragen zu einer sonstigen, in der vorgenannten Lizenz nicht enthaltenen Nutzungsart dieses TSPS 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 | 10.11.2020 | ▪ Initial Version.<br>▪ In der Version 1.0 bildet das TSPS ein übergeordnetes Practice Statement für die folgenden CPS-Dokumente:<br>CSM CPS, Root CPS und Cloud CPS<br>▪ Update nach observation report<br>▪ Anpassungen gemäß CAB/F SC35 (Cleanups and Clarifications) in den Abschnitten 4.2.2, 4.9.1, 6.1.5 und 6.1.6. |
| 1.1 | 23.04.2021 | ▪ Detaillierte Beschreibung der Validierungsmethoden in Abschnitt 4.2.1<br>▪ Spezifizierung der Anforderungen zur Meldung einer Kompromittierung des privaten Schlüssels in Abschnitt 4.9.12<br>▪ Jährliches Review des gesamten TSPS<br>▪ Ergänzungen in den Abschnitten 4.2.2, 4.9.1, 4.9.2, 5.4.2, 5.5.1, 5.5.2, 6.1.5, 6.1.6, 6.6.3, 7.1.1, 7.2, 7.2.2, 7.3, 8 |
| 1.2 | 02.07.2021 | ▪ Einführung von qualifizierten Siegelzertifikaten ohne QSCD für den digitalen EU Impfnachweis, siehe Abschnitt 7.1.2<br>▪ Update im Rahmen des BR Self Assessments<br>▪ Editorische Änderungen und Ergänzungen in den Abschnitten 2.2, 4.1.2, 4.2.1, 4.2.2, 4.9.1, 5.3.1, 5.7.3, 6.1.6, 6.7, 7.1.1, 7.1.2, 7.1.4, 7.2, 7.3, 8 |
| 1.3 | 14.10.2021 | ▪ Ergänzungen in den Abschnitten 1.3.2, 4.2.1 (Domain), 5.2.2, 5.3.3, 7.1.2 und 8 |
| 1.4 | 14.04.2022 | ▪ Informative Einführung des Policy Levels NCP<br>▪ Ergänzungen in Abschnitt 2.4, 4.2.1, 4.10.2 und 6.3.2<br>▪ Anpassungen in Abschnitt 4.2.2 aufgrund des Ballot SC50<br>▪ Ergänzung der Online-Ausweisfunktion eID in den IDENT-Verfahren unter PersIdent in Abschnitt 4.2.1<br>▪ Umbenennung des Policy Levels QCP-w in QEVCP-w und Einführung des Policy Levels QNCP-w<br>▪ Jährliches Review des gesamten TSPS |
| 1.5 | 14.11.2022 | ▪ Konkretisierungen in den Abschnitten 1.1.3, 1.4.1, 1.4.2, 4.2.1, 4.9.1, 4.9.12, 4.10.1, 5.5.1, 5.5.2, 6.1.5, 6.1.6, 6.2.11, 6.5.1, 6.6.1, 6.6.3, 7.1.2 und 8 |
| 1.6 | 16.02.2023 | ▪ Ergänzungen in Abschnitt 4.5.2<br>▪ Editorische Änderungen |
| 1.7 | 21.06.2023 | ▪ Ergänzungen und Konkretisierungen in Abschnitt 4.2.1, 7.1.2 und 7.2<br>▪ Jährliches Review des gesamten TSPS |

Inhaltsverzeichnis

# 1. Einleitung

Dieses Dokument ist das Trust Service Practice Statement (TSPS) der von D-Trust GmbH betriebenen Vertrauensdienste.

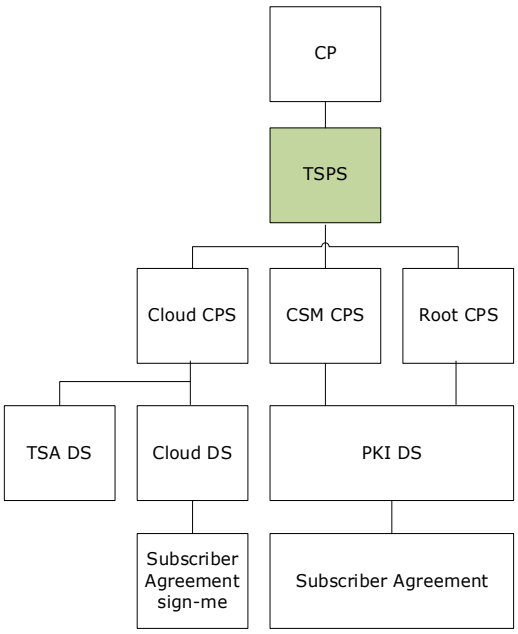
## 1.1 Überblick

### 1.1.1 Trust Service Provider (TSP - 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 hervor, indem Sie sich befinden. Aktuell sind die drei genannten CPS dem TSPS untergeordnet. Schrittweise werden weitere folgen.




**Verweise werden wie folgt angezeigt:**

**Diese Regelungen sind in der CP festgehalten.**
Die Regelungen in diesem Kapitel sind nicht in dem TSPS oder dem jeweiligen CPS dokumentiert, sondern sind ausschließlich in der CP hinterlegt.

**Diese Regelungen sind in dem jeweiligen CPS dokumentiert.**
Die Regelungen in diesem Kapitel sind nicht in dem TSPS oder der CP zu finden, sondern sind ausschließlich in dem jeweiligen CPS hinterlegt.

**Die spezifischen Regelungen sind in dem jeweiligen CPS dokumentiert.**
Für alle Vertrauensdienste geltende Regelungen sind in dem TSPS zu finden. Regelungen, die nur für einen bestimmten Vertrauensdienst gelten, sind in der entsprechenden CPS hinterlegt. Es müssen die Regelungen aus dem TSPS und dem entsprechenden CPS berücksichtigt werden.

Dieses TSPS nimmt Bezug auf die CP (Zertifikatsrichtlinie) der D-Trust GmbH mit der OID 1.3.6.1.4.1.4788.2.200.1.

Dieses TSPS und das jeweilige CPS definieren Verfahrensweisen im Rahmen der Vertrauensdienste während der gesamten Lebensdauer der CA- und Endanwenderzertifikate (EE-Zertifikate). Es werden Mindestmaßnahmen festgelegt, die von allen PKI-Teilnehmern zu erfüllen sind.

Die CP der D-Trust GmbH, das TSPS und das jeweilis anwendbare CPS sind rechtsverbindlich, soweit dies im Rahmen der deutschen bzw. europäischen Gesetzgebung zulässig ist. Sie enthalten Aussagen über Pflichten, Gewährleistung und Haftung für die PKI-Teilnehmer. Soweit Garantien oder Zusicherungen betroffen sind, enthalten dieses TSPS und das jeweilige CPS ausschließlich die für diesen Bereich ausdrücklich eingeräumten Garantien oder Zusicherungen.

Die Kenntnis, der in dieser TSPS beschriebenen Zertifizierungsverfahren und -regeln sowie der rechtlichen Rahmenbedingungen erlaubt es Zertifikatsnutzern Vertrauen in die Komponenten der PKI und in die PKI-Teilnehmer aufzubauen und Entscheidungen zu treffen, inwieweit das durch die PKI gewährte Vertrauens- und Sicherheitsniveau für die jeweilige Anwendung geeignet ist.

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

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 1.1.3 Eigenschaften der PKI

D-Trust GmbH definiert für jedes Produkt eine eigene D-Trust Policy-OID, die zusätzlich in die dazugehörigen Zertifikate aufgenommen wird. Die D-Trust Policy-OIDs sind in der CP der D-Trust GmbH in Abschnitt 1.1.3 dokumentiert.

Erläuterung der Policy Level qualifizierter Vertrauensdienste:

**QEVCP-w**[1]
EE-Zertifikate des Policy Levels QEVCP-w sind qualifizierte TLS-Zertifikate gemäß [EN 319 411-2], was an der QEVCP-w Policy-OID in den EE-Zertifikaten erkennbar ist. EE-Zertifikate werden nicht auf Chipkarten ausgegeben.

Qualifizierte Webseitenzertifikate der D-TRUST CA 2-2 EV 2016 erfüllen immer auch die Anforderungen an TLS-Zertifikate nach dem Policy Level EVCP gemäß [EN 319 411-1] und [EVGL], was an der EVCP Policy-OID in den EE-Zertifikaten erkennbar ist.

**QNCP-w**
EE-Zertifikate des Policy Levels QNCP-w sind qualifizierte TLS-Zertifikate gemäß [EN 319 411-2], was an der QNCP-w Policy-OID in den EE-Zertifikaten erkennbar ist. EE-Zertifikate werden nicht auf Chipkarten ausgegeben.

**QCP-l**
EE-Zertifikate des Policy Levels QCP-l sind qualifizierte Zertifikate gemäß [EN 319 411-2], was an der QCP-l Policy-OID in den EE-Zertifikaten erkennbar ist. EE-Zertifikate werden nicht auf Chipkarten ausgegeben.

[1] Das Policy Level QCP-w wird analog zu ETSI EN 319 411-2 in QEVCP-w umbenannt.

**QCP-l-qscd**
EE-Zertifikate des Policy Levels QCP-l-qscd sind qualifizierte Zertifikate gemäß [EN 319 411-2], was an der QCP-l-qscd Policy-OID in den EE-Zertifikaten erkennbar ist. Diese EE-Zertifikate werden auf Chipkarten ausgegeben.

**QCP-n-qscd**
EE-Zertifikate des Policy Levels QCP-n-qscd sind qualifizierte Zertifikate gemäß [EN 319 411-2], was an der QCP-n-qscd Policy-OID in den EE-Zertifikaten erkennbar ist. Diese EE-Zertifikate werden auf Chipkarten ausgegeben.

**BTSP**
Zertifikate des Policy Levels BTSP sind qualifizierte Dienstezertifikate für den Zeitstempeldienst gemäß [EN 319 421], was an der BTSP Policy-OID in den Dienstezertifikaten erkennbar ist.

Erläuterung der Policy Level nicht-qualifizierter Vertrauensdienste (publicly trusted):

**EVCP**
EE-Zertifikate des Policy Levels EVCP sind TLS-Zertifikate. Dass es sich um EV-Zertifikate handelt, ist in den EE-Zertifikaten an der EV-Policy-OID (entsprechend Abschnitt 1.1.3 der CP/ CPS) erkennbar. EV-Zertifikate werden nicht auf Chipkarten ausgegeben.

**OVCP**
Zu den EE-Zertifikaten des Policy Levels OVCP zählen TLS-Zertifikate und Maschinenzertifikate, die den Namen einer Organisation beinhalten. OV-Zertifikate werden nicht auf Chipkarten ausgegeben.

**DVCP**
Zu den EE-Zertifikaten des Policy Levels DVCP zählen TLS-Zertifikate bei denen das Subject (End-Entity) über den Domain Namen identifiziert wird. DV-Zertifikate werden nicht auf Chipkarten ausgegeben.

**NCP**
EE-Zertifikate des Policy Levels NCP sind Personenzertifikate oder Organisationszertifikate. Bei den Personenzertifikaten kann der Name einer Organisation optional als zusätzliches Attribut in das Zertifikat aufgenommen werden. NCP-Zertifikate werden nicht auf Chipkarten ausgegeben.

Das Policy Level NCP wird informativ in die Dokumentation aufgenommen. Perspektivisch werden Produkte des Policy Levels LCP auf das Policy Level NCP migriert. Das jeweilige Policy Level ist an der Policy OID in EE-Zertifikaten erkennbar.

**LCP**
EE-Zertifikate des Policy Levels LCP sind einfache Personenzertifikate oder Organisationszertifikate. Bei den Personenzertifikaten kann der Name einer Organisation optional als zusätzliches Attribut in das Zertifikat aufgenommen werden. LCP-Zertifikate werden nicht auf Chipkarten ausgegeben.

**V-PKI**
EE-Zertifikate des Zertifizierungslevels V-PKI (Verwaltungs-PKI) sind einfache Personenzertifikate oder Funktionszertifikate. V-PKI-Zertifikate werden über eine online Schnittstelle bereitgestellt und nicht auf Chipkarten ausgegeben.

Derzeit werden Produkte mit nicht-qualifizierten Policy Levels (z.B. EVCP+, NCP+), die die Verwendung einer sicheren Signaturerstellungseinheit (SSEE) voraussetzen nicht angeboten. Dennoch steht es dem Zertifikatsnehmer frei, eine SSEE für die Erzeugung und Aufbewahrung seiner privaten Schlüssel zu verwenden.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

## 1.2 Name und Kennzeichnung des Dokuments

| | |
|---|---|
| Dokumentname: | D-TRUST Trust Service Practice Statement (TSPS) |
| Version | 1.7 |

## 1.3 PKI-Teilnehmer

### 1.3.1 Certification authorities (CA)

Zertifizierungsstellen (Certification Authority – CA) werden vom Trust Service Provider (TSP) betrieben und stellen Zertifikate sowie Sperrlisten aus.

Je nach PKI sind folgende Arten von Zertifikaten möglich:

- Personenzertifikate für natürliche Personen (EE-Zertifikat),
- Siegelzertifikate für juristische Personen (EE-Zertifikat),
- Gruppenzertifikate für Personengruppen (EE-Zertifikat),
- Dienstezertifikate für juristische Personen (EE-Zertifikat),
- Zertifikate für Webserver, Geräte oder Maschinen (EE-Zertifikat) und
- Zertifizierungsinstanzen (untergeordnete CA-Zertifikate des TSP).

Die Wurzelinstanzen stellen Zertifikate ausschließlich mit der Erweiterung basicConstraints: cA=TRUE (CA-Zertifikat) aus. Untergeordnete CAs stellen EE-Zertifikate und/oder weitere CA-Zertifikate aus. Die Zertifizierungsstelle ist in den ausgestellten Zertifikaten und CRLs namentlich im Feld issuer benannt.

### 1.3.2 Registrierungsstellen (RA)

Die RA identifiziert und authentifiziert Zertifikatsnehmer (subscriber) oder Endanwender (subject), erfasst und prüft Anträge für verschiedene Zertifizierungsdienstleistungen.

Die konkreten Aufgaben und Pflichten, die die RA in Vertretung des TSP bzw. der CA übernimmt sind im jeweiligen Vertrag mit der RA definiert und verbindlich vereinbart. Die RA wird in diesem Rahmen eindeutig vom TSP identifiziert.

Registrierungsstellen, die nicht von der D-Trust betrieben werden, unterliegen den gleichen Vorgaben.

RA-Operatoren Tätigkeiten, sowohl intern als auch extern, erfolgen auf sicherheitskritischen Systemen zur Zertifikatsausstellung und sind durch eine erzwungene Multi-Faktor-Authentisierung geschützt (siehe auch Abschnitt 5.2.2).

TLS-Zertifikatsanträge werden ausshließlich von der internen RA der D-Trust bearbeitet. Die Domänenvalidierung erfolgt somit ausschließlich durch die D-Trust selbst und wird grundsätzlich nicht an Dritte (z. B. an eine externe RA) delegiert bzw. ausgelagert.

Die Domainprüfung im Rahmen der E-Mail Verifikationsmethode in Abschnitt 4.2.1 für S/MIME-Zertifikate wird ebenfalls nur durch die D-Trust selbst durchgeführt.

### 1.3.3 Zertifikatsnehmer (ZNE)

Zertifikatsnehmer (*subscriber*) sind natürliche oder juristische Personen, die EE-Zertifikate beantragen und innehaben. Der Zertifikatsnehmer kann mit dem im Zertifikat genannten Endanwender (*subject)* identisch sein.

Endanwender (*subject;* End-Entity (EE)) verwenden die privaten Endanwenderschlüssel (EE-Schlüssel). Die Identität des Endanwenders ist mit dem Zertifikat und dem zugehörigen Schlüsselpaar verknüpft. Der Endanwender kann mit dem Zertifikatsnehmer identisch sein. Je nach PKI sind zulässige Endanwender:

- natürliche Personen,
- juristische Personen,
- Personengruppen oder Teams,
- Geräte oder Maschinen
- Funktionen, die durch Mitarbeiter einer Organisation ausgefüllt werden und
- IT-Prozesse.

Die Verantwortung für Schlüssel und Zertifikat trägt der Zertifikatsnehmer, wenn das Schlüsselmaterial vom Zertifikatsnehmer erzeugt wurde bzw. sobald dieses durch den Trust Service Provider (TSP) an ihn übergeben wurde. Darüber hinaus ergeben sich nach [EN 319 411-1] bzw. [EN 319 411-2] oder BSI [TR-03145-1] weitere Pflichten. Spätestens zum Zeitpunkt der Antragstellung wird der Zertifikatsnehmer über diese Pflichten durch die Bereitstellung der CP, dieses TSPS, des CPS und der Verpflichtungserklärung (subscriber agreement) informiert und muss sich zu deren Einhaltung verpflichten.

**QCP-n-qscd**
Für qualifizierte Signaturzertifikate müssen Zertifikatsnehmer und Endanwender identisch sein.

**QEVCP-w, QNCP-w, QCP-l, QCP-l-qscd, EVCP, DVCP, OVCP, NCP, LCP, V-PKI**
Sind Zertifikatsnehmer und Endanwender nicht identisch, sind der Zertifikatsnehmer und der Endanwender für die Einhaltung der Verpflichtungserklärung verantwortlich.

**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, QCP-l, QCP-l-qscd**
Siegel- und TLS-Zertifikate werden ausschließlich für juristische Personen ausgestellt.

**BTSP**
Dienstezertifikate für die Ausstellung von qualifizierten Zeitstempeln werden ausschließlich für die D-Trust GmbH ausgestellt. Es wird ausschließlich ein Zertifikat für den qualifizierten Zeitstempel verwendet.[2]
Anwender des Zeitstempeldienstes gemäß [EN 319 421] sind natürliche oder juristische Personen, die den Zeitstempeldienst im Rahmen der Cloud PKI beim Trust Service Provider (TSP) beziehen.

### 1.3.4 Zertifikatsnutzer (ZNU)

Zertifikatsnutzer (englisch relying parties) sind natürliche oder juristische Personen, die die Zertifikate dieser PKI nutzen und Zugang zu den Diensten des TSP haben.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

## 1.4 Verwendung von Zertifikaten

### 1.4.1 Erlaubte Verwendungen von Zertifikaten

CA-Zertifikate werden ausschließlich und in Übereinstimmung mit ihrer Erweiterung (BasicConstraints, PathLengthConstraint) für die Ausstellung von CA- oder EE-Zertifikaten und CRLs benutzt.

[2] Siehe Repository: www.d-trust.net/repository

Die EE-Zertifikate dürfen für die Anwendungen benutzt werden, die in Übereinstimmung mit den im Zertifikat angegebenen Nutzungsarten (keyUsage) stehen.

Zertifikatsnutzer handeln auf eigene Verantwortung. Es liegt in der Verantwortung des Zertifikatsnutzers, einzuschätzen, ob das TSPS und das CPS den Anforderungen einer Anwendung entspricht und ob die Benutzung des betreffenden Zertifikats zu einem bestimmten Zweck geeignet ist.

Weiterhin gelten die Regelungen der CP der D-Trust GmbH.

### 1.4.2 Verbotene Verwendungen von Zetifikaten

Andere Verwendungsarten (keyUsage) als die im Zertifikat festgelegten, sind nicht zulässig.

Weiterhin gelten die Regelungen der CP der D-Trust GmbH.

**V-PKI**
Im Rahmen der V-PKI gelten zusätzlich die Regelungen der CP V-PKI BSI.

### 1.4.3 Verwendung von Dienstezertifikaten

Der TSP verwendet Dienstezertifikate zur Erbringung von Vertrauensdienste gemäß [eIDAS]. Dienstezertifikate werden durch den TSP selbst und zur eigenen Verwendung ausgestellt. Sie unterliegen den Anforderungen der jeweilig anwendbaren Zertifizierung.

Zu den Verwendungsarten zählen:

- CA-Zertifikate zur CA- und Zertifikatserstellung
- Signatur von Statusauskünften[3]
- Signatur von Zeitstempeln[4]

## 1.5 Administration der Policy

### 1.5.1 Zuständigkeit für das Dokument

Dieses TSPS und die ihm untergeordneten CPS Dokumente werden durch die D-Trust GmbH gepflegt. Der Beauftragte der Geschäftsführung übernimmt die Freigabe der Dokumente.

Dieses TSPS und die ihm untergeordneten CPS Dokumente werden mindestens jährlich durch den TSP überprüft und ggf. aktualisiert. Änderungen werden durch eine neue Versionsnummer im jeweiligen aktualisierten Dokument kenntlich gemacht und nach Freigabe der aktuellen Version durch die Geschäftsführung zeitnah im Repository der D-Trust neu veröffentlicht. Sollten Mitarbeiter bzw. externe Parteien (wie Kunden, exIdentstellen, Reseller) von den Änderungen betroffen sein, werden diejenigen vorab in Kenntnis gesetzt bzw. bei Bedarf entsprechend ertüchtigt die Änderungen umzusetzen.

Die Kontaktdaten des TSP sind in der CP Abschnitt 1.5.1 dokumentiert.

### 1.5.2 Meldung von Sicherheitsvorfällen mit Zertifikaten

Diese Reglungen sind in der CP dokumentiert.

### 1.5.3 Verträglichkeit von CPs fremder CAs mit diesem CPS

Sowohl in CA- als auch in EE-Zertifikaten können weitere CPs über Policy-OIDs referenziert werden, die diesem TSPS bzw. den jeweiligen CPS nicht widersprechen. Die Referenz einer Policy-OID in den Zertifikatserweiterungen bestätigt die Kompatibilität der

[3] OCSP-Auskünfte werden durch gesonderte OCSP-Dienstezertifikate signiert.

[4] Zeitstempel werden durch gesonderte Dienstezertifikate signiert.

Zertifizierungspraktiken mit der referenzierten CP (z.B. NCP 0.4.0.2042.1.1 gemäß [EN 319 411-1]).

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 1.6 Begriffe und Abkürzungen

#### 1.6.1 Begriffe und Namen

Die allgemeinen Regelungen sind in der CP dokumentiert.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

#### 1.6.2 Abkürzungen

| | |
|---|---|
| Certificate Policy (CP) | Zertifikatsrichtlinie |
| IDN | Internationalized Domain Name |

Allgemeine Regelungen sind in der CP festgehalten.

#### 1.6.3 Referenzen

Allgemeine Regelunge sind in der CP festgehalten.

## 2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

### 2.1 Verzeichnisse

Die allgemeinen Regelungen zu Verzeichnissen sind in der CP dokumentiert.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 2.2 Veröffentlichung von Informationen zu Zertifikaten

Der TSP veröffentlicht folgende Informationen:

- CA-Zertifikate,
- die CP der D-Trust GmbH,
- dieses TSPS,
- Sperrlisten (CRLs) und Statusinformationen (OCSP) und
- EE-Demo-Zertifikate

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

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

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

### 2.3 Häufigkeit von Veröffentlichungen

Diese Regelungen sind in dem jeweiligen CPS festgehalten.

2.4 Zugriffskontrollen auf Verzeichnisse

Zertifikate, Sperrlisten, TSPS, CPS und CPs können öffentlich und unentgeltlich 24x7 abgerufen werden. Der Verzeichnisdienst hat eine Verfügbarkeit von mindestens 98,5%. Der TSP stellt sicher, dass im Falle einer Störung die Ausfalldauer (downtime) maximal vier Stunden beträgt.

Es gibt keine Zugriffsbeschränkungen für lesenden Zugriff. Änderungen der Verzeichnis- und Webinhalte werden ausschließlich vom TSP vorgenommen.

Weitere, nicht öffentliche Dokumente, können bei begründetem Interesse auf Nachfrage in den relevanten Teilen zur Einsicht bereitgestellt werden.

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

Diese Regelungen sind im jeweiligen CPS dokumentiert.

3.1.2 Notwendigkeit für aussagefähige Namen

Diese Regelungen sind im jeweiligen CPS dokumentiert.

3.1.3 Anonymität oder Pseudonyme von Zertifikatsnehmern

Diese Regelungen sind im jeweiligen CPS dokumentiert.

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Diese Regelungen sind im jeweiligen CPS dokumentiert.

3.1.5 Eindeutigkeit von Namen

Diese Regelungen sind im jeweiligen CPS dokumentiert.

3.1.6 Anerkennung, Autentifizierung und die Rolle von Markennamen

Diese Regelungen sind im jeweiligen CPS dokumentiert.

3.2 Initiale Überprüfung der Identität

3.2.1 Nachweis für den Besitz des privaten Schlüssels

Diese Regelungen sind im jeweiligen CPS dokumentiert.

3.2.2 Identifizierung und Authentifizierung von Organisationen

Diese Regelungen sind im jeweiligen CPS dokumentiert.

3.2.3 Identifizierung und Authentifizierung natürlicher Personen

Diese Regelungen sind im jeweiligen CPS dokumentiert.

3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Diese Regelungen sind im jeweiligen CPS dokumentiert.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Diese Regelungen sind im jeweiligen CPS dokumentiert.

3.2.6 Kriterien für die Interoperabilität

Siehe Abschnitt 1.5.3.

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

Diese Regelungen sind im jeweiligen CPS dokumentiert.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Diese Regelungen sind im jeweiligen CPS dokumentiert.

## 4. Betriebsanforderungen zum Zertifikatslebenszyklus

4.1 Zertifikatsantrag und Registrierung

4.1.1 Berechtigung zur Antragstellung

CA-Zertifikate werden ausschließlich an juristische Personen ausgegeben.
Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

4.1.2 Registrierungsprozess und Zuständigkeiten

Die Einhaltung des Registrierungsprozesses gewährleistet der TSP. Teilaufgaben können von vertraglich gebundenen Partnern oder externen Anbietern übernommen werden, die die Maßgaben der CP, TSPS und CPS erfüllen.

Je nach Antragsweg und Policy Level sind bestimmten Dokumenten zuzustimmen, die damit zum Vertragsbestandteil werden und damit rechtsverbindlich gelten. Eine Übersicht dazu ist im Repository abgelegt:

https://www.d-trust.net/files/dokumente/pdf/terms-and-conditions_produkt-dienstleistung.pdf

Zur Übermittlung der Registrierungsdaten ist die Kommunikation zwischen den externen Registrierungsstellen und der internen Registrierungsstelle beim TSP über eine TLS-Verbindung verschlüsselt und authentisiert.

Der TSP legt den Registrierungsprozess je nach Policy Level wie folgt fest:

**QEVCP-w, QNCP-w, EVCP, QCP-l, QCP-l-qscd**

Dem Zertifikatsnehmer liegen vor Abschluss des Registrierungsprozesses CP, TSPS, CPS sowie eine Verpflichtungserklärung (Subscriber Agreement) vor, zu deren Einhaltung sich der Zertifikatsnehmer verpflichtet. Die Dokumente werden veröffentlicht. Die Verpflichtungserklärung entspricht den Vorgaben aus [EN 319 411-1] und [EN 319 411-2].
Der Antrag beinhaltet ggf. weiterhin die Einverständniserklärung des Zertifikatsnehmers zur Veröffentlichung der Zertifikate. Die Verpflichtungserklärung entspricht dem „Subscriber Agreement" gemäß den Vorgaben aus [BRG] und [EVGL]. Nachweise werden elektronisch oder papierbasiert hinterlegt.

**QCP-n-qscd**

Dem Zertifikatsnehmer liegen vor Abschluss des Registrierungsprozesses CP, TSPS, CPS sowie eine Verpflichtungserklärung (Subscriber Agreement) vor, zu deren Einhaltung sich der Zertifikatsnehmer verpflichtet. Die Dokumente werden veröffentlicht. Die Verpflichtungserklärung entspricht den Vorgaben aus [EN 319 411-1] und [EN 319 411-2].

Der Antrag beinhaltet weiterhin die Einverständniserklärung des Zertifikatsnehmers zur Veröffentlichung oder Nicht-Veröffentlichung der Zertifikate. Die Verpflichtungserklärung entspricht dem „Subscriber Agreement" gemäß den Vorgaben aus [BRG] und [EVGL]. Nachweise werden elektronisch oder papierbasiert hinterlegt.

**OVCP, DVCP**

Dem Zertifikatsnehmer liegen vor Abschluss des Registrierungsprozesses CP, TSPS, CPS sowie eine Verpflichtungserklärung (Subscriber Agreement) vor, zu deren Einhaltung sich der Zertifikatsnehmer verpflichtet. Die Dokumente werden veröffentlicht. Die Verpflichtungserklärung entspricht den Vorgaben aus [EN 319 411-1]. Der Antrag beinhaltet weiterhin die Einverständniserklärung des Zertifikatsnehmers zur Veröffentlichung der Zertifikate. Die Verpflichtungserklärung entspricht dem „Subscriber Agreement" gemäß den Vorgaben aus [BRG]. Nachweise werden elektronisch oder papierbasiert hinterlegt.

**NCP, LCP**

Dem Zertifikatsnehmer werden CP, TSPS, CPS sowie eine Verpflichtungserklärung (Subscriber Agreement) zur Verfügung gestellt, zu deren Einhaltung sich der Zertifikatsnehmer verpflichtet. Die Dokumente werden veröffentlicht. Die Verpflichtungserklärung entspricht den Vorgaben aus [EN 319 411-1]. Der Antrag beinhaltet weiterhin die Einverständniserklärung des Zertifikatsnehmers zur Veröffentlichung der Zertifikate. Wenn Zertifikatsnehmer und Endanwender voneinander abweichen, muss der Zertifikatsnehmer die Pflichten aus diesem Dokument und dem Subscriber Agreement bzw. der Verpflichtungserklärung nachweislich an den Endanwender übertragen.

**V-PKI**

Dem Zertifikatsnehmer werden CP, TSPS, CPS sowie eine Verpflichtungserklärung (Subscriber Agreement) zur Verfügung gestellt, zu deren Einhaltung sich der Zertifikatsnehmer verpflichtet. Die CPS wird veröffentlicht. Wenn Zertifikatsnehmer und Endanwender voneinander abweichen, muss der Zertifikatsnehmer die Pflichten aus diesem Dokument und dem Subscriber Agreement bzw. der Verpflichtungserklärung nachweislich an den Endanwender übertragen.
Der Zertifikatsnehmer muss sicherstellen, dass die privaten Schlüssel aus der V-PKI nur berechtigten Endanwendern übergeben und entsprechend verwendet werden.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

## 4.2 Verarbeitung des Zertifikatsantrags

### 4.2.1 Durchführung der Identifizierung und Authentifizierung

Vor Nutzung der Zertifizierungs- und Vertrauensdienste der D-Trust GmbH ist eine Identifizierung des Kunden erforderlich. Der Registrierungsprozess und ein für das gewählte Produkt zulässiges Identifizierungsprozess müssen vollständig durchlaufen und alle nötigen Nachweise müssen dabei erbracht werden.

Die Authentifizierung natürlicher Personen oder Organisationen sowie die Prüfung weiterer zertifikatsrelevanter Daten kann vor oder nach der Antragstellung erfolgen, muss aber vor der Ausstellung von Zertifikaten und ggf. Übergabe des Schlüsselmaterial sowie PINs abgeschlossen sein.

Natürliche Personen müssen eindeutig identifiziert werden. Zum vollständigen Namen müssen Attribute wie Geburtsort, Geburtsdatum oder andere anwendbare individuelle Merkmale Verwechslungen verhindern. Werden juristische Personen im Zertifikat benannt oder sind sie Zertifikatsnehmer, müssen deren vollständiger Name und rechtlicher Status sowie ggf. relevante Registerinformationen geprüft werden.

Die Identifizierung natürlicher Personen findet gemäß Abschnitt 3.2.3 der jeweiligen CPS statt.

**EVCP**

Eine natürliche Person kann in der Rolle des Contract Signer (Vertragsunterzeichner) für den Antragsteller fungieren, wenn sie ihre Vertretungsberechtigung der juristischen Person angemessen nachweisen kann. Der Contract Signer kann eine oder mehrere natürliche Personen autorisieren, die Rolle des Certificate Approvers (Zertifikatsgenehmiger, primärer Operator) einzunehmen. Diese Autorisierung muss nachgewiesen werden und wird überprüft. In diesem Rahmen überprüft der TSP den Namen und Titel des Contract Signers und des Certificate Approvers.Der Certificate Approver kann eine oder mehrere natürliche Personen autorisieren, die Rolle des Certificate Requester (Zertifikatsantragsteller, Technischer Antragsteller) einzunehmen.

Die Vorgaben aus Abschnitt 11.8 [EVGL] werden erfüllt.

Der TSP überprüft die folgenden Daten auf der HADDEX Sanktionsliste:

- den Namen des Applicants (Antragstellers), des Contract Signers (Vertragsunterzeichners), des Certificate Approvers (Zertifikatgenehmigers) oder
- den Gerichtsstand der Gründung, die Registrierung des Antragstellers oder
- den Ort der Geschäftstätigkeit.

Bei einer Eintragung kommt eine Zusammenarbeit nicht zustande.

Zur Überprüfung der Unterschrift des Zertifikatsrequests gemäß Abschnitt 11.9 [EVGL] werden je nach Antragsweg die folgenden Verfahren verwendet, die den Namen und Titel (Funktion im Unternehmen) des Unterzeichners auf sichere Weise feststellen:

1. Verwendung eines entsprechend sicheren Anmeldeverfahrens, das den Unterzeichner vor der Unterzeichnung identifiziert und
2. Verwendung einer digitalen Signatur, die mit Bezug auf ein entsprechend verifiziertes Zertifikat erstellt wurde.

Sofern die Methoden 1. oder 2. nicht anwendbar ist, kann mit dem Antragssteller eine Kontaktaufnahme über eine der verifizierten Kommunikationsmethoden gemäß Abschnitt 4 [EVGL] mit der Bitte erfolgen, dass der Contract Signer oder der Certificate Requester bestätigt, den Zertifikatsantrag unterschrieben zu haben.

D-Trust hat ein Prozess zur Identifizierung von High Risk Zertifikatsanfragen und zur erweiterten Bearbeitung dieser Zertifikatsanfragen implementiert, um einen Missbrauch zu verhindern.

Der TSP definiert die folgenden IDENT-Verfahren zur Ermittlung der Identität einer natürlichen Person:

**PersIdent**

Die natürliche Person muss sich von einer RA (z.B. dem TSP selbst, einer vertraglich verpflichteten Organisation bzw. Behörde) oder einem zugelassenen Identifizierungspartner, der die Maßgaben des TSPS und des CPS erfüllt, anhand eines gültigen amtlichen Ausweises persönlich identifizieren lassen.

Zulässige Dokumente sind ein Personalausweis oder Reisepass bei Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union oder eines Staates des Europäischen Wirtschaftsraumes oder Dokumenten mit gleichwertiger Sicherheit. Informationen zur Identifizierung werden als Nachweis archiviert.

Wenn die RA des TSP bzw. die externe Registrierungs- und Identifizierungsstelle des TSP die persönliche Identifizierung des Subscriber bzw. des Subject nicht selbst durchführen kann, dann können alternativ die zertifizierten Ident-Verfahren von Partnern genutzt werden.

**eID**
Die natürliche Person mit Wohnsitz in Deutschland authentifiziert sich mittels einer gültigen amtlichen elektronischen Ausweisfunktion gemäß Artikel 9 der eIDAS Verordnung. Zulässige Dokumente sind Personalausweise oder elektronische Aufenthaltstitel der Bundesrepublik Deutschland mit elektronischer Ausweisfunktion. Informationen zur Identifizierung werden als Nachweis archiviert.

**NotarIdent**
Die natürliche Person oder ein bevollmächtigter Vertreter der juristischen Person kann sich von einem zugelassenen Notar, der die Maßgaben des TSPS und des CPS erfüllt, anhand eines gültigen amtlichen Ausweises persönlich identifizieren lassen. Der TSP akzeptiert die Identifizierung nur durch die Notare, die in akzeptierten öffentlichen Notarverzeichnissen des jeweiligen EU-Staates ausgewiesen sind. Zulässige Dokumente sind Personalausweis oder Reisepass bei Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union oder eines Staates des Europäischen Wirtschaftsraumes, oder Dokumenten mit gleichwertiger Sicherheit. Die anwendbaren Datenschutzanforderungen sind seitens des Notars zu beachten. Nachweise werden hinterlegt.

**BotschaftsIdent**
Die natürliche Person oder ein bevollmächtigter Vertreter der juristischen Person kann sich in einer Deutschen Botschaft von einem Konsularbeamten anhand eines gültigen amtlichen Ausweises persönlich identifizieren lassen. Zulässige Dokumente sind Personalausweis oder Reisepass bei Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union oder eines Staates des Europäischen Wirtschaftsraumes, oder Dokumenten mit gleichwertiger Sicherheit. Die Identifizierung wird durch einen Konsularbeamten durch Dienstsiegel bestätigt. Nachweise werden hinterlegt.

**Dok-Ident**
Die nachzuweisenden Inhalte werden anhand von Kopien (Papierkopie, aber auch in elektronischer Form als gescanntes Dokument oder Fax) mit den Antragsdaten verglichen. Stichprobenartig werden Inhalte über einen telefonischen out-of-band-Mechanismus nachgefragt. Zulässige Dokumente sind die unter Pers-Ident aufgeführten, sowie EU Führerscheine, die über ein gesetzlich festgelegtes Ablaufdatum verfügen, Handelsregister- oder vergleichbare Auszüge, die nicht älter als ein halbes Jahr sind, Promotions-, Habilitations-, Ernennungsurkunden sowie Dokumente vergleichbaren Ranges. Nachweise werden hinterlegt.

**HR-DB**
Der TSP schließt vertragliche Vereinbarungen mit einer Organisation (Zertifikatsnehmer) und vereinbart, dass nur valide Daten übermittelt werden, die die Vorgaben der CP erfüllen. Im Rahmen üblicher Personalprozesse wird mindestens einmalig eine persönliche Identifizierung eines Mitarbeiters vorgenommen.

Ein autorisierter Mitarbeiter oder Funktionsträger einer Organisation übermittelt dem TSP über einen sicheren Kommunikationskanal Auszüge aus der Personaldatenbank (Human-Ressource DB) der Organisation bzw. Anträge, die auf Basis dieser Daten entstanden sind. Die anwendbaren Datenschutzanforderungen sind seitens der Organisation zu beachten. Der TSP vertraut auf die Richtigkeit und Eindeutigkeit der übermittelten Daten. Spätestens bei Übergabe der Token setzt der Zertifikatsnehmer den Endanwender über dessen Pflichten aus der Verpflichtungserklärung in Kenntnis. Es werden hinterlegt:

- elektronische oder papierbasierte Kopien der übermittelten Daten,
- die Bestätigung/der Nachweis des Übermittelnden als "autorisierten Mitarbeiter" bzw. "autorisierten Funktionsträger" der Organisation,
- der Nachweis, dass diese Daten von einem autorisierten Mitarbeiter zur Verarbeitung bereitgestellt wurden und der Nachweis, dass der Zertifikatsnehmer in die Verpflichtungserklärung eingewilligt hat.

Für die Identifizierung und Authentifizierung von Organisationen und Domains sowie weiterer zertifikatsrelevanter Attribute werden zur Antragsprüfung folgende Verfahren herangezogen, um die Nachweise zur Berechtigung zu ermitteln:

**Z-Bestätigung**
Ein Zeichnungsberechtigter der Organisation bestätigt zertifikatsrelevante Informationen. Dies geschieht schriftlich, es können auch elektronisch signierte Bestätigungen akzeptiert werden. Die Zeichnungsberechtigung muss entweder aus dem Existenznachweis der Organisation oder anderweitig nachgewiesen werden. Nachweise werden hinterlegt.

**A-Bestätigung**
Autorisierte Mitarbeiter oder Funktionsträger innerhalb einer Organisation oder vertrauenswürdige Dritte (z. B. Partner des TSP oder staatliche Institutionen) bestätigen bestimmte zertifikatsrelevante Informationen, die in ihrer Bestätigungskompetenz liegen. Dies geschieht schriftlich, es können auch elektronisch signierte Bestätigungen akzeptiert werden. Nachweise werden hinterlegt.

**out-of-band-Mechanismen**
Der TSP nutzt out-of-band-Mechanismen, um die Korrektheit von Antragsdaten zu prüfen, dabei werden Kommunikationswege und Prüfverfahren gewählt, die der Zertifikatsnehmer nicht beeinflussen kann. Die Nachweise werden elektronisch oder papierbasiert dokumentiert und hinterlegt.

Der Existenznachweis von Organisationen oder natürlichen Personen gegenüber dem TSP kann beispielsweise mittels Banküberweisung, Lastschrift- oder Kreditkarteneinzug erfolgen. Der TSP vertraut der Bank, die die Organisation bzw. die natürliche Person als Kunden führt. Zulässig sind seitens des TSP auch die folgenden Methoden:

a. Eine telefonische Nachfrage unter Nutzung einer Telefonnummer, die über ein öffentliches Telefonverzeichnis ermittelt wurde.

b. Eine Nachfrage über eine E-Mail-Adresse, sofern diese E-Mail-Adresse über die Register QGIS oder QIIS ermittelt wurde.

Zur Identifizierung natürlicher Personen kann eine postalische Sendung mittels "Einschreiben mit Rückschein" vom TSP an den Zertifikatsnehmer versendet werden, die Unterschrift auf dem Rückschein wird mit der Unterschrift auf den hinterlegten Nachweisen oder den Antragsunterlagen verglichen.

Die Organisationszugehörigkeit des Endanwenders kann ebenfalls mittels Testpost per "Einschreiben mit Rückschein" an die Organisation zu Händen des Endanwenders nachgewiesen werden. Die Unterschrift des Einschreibens wird mit der Unterschrift auf den hinterlegten Nachweisen oder den Antragsunterlagen verglichen. Organisationszugehörigkeit, E-Mail-Adresse, Inhalte von Extensions, sowie alle weiteren zertifikatsrelevanten Daten können auch mittels telefonischer Nachfrage des TSP über ein öffentliches Telefonverzeichnis bestätigt werden.

**Register**
Es findet ein manueller oder automatisierter Abgleich (bzw. Erfassung) der Antragsdaten mit Kopien von Registerauszügen oder elektronischen Registern statt. Zulässig sind Register staatlicher Institutionen, sogenannte Qualified Goverment Information Sources (QGIS), wie z.B Registergerichte, Bundeszentralamt für Steuern, Bundesanstalt für Finanzdienstleistungsaufsicht, berufsständischen Körperschaften öffentlichen Rechts, Deutsches Patent- und Markenamt oder vergleichbare und privatrechtliche Register, sogenannte Qualified Independent Information Sources (QIIS), wie z.B D-U-N-S, vergleichbare Wirtschaftsdatenbanken, staatliche Institutionen des Privatrechts. Die Registereinträge werden nur dann als gültig akzeptiert, wenn sie kein Attribut der Form "ungültig", "inaktiv" oder ähnliches enthalten.

**Registerprüfung im Rahmen des PSD2-Verfahrens**

Im Rahmen des PSD2-Verfahrens gemäß Abschnitt 5 der [TS 119 495] werden in der Registerprüfung, die von der National Competent Authority (NCA) herausgegebenen PSD2 spezifische Informationen zusätzlich geprüft und ins Zertifikat aufgenommen:

Für QEVCP-w, QNCP-w, QCP-l, und QCP-l-qscd mit der Ausprägung PSD2 wird zusätzlich die Rolle des Zahlungsdienstleisters (PSP) geprüft und ins Zertifikat aufgenommen. Einem Zahlungsdienstleister sind durch die nationale zuständige Behörde (NCA) eine oder mehrere Rollen (RolesOfPSP) zugeordnet:

i) kontoführende Zahlungsdienstleister (account servicing);
OID: id-psd2-role-psp-as { 0.4.0.19495.1.1 }
Rolle: PSP_AS

ii) Zahlungsauslösedienstleister (payment initiation);
OID: id-psd2-role-psp-pi { 0.4.0.19495.1.2 }
Rolle: PSP_PI

iii) Kontoinformationsdienstleister (account information);
OID: id-psd2-role-psp-ai { 0.4.0.19495.1.3 }
Rolle: PSP_AI

iv) Zahlungsdienstleister, die kartengebundene Zahlungsinstrumente ausstellen (issuing of card-based payment instruments)
OID: id-psd2-role-psp-ic { 0.4.0.19495.1.4 }
Rolle: PSP_IC

Für QEVCP-w, QNCP-w, QCP-l und QCP-l-qscd mit der Ausprägung PSD2 werden weiterhin die nationalen zuständigen Behörden (National Competent Authority - NCA) durch einen Namen „NCAName" und einen Identifikator „NCAId" beschrieben. Eine Liste der gültigen Werte für „NCAName" und „NCAId" wurden von der EBA (European Banking Authority) bereitgestellt und sind in [TS 119 495], Annex D veröffentlicht.

Nachweise werden hinterlegt.

**Non-Register**
Staatliche Einrichtungen/öffentlich-rechtliche Institutionen bestätigen zertifikatsrelevante Informationen mit Dienstsiegel und Unterschrift. Weiterhin können staatliche Organisationen auf Grund gesetzlicher Legitimation authentisiert werden. Nachweise werden hinterlegt.

**Prüfung im Rahmen der Verwaltungs-PKI (V-PKI)**
Antragsteller/ Vertragspartner werden an das BSI gemeldet. Sobald das BSI den Antragsteller/ Vertragspartner bestätigt, werden diese an das CSM angebunden und dürfen Zertifikate aus der V-PKI beziehen.

**Körperschaften**
Der TSP schließt vertragliche Vereinbarungen mit Körperschaften des öffentlichen Rechts und vereinbart, dass nur Daten übermittelt werden, die die Vorgaben der CP erfüllen. Ein autorisierter Mitarbeiter oder Funktionsträger dieser Körperschaft des öffentlichen Rechts übermittelt dem TSP über einen sicheren Kommunikationskanal Personendaten bzw. Antragsformulare, die auf Basis dieser Daten entstanden sind. Die anwendbaren Datenschutzanforderungen sind seitens der Körperschaft zu beachten. Ferner gelten die gleichen Verfahren entsprechend HR-DB.

**Kontrolle via Domain**

**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP (TLS-Zertifikate)**

Die Kontrolle über eine Domain, die in einem DNS Namen verwendet wird, muss durch die eingetragene Organisation eindeutig nachgewiesen werden. Hierzu erfolgt die Prüfung der Domain mit Hilfe der von D-Trust unterstützten Domainvalidierungsmethoden gemäß der Baseline Requirements und den von Mozilla geforderten oder empfohlenen Praktiken ausschließlich durch den TSP selbst (siehe Abschnitt 1.3.2).

Die D-Trust verwendet folgende Domainvalidierungsmethoden gemäß [BRG]:

- 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact: Bei dieser Methode erfolgt die Übermittlung eines Zufallswerts ausschließlich per E-Mail. Die Ermittlung der E-Mail-Adresse als Domainkontakt erfolgt nicht über das *Whois*-Protokoll. Wird dem TSP der Erhalt des Zufallswerts korrekt nachgewiesen, gilt die Domain als validiert.
- 3.2.2.4.4 Constructed Email to Domain Contact: Bei dieser Methode erfolgt die Übermittlung eines Zufallswerts ausschließlich per E-Mail. Diese E-Mail ist wie folgt aufgebaut: local part gemäß [BRG] Abschnitt 3.2.2.4.4, gefolgt von einem @-Zeichen und gefolgt vom ADN. Wird dem TSP der Erhalt des Zufallswerts korrekt nachgewiesen, gilt die Domain als validiert.
- 3.2.2.4.7 DNS Change: Bei dieser Methode erfolgt die Übermittlung eines Zufallswerts per E-Mail oder die Anzeige eines Zufallswerts erfolgt in der Antragsplattform „CSM". Das Geheimnis ist im CNAME-, TXT- oder CAA-RR des ADN oder des mit einem Präfix-Label versehenden ADN, welches mit einem Unterstrich beginnt, zu hinterlegen. Wird dem TSP der Zufallswert auf diese Art korrekt nachgewiesen, gilt die Domain als validiert.
- 3.2.2.4.13 Email to DNS CAA Contact: Bei dieser Methode erfolgt die Übermittlung eines Zufallswerts ausschließlich per E-Mail. Die E-Mail wird an den DNS CAA Contact versendet. Der hierfür notwendigte CAA Resource Record Set wird mit Hilfe des in RFC 8659, Abschnitt 3 definierten Suchalgorithmus ermittelt. Wird dem TSP der Zufallswert korrekt nachgewiesen, gilt die Domain als validiert.
- 3.2.2.4.14 Email to DNS TXT Contact: Bei dieser Methode erfolgt die Übermittlung eines Zufallswerts ausschließlich per E-Mail. Die E-Mail wird an den DNS TXT Record Email Contact des ADN zur Validierung des FQDN versandt. Wird dem TSP der Zufallswert korrekt nachgewiesen, gilt die Domain als validiert.
- 3.2.2.4.18 Agreed-Upon Change to Website v2.: Bei dieser Methode erfolgt die Übermittlung eines Zufallswerts per E-Mail oder die Anzeige eines Zufallswerts erfolgt in der Antragsplattform „CSM". Wird dem TSP der Zufallswert gemäß [BRG] Abschnitt 3.2.2.4.18 beschriebenen Weise nachgewiesen, gilt die Domain als validiert.

D-Trust dokumentiert für jede validierte Domain bzw. FQDN die verwendete Prüfungsmethode einschließlich der zu dem Zeitpunkt verwendete BRG/SBR-Versionsnummer. Die Aufzeichnungen werden archiviert.

**OVCP, DVCP**

Die genannten Domänenvalidierungsmethoden sind im Rahmen von OVCP und DVCP auch für die Validierung von Wildcard-Domänennamen geeignet. Zusätzlich wird die beantragte Domain gegen eine "öffentliche Suffix-Liste" geprüft, um die Ausstellung eines Wildcard-Zertifikats für einen registrierbaren Teil eines Country Code Top-Level Domain Namespace zu verhindern.

Die Methode 3.2.2.4.18 zur Domänenvalidierung von Wildcard TLS-Zertifikaten wird spätestens zum 30.11.2021 eingestellt.

**QEVCP-w, QNCP-w, EVCP**
Für diese Policy Level werden keine Wildcard TLS-Zertifikate ausgestellt.

**QEVCP-w, QNCP-w, EVCP**
Bei TLS-Zertifikaten der Policy Level QEVCP-w, QNCP-w und EVCP wird zusätzlich eine Überprüfung des Domainnamens gegen bekannte Phishing Domains und anderen Blocklists durchgeführt.

**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP**
Nicht registrierungspflichtige Domainnamen, Domains der Top-Level-Domain „.int" sowie Top-Level-Domains im Allgemeinen und onion-Zertifikate sind nicht zulässig.

Um Angriffe wie das "homographic spoofing of Internationalized Domain Names (IDNs)" zu verhindern, lässt die D-Trust IDNs von Validierungsspezialisten (Validation Specialists) einzeln und individuell prüfen. Die Freigabe erfolgt im 4-Augen-Prinzip. Bei Bedenken wird die Ausstellung von Zertifikaten abgelehnt.

Sofern E-Mail-Adressen im Rahmen der Domain-Validierung verwendet werden, müssen die E-Mail-Adressen in den TSP-Validierungsprozess so übernommen werden, wie sie in den zugelassenen Quellen vorgefunden werden.

Die Ergebnisse der Abfrage werden hinterlegt.

**Kontrolle über die Mailbox**

**NCP, LCP**
Die Kontrolle über eine Mailbox (Postfach) muss durch die im Zertifikatsantrag eingetragene Organisation über eine der folgenden Methoden nachgewiesen werden:

- **via Domain**
  Die Domainprüfung erfolgt analog zum vorangegenen Abschnitt „Kontrolle via Domain" wie bei TLS-Zertifikaten.

- **via E-Mail**
  Der TSP schickt an die zu bestätigende E-Mail-Adresse eine E-Mail mit einem Geheimnis, deren Empfang innerhalb von 24 Stunden bestätigt werden muss (Challenge-Response/ Geheimnisaustausch). Nach abgeschlossener Validierung muss das dazugehörige Zertifikat innerhalb von 30 Tagen ausgestellt sein.

**QCP-n-qscd**
E-Mail-Adressen von natürlichen Personen werden nicht überprüft.

Die Ergebnisse der Abfrage werden hinterlegt.

**IP-Adressen**
IP-Adressen werden nicht validiert und sind nicht zugelassen.

**CAA**
CAA steht für Certification Authority Authorization. Mit diesem Ressource Record (gemäß RFC6844) wird festgelegt, welche CA für die Internet-Domain TLS-Zertifikate ausstellen darf.

D-Trust prüft Fully Qualified Domain Names (FQDN) sowohl bei Antragsannahme als auch unmittelbar vor Freischaltung des Zertifikats auf einen entsprechenden CAA-Eintrag im Feld „issue" und „issuewild". Geprüfte Domains können zur Zertifikatserstellung verwendet werden, wenn entweder kein CAA Eintrag existiert oder der CAA-Eintrag leer ist oder D-Trust als CA von dem Domaininhaber in einer der folgenden Varianten eingetragen wurde: d-trust.net; dtrust.de; d-trust.de; dtrust.net.

D-Trust kann keine TLS-Zertifikate ausstellen, wenn in dem CAA Ressource Record im Feld „issue" bzw. „issuewild" eine andere CA aufgeführt ist.

### 4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Die Prüfung der Zertifikatsinhalte und der entsprechenden Nachweise erfolgt mindestens im 4-Augen-Prinzip.

Treten bei der Prüfung der Identität oder bei der Prüfung auf Korrektheit der Daten im Zertifikatsantrag bzw. den Nachweisdokumenten Unstimmigkeiten auf, die nicht restlos ausgeräumt werden können, wird der Antrag abgelehnt.

Weitere Gründe für die Antragsablehnung können sein:

- Verdacht auf die Verletzung der Namensrechte Dritter,
- Nichteinhalten von Fristen für den Nachweis der Daten,
- Zahlungsrückstände des Antragstellers gegenüber dem TSP,
- Umstände, die den Verdacht nahelegen, dass eine Zertifikatsausstellung den Betreiber der CA in Misskredit bringt oder bringen könnte (z.B. aufgrund des Verdachts auf Phishing oder anderer betrügerischer oder arglistiger Verwendung),
- Wenn die Anforderungen aus den Abschnitten der TSPS 6.1.5 und 6.1.6 bei der Erzeugung des Schlüsselpaars nicht eingehalten werden,
- Wenn es einen eindeutigen Hinweise darauf gibt, dass die spezifische Methode zur Generierung des privaten Schlüssels fehlerhaft war,
- Wenn der TSP Kenntnis davon hat, dass die Methode, die der Antragsteller zur Erzeugung seiner privaten Schlüssel nutzt, einer Kompromittierung ausgesetzt sein könnte,
- Wenn der TSP Kenntnis davon hat, dass der private Schlüssel des Antragstellers zuvor eine Schlüsselkompromittierung erlitten hat, z.B. durch die Bestimmungen in Abschnitt 4.9.1.1 [BRG] oder
- Wenn dem TSP auf der Grundlage des öffentlichen Schlüssels bekannt ist, dass der Antragsteller zur Berechnung des privaten Schlüssels eine schwache Methode genutzt hat, z. B. ein schwacher Debian-Schlüssel.

Der TSP ist berechtigt, Zertifikatsanträge auch ohne die Angabe von Gründen abzulehnen.

Erhält der TSP PKCS#10- oder andere Zertifikats-Requests, werden deren Inhalte durch den TSP auf Korrektheit überprüft.

**NCP, LCP, QCP-n-qscd, QCP-l-qscd, QCP-l**
Bestimmte Zertifikatsinhalte (z.B. O oder OU) können vertraglich festgelegt werden.

Erhält der TSP vorab Zertifikatsdaten über eine mandantenfähige Onlineschnittstelle, kann eine Vorabprüfung der Zertifikatsdaten erfolgen. Wird dann die eigentliche Zertifikatsanforderung nach der Prüfung durch den TSP übermittelt, kann eine Sofortausstellung von Zertifikaten erfolgen.

Erst nachdem der TSP den Zertifikatsantrag positiv überprüft hat und das beantragte Zertifikat übergeben wurde, gilt der Antrag als vorbehaltlos.

### 4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Es gibt keine Vorgaben für die Fristen der Bearbeitung von Zertifikatsanträgen.

## 4.3 Ausstellung von Zertifikaten

### 4.3.1 Vorgehen des TSP bei der Ausstellung von Zertifikaten

Im Hochsicherheitsbereich des Trustcenters werden digitale Zertifikate erstellt. Die technischen Ereignisse zur Erstellung werden auditierbar geloggt bzw. protokolliert.

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

Bei der Zertifikatserstellung wird sichergestellt, dass die korrekte Zeit verwendet wird.

Die vollständige Antragsdokumentation wird entweder vom TSP gemäß Abschnitt 5.5 revisionssicher abgelegt oder der TSP schließt vertragliche Vereinbarungen mit Partnern, dass die Antragsunterlagen und/oder Requests sicher und vollständig bis zum Ablauf der Frist nach Abschnitt 5.5.2. zu verwahren sind. Diese Antragsdokumentation kann jederzeit dem erstellten Zertifikat zugeordnet werden.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausstellung des Zertifikats

Es erfolgt keine gesonderte Benachrichtigung des Zertifikatsnehmers nach der Ausstellung des Zertifikats.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

## 4.4 Zertifikatsübergabe

### 4.4.1 Verhalten bei der Zertifikatsübergabe

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

Der Zertifikatsnehmer ist vor der Verwendung seines Zertifikats verpflichtet, die Zertifikatsinhalte auf Korrektheit zu überprüfen.

Entdeckt der Zertifikatsnehmer Fehler in seinen Zertifikaten oder bei dessen Verwendung, so hat er dies dem TSP unverzüglich mitzuteilen. Die Zertifikate werden widerrufen.

Fehlerhafte Angaben in den Zertifikaten gelten nur insoweit als vertraglicher Mangel im Sinne des Gesetzes, soweit der TSP nach dieser CPS eine Überprüfung der von dem Fehler betroffenen Angaben vornimmt. Im Übrigen gelten im Falle von Fehlern und deren Bestehen die entsprechenden Nacherfüllungsregeln der jeweils gültigen [AGB].

Eine Abnahme durch den Kunden erfolgt nicht, es handelt sich um eine Dienstleistung, nicht um eine Werkleistung.

### 4.4.2 Veröffentlichung des Zertifikats durch den TSP

Diese Regelungen sind im jeweiligen CPS dokumentiert.

### 4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats

Diese Regelungen sind im jeweiligen CPS dokumentiert.

## 4.5 Verwendung des Schlüsselpaars und des Zertifikats

### 4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Diese Regelungen sind im jeweiligen CPS dokumentiert.

#### 4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Die Zertifikate der D-Trust können von allen Zertifikatsnutzern verwendet werden. Es kann jedoch nur dann darauf vertraut werden, wenn

1) die Zertifikate entsprechend den dort vermerkten Nutzungsarten (Schlüsselverwendung, erweiterte Schlüsselverwendung, ggf. einschränkende Extentions) benutzt werden.
2) alle weiteren in Vereinbarungen oder an anderer Stelle angegebenen Vorsichtsmaßnahmen[5] getroffen wurden, eventuelle Einschränkungen im Zertifikat und jegliche anwendungsspezifischen Vorkehrungen seitens des Zertifikatsnutzers berücksichtigt und als kompatibel erkannt wurden.
3) die Verifikation der Zertifikatskette bis zu einem vertrauenswürdigen Root-Zertifikat erfolgreich durchgeführt wurde, um den Vertauensstatus der PKI zu überprüfen (z.B. EU Trusted List gemäß eIDAS[6] oder Rootstores von Softwareherstellern).
4) geprüft wurde, dass das Zertifikat nicht auf der zugehörigen Certificate Revocation List (CRL) als gesperrt geführt wird oder der Status der Zertifikate über den Statusabfragedienst (OCSP) positiv[7] geprüft wurde.

Sollten die Prüfmechanismen aus Punkt 3 nicht greifen, kann die Existenz und Gültigkeit eines Zertifikats über den Statusabfragedienst (OCSP) geprüft werden.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 4.6 Zertifikatserneuerung (certificate renewal)

Diese Regelungen sind im jeweiligen CPS dokumentiert.

### 4.7 Zertifikatserneuerung mit Schlüsselerneuerung

Änderungen von Angaben, die bei der Zertifikatserneuerung berücksichtigt werden sollen, müssen der D-Trust GmbH in der Regel spätestens sechs Wochen vor Ablauf der Gültigkeit des Zertifikats mitgeteilt werden.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 4.8 Zertifikatsänderung

Zertifikatsänderungen werden nicht angeboten.

### 4.9 Widerruf und Suspendierung von Zertifikaten

#### 4.9.1 Bedingungen für einen Widerruf von Zertifikaten

Die Verfahren des TSP erfüllen die Bedingungen aus [EN 319 411-1].

**QEVCP-w, EVCP**
Die Verfahren des TSP erfüllen zusätzlich die Bedingungen aus [EN 319 411-2] und [EVGL].

[5] https://www.d-trust.net/de/support/repository

[6] Regulation (EU) No 910/2014

[7] Positiv geprüft bedeutet, das eine dritte Partei über die OCSP-Statusabfrage feststellen kann, dass D-Trust das angefragte Zertifikat ausgestellt hat. Siehe Abschnitt 7.3.

**QCP-l, QNCP-w**
Die Verfahren des TSP erfüllen zusätzlich die Bedingungen aus [EN 319 411-2].

Zertifikatsnehmer, betroffene Dritte oder eine sonstige dritte Partein sind aufgefordert, den Widerruf unverzüglich zu beantragen, wenn der Verdacht besteht, dass private Schlüssel kompromittiert wurden oder Inhaltsdaten des Zertifikats nicht mehr korrekt sind (z. B. der Wegfall der Zugehörigkeit des Zertifikatsnehmers zu einer Organisation).

Beantragt der Zertifikatsnehmer eine Sperrung, wird dieser unverzüglich ausgeführt. Beantragt ein betroffener Dritter oder eine sonstige dritte Partei eine Sperrung, erfolgt vor der Sperrung eine Risikoabschätzung. Der Zertifikatnehmer wird über die Folgen der Sperrung vorab informiert.

Der Widerruf eines Zertifikats wird u.a. bei folgenden Ereignissen durchgeführt:

- auf Verlangen des Zertifikatsnehmers bzw. betroffenen Dritten (z.B. die im Zertifikat genannte Organisation),
- wenn das Zertifikat auf Grund falscher Angaben erwirkt wurde,
- wenn die ursprüngliche Zertifikatsanforderung nicht autorisiert wurde und die Autorisierung nicht rückwirkend erteilt wird,
- wenn der TSP Kenntnis davon erlangt, dass der private CA- bzw. EE-Schlüssel einer nicht authorisierten Person oder Organisation kommuniziert wurde, die dem Zertifikatsnehmer nicht zugehörig ist,
- wenn der private Schlüssel des Zertifikatsnehmers zugehörig zum öffentlichen Schlüssel im Zertifikat kompromittiert wurde,
- wenn dem TSP nachgewiesen werden kann, dass auf der Grundlage des öffentlichen Schlüssels im Zertifikat der zugehörige private Schlüssel errechnet werden kann,
- wenn dem TSP nachgewiesen werden kann, dass der Prüfung der Domainauthorisierung oder -kontrolle über den FQDN im Zertifikat nicht vertraut werden kann,
- wenn die TSP feststellt, dass das Zertifikat nicht gemäß der anwendbaren CP, TSPS,CPS und den [BRG] ausgestellt wurde oder dass die SubCA die Anforderungen der anwendbaren CP, TSPS, CPS oder die [BRG] nicht erfüllt,
- wenn die TSP feststellt, dass der Antragsteller gegen die Verpflichtungserklärung bzw. gegen die anwendbaren CP, TSPS, CPS oder die [BRG] verstößt,
- wenn zur Antragsstellung gültige Zertifikatsinhalte während des Gültigkeitszeitraums ungültig werden, z.B. durch eine Namensänderung oder mit dem Verlust der Organisationszugehörigkeit,
- wenn der TSP seine Tätigkeit beendet und diese nicht von einem anderen TSP fortgeführt wird.

**Qualifizierte Zertifikate mit der Ausprägung PSD2**
Bei qualifizierten Webseitenzertifikaten (QWACs) mit der Ausprägung PSD2 sind zusätzlich die national zuständigen Behörden (NCAs) als Herausgeber der PSD2 spezifischen Informationen berechtigt den Widerruf zu veranlassen, wenn sich die von Ihnen herausgegebenen Informationen aus Abschnitt 4.2.1 (Register) geändert haben, die sich auf die Gültigkeit des Zertifikats auswirken können.

Der Widerruf eines qualifizierten Webseitenzertifikats (QWACs) mit der Ausprägung PSD2 wird gemäß Abschnitt 6.2.6 [TS 119 495] zusätzlich bei folgenden Ereignissen durchgeführt:

- die Zulassung des Zahlungsdienstleisters (PSP) wurde widerrufen,
- eine im Zertifikat enthaltene Rolle des Zahlungsdienstleisters (PSP) wurde widerrufen

Unabhängig davon ist der TSP berechtigt, Zertifikate zu widerrufen, wenn:

- die D-Trust als Trust Service Provider (TSP) gesetzlich zum Widerruf verpflichtet ist,
- der private Schlüssel der ausstellenden oder einer übergeordneten CA kompromittiert wurde,
- das Zertifikat der ausstellenden oder einer übergeordneten CA widerrufen wurde,
- Schwächen im verwendeten Kryptoalgorithmus bekannt werden, die ernste Risiken für die erlaubten Anwendungen während der Zertifikatslaufzeit darstellen,
- die eingesetzte Hard- und Software Sicherheitsmängel aufweist, die ernste Risiken für die erlaubten Anwendungen während der Zertifikatslaufzeit darstellen,
- die eindeutige Zuordnung des Schlüsselpaars zu dem Zertifikatsnehmer nicht mehr gegeben ist,
- ein Zertifikat aufgrund falscher Angaben erwirkt wurde,
- ein begründeter Verdacht des Missbrauchs eines Zertifikats besteht,
- der Kunde nach zweimaliger Mahnung mit dem Entgelt in Verzug ist bzw. gegen die anwendbare AGB verstoßen hat,
- das Vertragsverhältnis gekündigt oder in sonstiger Weise beendet wurde,
- die CA an einen anderen TSP übergeben wird, ohne dass die dazugehörigen Sperrinformationen der ausgestellten EE-Zertifikate mit übergeben werden.

**NCP, LCP**

Für Zertifikate, die in der Lage sind, E-Mails zu signieren oder zu verschlüsseln und eine E-Mail-Adresse enthalten gelten ebenfalls die Sperrgründe gemäß Mozilla Root Store Policy 2.7, Kapitel 6.2. Je nach Sperrgrund muss das Zertifikat innerhalb von 24 Stunden gesperrt werden bzw. kann die Sperrung innerhalb von fünf Tagen erfolgen.

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

Es werden die Fristen aus Abschnitt 4.9 [BRG] eingehalten. Der Widerruf eines Zertifikats eines Zertifikatsnehmers bzw. einer ausstellenden CA erfolgt, wenn mindestens einer der Sperrgründe aus Abschnitt 4.9 [BRG] zutreffend ist.

Der TSP bietet PKI-Teilnehmern und Dritten gemäß [BRG] für TLS-Zertifikate und für ihre ausstellende oder übergeordnete CA einen zusätzlichen 24x7-Dienst, der es bei entsprechendem Verdacht ermöglicht, die Kompromittierung privater Schlüssel, den Missbrauch öffentlicher Schlüssel, einen Betrug oder technische Nicht-Konformitäten zu melden.

Sicherheitsvorfälle für diese Zertifikate bei der D-Trust können gemäß CP Abschnitt 1.5.2 beschrieben und gemeldet werden.

Der Widerruf enthält eine Angabe des Zeitpunkts des Widerrufs und wird nicht rückwirkend erstellt. Weiterhin kann ein Widerruf nicht rückgängig gemacht werden.

Sperrberechtigte müssen sich gemäß Abschnitt 3.4 des anwendbaren CPS authentifizieren. Nicht authentifizierbare Sperranträge werden nicht angenommen bzw. durchgeführt.

### 4.9.2 Berechtigung zum Widerruf

Der TSP ist grundsätzlich sperrberechtigt.

Der Zertifikatsnehmer hat stets die Berechtigung seine Zertifikate zu widerrufen, wenn er sich gegenüber dem TSP authentifizieren kann.

Enthält ein Zertifikat Angaben über die Vertretungsvollmacht des Zertifikatsnehmers für eine dritte Person, so kann auch die dritte Person einen Widerruf des betreffenden Zertifikates verlangen.

Enthält ein Zertifikat amts- und berufsbezogene oder sonstige Angaben zur Person (z.B. die Angabe „Steuerberater"), so kann auch die dritte Person, die in die Aufnahme dieser Angaben in das Zertifikat eingewilligt hat, oder die für die amts- und berufsbezogenen oder sonstigen Angaben zur Person zuständige Stelle (z.B. zuständige Kammer) einen Widerruf verlangen, wenn die Vertretungsmacht entfällt oder die Voraussetzungen für die amts- und berufsbezogenen oder sonstigen Angaben zur Person nach Aufnahme in das Zertifikat entfallen.

Zusätzliche Sperrberechtigte Dritte können benannt werden und haben dann stets die Berechtigung zum Widerruf dieser Zertifikate.

Es gilt jede Person als sperrberechtigt, soweit sie dem TSP das zutreffende Sperrpasswort mitteilt.

**EVCP, OVCP, DVCP, QEVCP-w, QNCP-w**
Grundsätzlich kann jede sonstige dritte Partei einen Zertifikatssicherheitsvorfall (Certificate Problem Report) gemäß CP 1.5.2 melden. Im begründeten Fall führt dies zur Sperrung des Zertifikats durch den TSP gemäß Abschnitt 4.9 [BRG].

### 4.9.3 Verfahren für einen Sperrantrag

Allgemeine Informationen zum Widerruf/ zur Sperrung von Zertifikaten sind über die Webseite

https://www.d-trust.net/de/support/sperrung-von-zertifikaten abrufbar.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 4.9.4 Fristen für einen Sperrantrag

Der Endanwender oder Zertifikatsnehmer muss in eigener Verantwortung dafür sorgen, dass er oder eine für ihn sperrberechtigte Person unverzüglich den Widerruf beantragt, sobald Gründe für einen Widerruf des betroffenen Zertifikats bekannt werden.

### 4.9.5 Zeitspanne für die Bearbeitung des Sperrantrags durch den TSP

Diese Regelungen sind im jeweiligen CPS dokumentiert.

### 4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Diese Regelungen sind im jeweiligen CPS dokumentiert.

### 4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Diese Regelungen sind im jeweiligen CPS in Abschnitt 2.3 dokumentiert.

### 4.9.8 Maximale Latenzzeit für Sperrlisten

Diese Regelungen sind im jeweiligen CPS dokumentiert.

#### 4.9.9 Online-Verfügbarkeit von Sperrinformationen

Diese Regelungen sind im jeweiligen CPS dokumentiert.

#### 4.9.10 Notwendigkeit zur Online-Prüfung von Sperrinformationen

Es gibt keine Pflicht zur Online-Prüfung von Sperrinformationen.

#### 4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Keine Vorgaben.

#### 4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

D-Trust sperrt ein Zertifikat aufgrund der Kompromittierung des privaten Schlüssels, wenn über eine der folgenden Methoden die Schlüsselkompromittierung demonstriert werden kann:

- Übermittlung des kompromittierten privaten Schlüssels oder
- Signierung eines CSRs mit dem Common Name Eintrag „Proof of Key Compromise for D-TRUST" durch den kompromittierten privaten Schlüssel

Zur Meldung der Schlüsselkompromittierung bietet D-Trust für TLS-Zertifikate einen Certificate Problem Report und für alle anderen Zertifikate die Übermittlung der Meldung an eine E-Mail-Adresse an. Dieser wird in der CP Kapitel 1.5.2 beschrieben und ist zu nutzen.

Sollte eine Schlüsselkompromittierung erfolgreich nachgewiesen werden, sperrt D-Trust das Zertifikat gemäß den Vorgaben aus Abschnitt 4.9. [BRG].

#### 4.9.13 Bedingungen für eine Suspendierung

Suspendierungen von Zertifikaten werden nicht angeboten.

### 4.10 Satusabfragedienst für Zertifikate

#### 4.10.1 Funktionsweise des Statusabfragedienst

Der Statusabfragedienst ist über das Protokoll OCSP verfügbar. Die Erreichbarkeit des Dienstes wird als URL in den Zertifikaten angegeben.

Die Formate und Protokolle der Dienste sind in den Abschnitten 7.2 und 7.3 des jeweiligen CPS beschrieben.

Die Systemzeit des OCSP-Responder wird täglich mit dem deutschen DCF77-Zeitsignal und verlässlichen Zeitservern (NTP) im Internet synchronisiert.

#### 4.10.2 Verfügbarkeit des Statusabfragedienst

Der Statusabfragedienst steht 24 Stunden an 7 Tagen der Woche bereit und hat eine Verfügbarkeit von 99,95%. Der TSP stellt sicher, dass im Falle einer Störung die Ausfalldauer (downtime) maximal vier Stunden beträgt.

Die Anforderungen aus Abschnitt 4.10.2 [BRG] werden erfüllt.

#### 4.10.3 Optionale Leistungen

Keine Vorgaben.

### 4.11 Austritt aus dem Zertifizierungsdienst

Die Gültigkeit eines Zertifikats endet mit dem im Zertifikat vermerkten Ablaufdatum. Der Sperrauftrag zu einem Zertifikat durch Zertifikatsnehmer oder sperrberechtigte Dritte löst die Sperrung durch den TSP aus. Die vertraglichen Hauptleistungspflichten des TSP sind damit vollständig erfüllt.

Werden innerhalb eines Vertauensdienstes Sperrlisten angeboten, wird bei Einstellung des Vertauensdienstes eine letzte CRL mit dem Eintrag "99991231235959Z" im Feld *nextUpdate* erstellt und veröffentlicht.

Wird innerhalb eines Vertauensdienstes ein OCSP Auskunftsdienst angeboten, werden OCSP Auskünfte in der Regel mit einem OCSP Signer Zertifikat aus der jeweiligen PKI des EE-Zertifikats signiert. Sollte dies nicht mehr möglich sein (gesperrt, abgelaufen), so wird ein OCSP Signer Zertifikat aus einer sicherheitstechnisch identischen CA (identisches Level, z.B. eIDAS oder Basic) genutzt.

### 4.12 Schlüsselhinterlegung und –wiederherstellung

Diese Regelungen sind im jeweiligen CPS dokumentiert.

#### 4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von privaten Schlüsseln

Diese Regelungen sind im jeweiligen CPS dokumentiert.

#### 4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Diese Regelungen sind im jeweiligen CPS dokumentiert.

## 5. Nicht-technische Sicherheitsmaßnahmen

Die spezifischen Regelungen sind in dem jeweiligen CPS dokumentiert.

Die D-Trust betreibt ein Informationssicherheitsmanagementsystem (ISMS) gemäß ISO/IEC 27001. Der Betrieb des TSP unterliegt diesem ISMS. Eine Information Security Policy regelt die verbindlichen Vorgaben für den Betrieb. Diese wurde von der Geschäftsführung der D-Trust GmbH freigegeben und an alle Mitarbeiter des TSP kommuniziert. Es erfolgt ein jährliches als auch anlassbezogenes Review und Update der Security Policy.

Führen prozess- bzw. betriebsbedingte Änderungen zu einem Update der Security Policy, sind die daraus resultierenden Änderungen für den TSP Betrieb von der Geschäftsführung zu genehmigen. Die aktualisierte und genehmigte Security Policy ist zeitnah durch die Führungskräfte an alle davon betroffenen Mitarbeiter zu kommunizieren. Die Einhaltung der Security Policy ist für Mitarbeiter verpflichtend. Es erfolgt mindestens eine jährliche Unterweisung zu bestehenden und aktualisierten Sicherheitsvorgaben.

Bis auf vereinzelte Identifizierungsdienstleistungen findet eine Auslagerung von Tätigkeiten an externe Dienstleister im Anwendungsbereich nicht statt. Soweit anwendbar werden notwendige Aspekte der Security Policy für Dienstleister ebenfalls verpflichtend.

### 5.1 Bauliche Sicherheitsmaßnahmen

Ein Konzept zur Infrastruktursicherheit dokumentiert detailliert die baulichen Sicherheitsmaßnahmen. Die Umsetzung wurde durch eine anerkannte Konformitätsbewertungsstelle geprüft. Für den Sicherheitsbereich des Trust Center hat die D-Trust eine Zertifizierung, die die Erfüllung aller Anforderungen für hohen Schutzbedarf des Prüfkatalogs Trusted Site Infrastructure TSI V3.2 Level 3 (gemäß Prüfkriterienkatalog für „Trusted Site Infrastructure" der TÜV Informationstechnik GmbH) bestätigt. Die Prüfung zur Re-Zertifizierung wird alle zwei Jahre wiederholt.

### 5.2 Verfahrensvorschriften

#### 5.2.1 Rollen- und Berechtigungskonzept

Teil der Dokumentation ist ein Rollen- und Berechtigungskonzept, in dem Mitarbeiter einer oder mehrere Rollen durch das Management des TSP zugeordnet werden und entsprechende

Berechtigungen durch einen gesteuerten Prozess erhalten. Die Berechtigungen der einzelnen Rollen beschränken sich auf diejenigen, die sie zur Erfüllung ihrer Aufgaben benötigen. Die Zuordnung der Berechtigungen wird regelmäßig durch das Sicherheitsmanagement revisioniert und umgehend nach Entfall des Bedarfs entzogen.

Rollen mit Sicherheitsverantwortung für den Betrieb des TSP, genannt „Trusted Roles", (mit unter anderem den Aufgaben des Sicherheitsbeauftragten, System Administrator, System Operator, System Auditor, Registration Officer, Revocation Officer und Validation Specialist) werden in den Berechtigungskonzepten der D-Trust festgelegt. Diese Rollen dürfen nur von fachkundigen und zuverlässigen Mitarbeitern übernommen werden. Mitarbeiter, die diese Rolle erhalten, werden gesondert unterwiesen und müssen die Übernahme der Rolle aktiv bestätigen.

Für die jeweiligen Rollen werden Stellenbeschreibungen erstellt. Diese legen die Aufgaben, das geforderte Mindestmaß an Qualifikation und Erfahrungen für die jeweilige Rolle fest. Ein Mitarbeiter, kann eine bzw. mehrere Rollen ausfüllen, vorausgesetzt die Rollen schließen sich nicht gegenseitig aus. Zusätzlich muss ein Mitarbeiter nachweisen, dass er die nötige Qualifikation und Erfahrung für diese Rolle erworben hat.

Mitarbeiter werden regelmäßig geschult, um ihre Rollen und damit verbundenen Verantwortlichkeiten zu erfüllen. Vom Informationssicherheitsmanagement regelmäßig veranlasste Sensibilisierungsmaßnahmen unterstützen die Einhaltung geltender Sicherheitsvorgaben. Mitarbeiter können sich im Rahmen von Schulungen die Qualifikation für weitere Rollen erwerben.

Die Anforderungen an die Rollen werden in Stellenbeschreibungen dokumentiert und können von den Mitarbeitern jederzeit eingesehen werden.

Im Falle von sich ausschließenden Rollen, kann ein Mitarbeiter nur eine dieser Rollen übernehmen (4-Augen-Prinzip). Eine Risikobewertung findet regelmäßig statt.

Mitarbeiter, die im Bereich der Zertifizierungs- und Sperrdienste tätig sind, agieren unabhängig und sind frei von kommerziellen und finanziellen Zwängen, die ihre Entscheidungen und Handlungen beeinflussen könnten. Die organisatorische Struktur des TSP berücksichtigt und unterstützt die Mitarbeiter in der Unabhängigkeit ihrer Entscheidungen.

### 5.2.2 Mehraugenprinzip

Besonders sicherheitskritische Vorgänge müssen mindestens im 4-Augen-Prinzip durchgeführt werden. Dies wird durch technische und organisatorische Maßnahmen wie beispielsweise Zutritts, Zugangs- und Zugriffsberechtigungen als auch die Abfrage von Wissen durchgesetzt.

Bei der Validierung von Subject Daten (insbesondere bei TLS-Zertifikaten) wird sichergestellt, dass ein erfahrener Validierungsspezialist im Mehraugenprinzip eingesetzt wird.

Sicherheitskritische Systeme zur Zertifikatsausstellung sind zusätzlich durch eine Multi-Faktor-Authentisierung geschützt.

### 5.2.3 Identifikation und Authentifizierung für einzelne Rollen

Der durchführende Mitarbeiter muss sich, bevor sie Zugang oder Zugriff auf sicherheitskritische Anwendungen erhält, erfolgreich authentifizieren. Auch der Zutritt zu sicherheitskritschen Bereichen wird personalisiert gesteuert. Über Event-Logs kann der durchführende Mitarbeiter nachträglich einer Aktion zugeordnet werden; sie ist rechenschaftspflichtig.

### 5.2.4 Rollenausschlüsse

Das Rollen- und Berechtigungskonzept sieht diverse Rollenausschlüsse vor, um Interessenskonflikte zu verhindern, das Mehraugenprinzip zu erzwingen und schädliches Verhalten vorzubeugen.

## 5.3 Eingesetztes Personal

Diese Regelungen sind im jeweiligen CPS dokumentiert.

### 5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

Der TSP gewährleistet, dass die im Bereich des Zertifizierungsdienstes tätigen Personen über die für diese Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen. Dies beinhaltet unter anderem die Anforderungen der [BRG] und der [EVGL].

Die Identität, Zuverlässigkeit und Fachkunde des Personals wird vor Aufnahme der Tätigkeit überprüft. Regelmäßige und anlassbezogene Schulungen gewährleisten die Kompetenz in den Tätigkeitsbereichen sowie die allgemeine Informationssicherheit. Schulungen und Leistungsnachweise werden dokumentiert.

Insbesondere Führungskräfte werden nach speziellen Kriterien ausgewählt. Sie müssen nachweisen, dass sie in Bezug auf den bereitgestellten Vertrauensdienst über Kenntnisse der Sicherheitsverfahren für Mitarbeiter mit Sicherheitsverantwortung und über ausreichende Erfahrung in Bezug auf Informationssicherheit und Risikobewertung verfügen. Nachweise können in Form von Zertifikaten und Lebensläufen erbracht werden. Kann die erforderliche Qualifikation nicht ausreichend nachgewiesen werden, ist diese durch eine entsprechende Schulungsmaßnahme zu erwerben, bevor der Mitarbeiter Managementfunktionen übernehmen darf.

### 5.3.2 Zuverlässigkeitsprüfungen

Personen, die in sicherheitsrelevanten Bereichen des TSP tätig sind, müssen unter anderem regelmäßig polizeiliche Führungszeugnisse vorlegen.

### 5.3.3 Schulungen

Der TSP schult Personen, die im Zertifizierungsdienst tätig sind. Das Ziel ist, dass jeder Mitabeiter die Prüfaufgaben zuverlässig kennt und alle Mitabeiter die Anweisungen gleichermaßen umsetzen, um gängige Bedrohungen des Informationsüberprüfungsprozesses (einschließlich Phishing und anderer Social-Engineering-Taktiken) zu erkennen und zu verhindern. Die Schulungen umfassen die Anforderungen aus den eigenen Zertifizierungspraktiken als auch die externen anwendbaren Anforderungen (z.B. BRG, ETSI, BSI).

Bei Nicht-Teilnahme an Pflichtschulungen können Mitarbeiter von sicherheitsrelevanten Tätigkeiten ausgeschlossen werden.

Übergreifend betreibt der TSP ein nach ISO 27001 zertifiziertes ISMS. Im Rahmen dessen werden den Mitarbeitern entsprechend sicherheitsrelevante Vorgaben bzw. Verhaltensregeln zugänglich gemacht.

### 5.3.4 Häufigkeit von Schulungen und Belehrungen

Der TSP schult Personen, die im Zertifizierungsdienst tätig sind zu Beginn ihres Einsatzes, jährlich und bei Bedarf.

### 5.3.5 Häufigkeit und Folge von Job-Rotation

Rollenwechsel werden dokumentiert. Die entsprechenden Mitarbeiter werden geschult.

### 5.3.6 Maßnahmen bei unerlaubten Handlungen

Der TSP schließt unzuverlässige Mitarbeiter von den Tätigkeiten im Zertifizierungsdienst aus.

Verstöße von Mitarbeitern gegen die Richtlinien oder die Prozesse des TSP-Betriebs werden analysiert und bewertet. Kann das Vertrauensverhältnis nicht sichergestellt werden, werden diese Mitarbeiter von sicherheitsrelevanten Tätigkeiten ausgeschlossen.

### 5.3.7 Anforderungen an externe Mitarbeiter

Externe Mitarbeiter, welche im Bereich der Vertrauensdienste aktiv sind, erfüllen die Anforderungen aus Kapitel 5.3 dieses TSPS und unterliegen den Sanktionen nach Kapitel 5.3.6 dieses TSPS.

### 5.3.8 Ausgehändigte Dokumentation

Umfangreiche Verfahrensanweisungen definieren für alle Tätigkeiten die zuständigen Mitarbeiterrollen und -rechte sowie entsprechende manuelle und maschinelle Prüfungen. Durch die sicherheitstechnische Infrastruktur der D-Trust GmbH ist gewährleistet, dass von diesen definierten Verfahren nicht abgewichen werden kann.

## 5.4 Überwachungsmaßnahmen

### 5.4.1 Überwachung des Zutritts

Die Überwachung des Zutritts wird durch Videoüberwachung und Zonenverfolgung sichergestellt.

Besucher müssen mindestens 24 Stunden vor dem Besuch namentlich angemeldet werden und befinden sich stets in Begleitung eines Mitarbeiters des TSP.

### 5.4.2 Überwachung von Risiken

Relevante Assets werden angemessen erfasst, sowie entsprechende Änderungen dieser Assets überprüft und wenn anwendbar durch das vom Management beauftragte Personal des TSP freigegeben. Auf dessen Basis erfolgt die Identifikation, die Analyse, die Bewertung sowie die Behandlung und die Überwachung von Risiken.

Es werden in einer mindestens jährlichen Risikoanalyse, die Bedrohung für den Betrieb des TSP umfassend analysiert sowie Anforderungen und Gegenmaßnahmen als auch deren Umsetzung definiert. Ferner wird im Rahmen der Risikoübernahme das verbleibende Restrisiko ausgewiesen, in der die Vertretbarkeit des Restrisikos aufgezeigt und ggf. von der Geschäftsführung akzeptiert wird.

## 5.5 Archivierung von Aufzeichnungen

### 5.5.1 Arten von archivierten Aufzeichnungen

Es wird zwischen Aufzeichnungen in elektronischer und papierbasierter Form unterschieden.

Archiviert werden die vollständigen Antragsunterlagen, Dokumente zu Verfahrensrichtlinien (CP, TSPS, CPS), Zertifikate, Sperrdokumentation, elektronische Dateien und Protokolle zum Zertifikatslebenszyklus. Dabei werden die Vorgänge zeitlich erfasst. Wenn anwendbar, umfasst dies auch die entsprechenden Systemprotokolle, die im Rahmen der genannten Ereignisse entstehen.

**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP**
Es werden mindesten die in Abschnitt 5.4.1[BRG] geforderten Ereignisse auditierbar geloggt bzw. protokolliert.

Der TSP stellt sicher, dass von ihm archivierte Daten während ihrer Speicherfristen nicht unberechtigt manipuliert werden können.

Weiterhin werden sicherheitsrelevante Ereignisse entsprechend aufgezeichnet. Die Systemzeit wird täglich mit dem deutschen DCF77-Zeitsignal und verlässlichen Zeitservern (NTP) im Internet synchronisiert.

### 5.5.2 Aufbewahrungsfristen für archivierte Daten

Die Nachvollziehbarkeit der Identifizierung auf deren Grundlage ein Zertifikat ausgestellt wird, ist ein Qualitätsmerkmal des Zertifikates. Die Dokumente zur Antragstellung und Prüfung, die Daten zum Zertifikatslebenszyklus sowie die Zertifikate selbst werden gemäß den gesetzlichen oder in Zertifizierungen vorgegebenen Aufbewahrungsfristen produktabhängig erstellt und entsprechend aufbewahrt[8].

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

Für qualifizierte Signatur- und Siegelzertifikate gelten für Zertifikate, Zertifikatsnachweisdaten, einschließlich der Kontaktdaten die Vorgaben des § 16 Abs. 4 Vertrauensdienstegesetz zur dauerhaften Aufbewahrung. Dies entspricht der gesamten Dauer des Betriebes des Trust Service Provider (TSP).

Vor Einstellung des Betriebs ist die Übergabe an die Bundesnetzagentur oder einen anderen qualifizierten Trust Service Provider (TSP) vorgeschrieben.

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

Gemäß Abschnitt 5.5.2 [BRG] gilt für die Archivierung von Zertifikatsnachweisdaten wie Daten zur Antragstellung, Identifizierung, Sperrung und die Zertifikate selbst eine Aufbewahrung von sieben Jahren nachdem das Zertifikat seine Gültigkeit verloren hat.

Für die in Abschnitt 5.4.3. [BRG] definierten Audit Logs gilt eine Aufbewahrung von mind. zwei Jahren.

**NCP, LCP, V-PKI**

Im Rahmen der Archivierung von Zertifikatsnachweisdaten wie Daten zur Antragstellung, Identifizierung, Sperrung und die Zertifikate selbst erfolgt eine Aufbewahrung von mindestens sieben Jahren nachdem das Zertifikat seine Gültigkeit verloren hat.

Für die Audit Logs gilt eine Aufbewahrung von mind. zwei Jahren.

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

Vor Einstellung des Betriebs werden die archivierten Daten an einen anderen (qualifizierten) Trust Service Provider (TSP) oder an die Bundesdruckerei übergeben. Der TSP verfügt über eine Zusicherung der Bundesdruckerei für die Erfüllung der Mindestanforderungen an die Aufbewahrungsfristen.

Die Archivierung und Nachverfolgung von Zertifikaten und Registrierungsdaten werden vom TSP bzw. von vertraglich gebundenen Partnern oder externen Anbietern, die die Maßgaben der CP, TSPS und CPS erfüllen, durchgeführt, so dass diese im Falle eines erforderlichen Backups genutzt werden können. Dabei sollen die Maßgaben der TR-03145-1 Kapitel 6.10 eingehalten werden.

Die Frist beginnt nach Ablauf der Gültigkeit des Zertifikates, das zuletzt auf der Basis dieser Dokumente ausgestellt wurde.

Event-Logs der IT-Systeme werden mindestens 6 Monate gespeichert. Die Speicherdauer von personenbezogenen Videoaufzeichnungen und Aufzeichnungen der administrativen Tätigkeiten beträgt 90 Tage.

[8] Sind auf dem Token zusätzlich zu den nicht-qualifizierten Zertifikaten der Root-PKI weitere qualifizierte Endnutzerzertifikate, gelten die Aufbewahrungsfristen dieser Zertifikate.

Für das Archivierungssystem wird die Systemzeit täglich mit dem deutschen DCF77-Zeitsignal und verlässlichen Zeitservern (NTP) im Internet synchronisiert.

#### 5.5.3 Sicherung des Archivs

Das Archiv des Trust Service Provider (TSP) befindet sich in gesicherten Räumen und unterliegt dem Rollen- und Zutrittskonzept des TSP.

#### 5.5.4 Datensicherung des Archivs

Vertraulichkeit und Integrität der Daten werden gewahrt. Die Dokumentation erfolgt unverzüglich, so dass sie nachträglich nicht unbemerkt verändert werden kann. Die europäischen und deutschen Datenschutzanforderungen werden eingehalten.

#### 5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

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

#### 5.5.6 Archivierung (intern / extern)

Die Archivierung erfolgt intern beim TSP, sowie extern in gleichwertig gesicherten Räumen.

#### 5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen

Das Verfahren zur Beschaffung und Verifikation von Archivinformationen unterliegt dem Rollenkonzept des Trust Service Provider (TSP).

### 5.6 Schlüsselwechsel beim TSP

Eine angemessene Zeit vor Ablauf einer CA oder Sub-CA werden neue CA- oder Sub-CA-Schlüssel generiert, neue CA- oder Sub-CA-Instanzen aufgesetzt und veröffentlicht. Dies gilt auch für Dienstezertifikate falls diese relevant sind.

### 5.7 Kompromittierung und Geschäftsweiterführung beim TSP

#### 5.7.1 Behandlung von Vorfällen und Kompromittierungen

Der TSP verfügt über ein Notfallkonzept sowie einen Wiederanlaufplan, die den beteiligten Rollen bekannt sind und von ihnen im Bedarfsfall umgesetzt werden. Die Verantwortlichkeiten sind klar verteilt und bekannt.

Sollte eine Systemwiederherstellung erforderlich sein, sind die Verantwortlichkeiten und entsprechenden „Trusted Roles" im Berechtigungskonzept der D-Trust deklariert und den jeweiligen Mitarbeitern bekannt. Siehe Abschnitt 5.2.1.

#### 5.7.2 Wiederherstellung nach Kompromittierung von Ressourcen

Die Recovery-Prozeduren für die Wiederherstellung der Betriebsfähigkeit des TSP sind definiert. Es erfolgt ein tägliches Backup und ein Backup nach Veränderungen. Backups werden in einem anderen Brandabschnitt aufbewahrt. Die Wiederherstellungen von kritischen CA-Systemen werden im Rahmen von Notfallübungen regelmäßig getestet.

#### 5.7.3 Kompromittierung des privaten CA-Schlüssels

Im Fall einer Kompromittierung oder der Bekanntgabe von Unsicherheit von Algorithmen oder assoziierten Parametern, veranlasst der TSP folgendes:

- betroffene CA-Zertifikate sowie deren ausgestellte und bisher nicht ausgelaufene Zertifikate werden widerrufen,
- involvierte Zertifikatsnehmer werden über den Vorfall und dessen Auswirkungen informiert,

- die zuständige Aufsichtsstelle sowie im Falle von publicly trusted CA-Zertifikaten die Certificate Consumer Mitglieder des CA Browser/Forums werden informiert und der Vorfall wird auf den Webseiten des TSP veröffentlicht mit dem Hinweis, dass Zertifikate, die von dieser CA ausgestellt wurden, ihre Gültigkeit verlieren und der Sperrstatus verifiziert werden kann.

Aus der Analyse der Gründe für die Kompromittierung werden, wenn möglich, Maßnahmen ergriffen, um zukünftige Kompromittierungen zu vermeiden. Unter Berücksichtigung der Gründe für die Kompromittierung werden neue CA-Signaturschlüssel generiert und neue CA-Zertifikate ausgestellt.

#### 5.7.4 Möglichkeiten zur Geschäftsfortführung

In einem Notfall entscheidet der TSP je nach Art des Vorfalls, ob ein Recovery des in Abschnitt 6.2.4 beschriebene Backups der CA durchgeführt oder bei Kompromittierung gemäß Abschnitt 5.7.3 verfahren wird. Im Anschluss wird die Wiederherstellung zum Normalbetrieb angestrebt, die alle benötigten Dienste für einen Zertifikatsnehmer wieder bereitstellt.

### 5.8 Beendigung des TSP bzw. die Beendigung des Dienstes

Die D-Trust verfügt über einen fortlaufend aktualisierten Beendigungsplan.

Bei Beendigung der Dienste von CAs informiert der TSP alle Zertifikatsnehmer und beendet alle Zugriffsmöglichkeiten von Unterauftragnehmern des TSP in Bezug auf die betroffenen CAs. Alle noch gültigen und von den betroffenen CAs ausgestellten Zertifikate werden widerrufen. Betroffene private CA-Schlüssel werden zerstört.

Im Fall einer geplanten Betriebseinstellung informiert der TSP alle Endanwender, Zertifikatsnehmer und Dritte vorab.

Der Verzeichnisdienst und Dokumente zur Antragstellung sowie das Repository (CP, CPS, TSPS und CA-Zertifikate) werden an die Bundesdruckerei GmbH übergeben und unter äquivalenten Bedingungen weitergeführt. Die Aufrechterhaltung des Verzeichnisdienstes wird bis Ablauf der EE-Zertifikatsgültigkeit, zugesichert und entweder einem anderen TSP oder der Bundesdruckerei GmbH übergeben.

Der TSP verfügt über eine entsprechende Zusicherung der Bundesdruckerei für die Erfüllung dieser Mindestanforderungen.

Mit Beendigung des Betriebes werden alle Funktionalitäten der betroffenen CAs eingestellt.

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

Die Zertifikatsdatenbank wird zusammen mit den Widerrufsinformationen und dem Repository (CP, TSPS, CPS und CA-Zertifikate) gemäß § 16 Absatz 1 VDG an die Bundesnetzagentur übergeben.

## 6. Technische Sicherheitsmaßnahmen

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

### 6.1 Erzeugung und Installation von Schlüsselpaaren

#### 6.1.1 Erzeugung von Schlüsselpaaren

CA-Schlüssel und Schlüssel für Dienstezertifikate werden in einem „FIPS 140-2 Level 3" ODER einem CC-evaluiertem (gemäß Protection Profile EN 419 211-5) Hardware Security Module (HSM) erzeugt. Das HSM befindet sich im Hochsicherheitsbereich des Trustcenters.

Die Key-Ceremony erfolgt nach festgelegten Verfahren. In Abhängigkeit der CA erfolgt die Key-Ceremony durch dafür vorgesehene Trusted Roles im Beisein des Security Officers und falls erforderlich unter Aufsicht eines unabhängigen Dritten. Die Tätigkeiten während der Key Ceremony werden mittels Checkliste geprüft und protokolliert. Bei der Schlüsselerzeugung wird die Durchsetzung des Rollenkonzepts und somit das 4-Augen-Prinzip durch die willentliche Eingabe der Aktivierungsdaten zur Signaturerzeugung des CA Zertifikats erzwungen. Bei der Erzeugung von CA-Schlüsseln ist gegebenenfalls ein unabhängiger Auditor anwesend oder der Auditor kann sich nach der Schlüsselerzeugung durch eine Videoaufzeichnung vom ordnungsgemäßen Ablauf der Schlüsselerzeugung überzeugen.

Weiterhin wird die Erstellung von CA-Schlüsseln und ggf. Dienstezertifikaten:

- für Produkte innerhalb der **Root CPS und CSM CPS:** gemäß [EN 319 411-1] bzw. [EN 319 411-2],
- für Produkte innerhalb der **Cloud CPS:** gemäß [EN 319 421] bzw. [EN 319 411-1] bzw. [EN 319 411-2]

dokumentiert.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Diese Regelungen sind im jeweiligen CPS dokumentiert.

### 6.1.3 Lieferung öffentlicher Schlüssel an den TSP

Diese Regelungen sind im jeweiligen CPS dokumentiert.

### 6.1.4 Lieferung öffentlicher CA-Schlüssel and Zertifikatsnutzer

Diese Regelungen sind im jeweiligen CPS dokumentiert.

### 6.1.5 Schlüssellängen

Für CA- und Dienstezertifikate werden derzeit RSA-Schlüssel mit einer Schlüssellänge von mindestens 2048 Bit verwendet.

ECC-Schlüssel mit 384 Bit werden für die neuen Root-CAs und Sub-CAs mit dem Policy Level DVCP, QCP-n und QCP-l verwendet.

Für EE-Zertifikate werden derzeit RSA-Schlüssel mit einer Schlüssellänge von mindestens 2048 Bit und ECC-Schlüssel mit einer Schlüssellänge von mindestens 256 Bit verwendet.

**QEVCP-w, QNCP-w, EVCP,OVCP, DVCP, NCP, LCP**
Die verwendeten RSA Schlüssellängen sind durch den Modulus 8 teilbar.

Signatur- und Verschlüsselungsalgorithmus sind im Abschnitt 7.1.3 genannt.

### 6.1.6 Festlegung der Schlüsselparameter und Qualitätskontrolle

Dieses TSPS erläutert die jeweiligen Festlegungen für die folgenden Policy Level:

- **OVCP, DVCP, NCP, LCP:** Dienste-, CA- und EE-Zertifikate werden auf Grundlage von Schlüsseln ausgestellt, die [ETSI-ALG], [EN 319 411-1] und [BRG] in der aktuell gültigen Fassung entsprechen, soweit Kompatibilität im Verwendungsumfeld gewährleistet ist.
- **QEVCP-w, EVCP:** CA- und EE-Zertifikate werden ausschließlich auf Grundlage von Schlüsseln ausgestellt, die [ETSI-ALG], [EN 319 411-1], [EN 319 411-2], [BRG] und [EVGL] in der aktuell gültigen Fassung entsprechen.

- **QNCP-w:** CA- und EE-Zertifikate werden ausschließlich auf Grundlage von Schlüsseln ausgestellt, die [ETSI-ALG], [EN 319 411-1], [EN 319 411-2] und [BRG] in der aktuell gültigen Fassung entsprechen.
- **QCP-l, QCP-l-qscd, QCP-n-qscd:** EE-Zertifikate werden ausschließlich auf Grundlage von Schlüsseln ausgestellt, die [ETSI-ALG], [EN 319 411-1] und [EN 319 411-2] in der aktuell gültigen Fassung entsprechen.
- **V-PKI:** EE-Zertifikate werden auf Grundlage von Schlüsseln ausgestellt, die bei Projekten der Bundesregierung nach den kryptographischen Vorgaben aus BSI [TR-02102-1] generiert wurden.

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

Für ECDSA-Schlüsselpaare stellt der TSP sicher, dass der Schlüssel einen gültigen Punkt auf der elliptischen Kurve NIST P-256, NIST P-384 oder NIST P-521 darstellt.

Signatur- und Verschlüsselungsalgorithmus sind im Abschnitt 7.1.3 genannt.

### 6.1.7 Schlüsselverwendungen

Private Root-CA-Schlüssel werden ausschließlich zum Signieren von CA-Zertifikaten, Dienstezertifikaten und Sperrlisten verwendet. Alle anderen privaten CA-Schlüssel werden zum Signieren von CA-Zertifikaten, Dienstezertifikaten, EE-Zertifikaten und Sperrlisten benutzt (siehe Abschnitt 7.1.2).

Die EE-Schlüssel dürfen nur für die im Zertifikat benannten Nutzungsarten verwendet werden. Die Nutzungsarten werden in den Feldern *keyUsage* und *extKeyUsage* im Zertifikat definiert und ggf. durch weitere Extentions eingeschränkt (siehe Abschnitt 7.1.2).

Private Schlüssel von Dienstezertifikaten für Zeitstempel werden ausschließlich im Rahmen des Zeitstempeldienstes verwendet.

## 6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

### 6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

Während des gesamten Lebenszyklus (einschließlich Lieferung und Lagerung) werden die Module durch technische und organisatorische Maßnahmen vor unbefugter Manipulation geschützt.

Zur Sicherung der CA-Schlüssel wird ein HSM eingesetzt, das entsprechend FIPS 140-2 Level 3 ODER gemäß Common Criteria (gemäß Protection Profile EN 419 211-5) evaluiert wurde.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

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

Diese Regelungen sind im jeweiligen CPS dokumentiert.

### 6.2.3 Hinterlegung privater Schlüssel (key escrow)

Diese Regelungen sind im jeweiligen CPS dokumentiert.

### 6.2.4 Backup privater Schlüssel

Es ist ein Backup der privaten CA-Schlüssel vorhanden. Ein CA-Schlüssel-Backup erfordert für diese Tätigkeit am HSM zwei autorisierte Personen und findet in der sicheren Umgebung des Trustcenters statt. Für das Backupsystem gelten die gleichen Voraussetzungen und Sicherungsmaßnahmen wie für das Produktivsystem. Eine Wiederherstellung privater Schlüssel erfordert ebenfalls zwei autorisierte Personen. Weitere Kopien der privaten CA-Schlüssel existieren nicht.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 6.2.5 Archivierung privater Schlüssel

Private CA- und EE-Schlüssel werden nicht archiviert.

### 6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Ein Transfer privater CA-Schlüssel in oder aus dem HSM erfolgt nur zu Backup- und Wiederherstellungszwecken. Ein 4-Augen-Prinzip wird erzwungen. Bei Export/Import in ein anderes HSM schützt eine Verschlüsselung den privaten CA-Schlüssel.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Die privaten Schlüssel für CA- und Dienstezertifikate liegen verschlüsselt im HSM vor.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 6.2.8 Aktivierung privater Schlüssel

Die privaten CA- und Diensteschlüssel können nur im 4-Augen-Prinzip und von den zuständigen Rollen und für die zulässigen Nutzungsarten (*keyCertSign, cRLSign*) aktiviert werden.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 6.2.9 Deaktivierung privater Schlüssel

Die privaten Schlüssel für CA- und Dienstezertifikate werden durch Beendigung der Verbindung zwischen HSM und Anwendung durch dafür vorgesehene Trusted Roles deaktiviert.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 6.2.10 Zerstörung privater Schlüssel

Die privaten CA-Schlüssel werden durch dafür vorgesehene Trusted Roles gelöscht, wenn ihre geplante Nutzungsdauer abgelaufen ist. Die Nutzungsdauer ist gemäß ETSI ALGO Paper TS 119 312 und SOG-IS festgelegt. Dies erfolgt durch Löschen auf dem HSM und gleichzeitigem Löschen der auf Datenträgern angelegten Backups. Bei Stilllegung des HSMs werden die privaten Schlüssel auf dem Gerät gelöscht.

Werden die Dateien, die den privaten EE-Schlüssel enthalten, gelöscht, so ist der private Schlüssel zerstört.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 6.2.11 Beurteilung kryptographischer Module

Der TSP betreibt geeignete hard- und softwarebasierte Schlüsselgeneratoren gemäß [EN 319 421] bzw. [EN 319 411-1] und [EN 319 411-2] und bei Projekten der Bundesregierung gemäß BSI [TR-02102-1], um die Qualität der Schlüssel zu sichern.

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

Die Liste der QSCDs in Deutschland wird von der Aufsichtsbehörde Bundesnetzagentur (BNetzA) öffentlich bereitgestellt.

D-Trust überwacht die Gültigkeitsdauer der verwendeten QSCDs. Es wird sichergestellt, dass keine Zertifikate mit längerer Laufzeit als die Gültigkeitsdauer der QSCD ausgestellt werden oder es wird alternativ sichergestellt, dass bei Ablauf der Gültigkeit der QSCD die Zertifikate gesperrt werden.

## 6.3 Andere Aspekte des Managements von Schlüsselpaaren

### 6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche Dienste-, CA- und EE-Schlüssel werden in Form der erstellten Zertifikate archiviert.

### 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.

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

Die ausstellenden CA stellen keine EE-Zertifikate aus, die länger gültig sind als das CA-Zertifikat selbst.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

## 6.4 Aktivierungsdaten

### 6.4.1 Erzeugung und Installation von Aktivierungsdaten

Die Aktivierungsdaten der Dienste-und CA-Schlüssel werden durch die Smartcard bzw. das HSM abgefragt. Ein 4-Augen-Prinzip wird erzwungen.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 6.4.2 Schutz von Aktivierungsdaten

Die Aktivierungsdaten der Dienste- und CA-Schlüssel setzen sich aus zwei Geheimnissen zusammen, von denen jeweils ein berechtigter Mitarbeiter eines kennt. Der Zugriff auf die Aktivierungsdaten ist nur autorisierten Mitarbeitern möglich.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 6.4.3 Andere Aspekte von Aktivierungsdaten

Diese Regelungen sind im jeweiligen CPS dokumentiert.

## 6.5 Sicherheitsmaßnahmen in den Rechneranlagen

### 6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Die vom TSP eingesetzten Computer, Netze und andere Komponenten stellen in der eingesetzten Konfiguration sicher, dass nur Aktionen durchgeführt werden können, die nicht im Widerspruch zur CP der D-Trust GmbH und

- für Produkte innerhalb der **CSM CPS:** der CSM CPS, [EN 319 411-1] bzw. [EN 319 411-2] und im Fall von EV-Zertifikaten zu [EVGL],
- für Produkte innerhalb der **Root CPS:** der Root CPS, [EN 319 411-1] bzw. [EN 319 411-2] und im Fall von EV-Zertifikaten zu [EVGL],
- für Produkte innerhalb des **Cloud CPS:** der Cloud CPS, [EN 319 421], [EN 319 411-1] bzw. [EN 319 411-2],
- für Produkte innerhalb des **Device CPS:** der Device CPS, [TR-03145-1],
- für Produkte innerhalb der **E.ON CPS:** der E.ON CPS und [EN 319 411-1] oder
- für Produkte innerhalb der **Uniper CPS:** der Uniper CPS und [EN 319 411-1]

stehen.

Die Computersicherheit des TSP wird für exponierte Systeme u.a. durch mehrstufige Sicherheitssysteme zum Zwecke des perimetrischen Virenschutzes, Endpoint-Protection und integritätssichernde Werkzeuge sichergestellt.

Es wird sichergestellt, dass sicherheitsrelevante Softwareupdates in angemessener Zeit auf den relevanten Systemen installiert werden. Die Bewertung und ggf. die Behebung von identifizierten Schwachstellen erfolgt innerhalb von 48 Stunden. Ist die Behebung innerhalb von 48 Stunden nicht möglich, so enthält die Bewertung einen konkreten Behandlungsplan.Abweichungen hiervon werden vom TSP angemessen dokumentiert und ggf. im Risikomanagement des TSP adressiert.

Zertifikatsnehmer und Zertifikatsnutzer müssen vertrauenswürdige Computer und Software verwenden.

Die Systemzeit der relevanten CA-Systeme wird durch eine redundant angeschlossene Funkuhr sichergestellt.

Alle zum Betrieb notwendigen Systeme (Statusdienst, Sperrdienst, Zertifikatsmanagement) sind mindestens über ein Aktiv/Passiv-Cluster (Hot standby) redundant ausgelegt.

**LCP, NCP**

Bei der Neubeantragung von Zertifikaten, deren Schlüssel vom TSP generiert wird, sind Systeme beteiligt, die mindestens mit einem Ersatzserver (Cold standby) redundant ausgelegt sind.

### 6.5.2 Beurteilung von Computersicherheit

Die für die CA-Schlüssel eingesetzten Computer, Netze und andere Komponenten wurden durch anerkannte Konformitätsbewertungsstellen geprüft und unterliegen gemäß [EN 319 401] einem entsprechenden Monitoring.

### 6.5.3 Monitoring

Zur Sicherstellung der Verfügbarkeit erfolgt ein kontinuierliches Monitoring der relevanten Systeme. Jede Störung wird erfasst, dokumentiert und gemäß ihrer Auswirkung mit einem Schweregrad gekennzeichnet und daraufhin priorisiert. Die Behandlung von kritischen Meldungen erfolgt im Rahmen des Prozesses Incident Management. Meldungen zu sicherheitsrelevanten Ereignissen werden an eine zentrale Stelle übermittelt und gemäß Kritikalität ausgewertet.

Bei langanhaltenden Störungen mit Verfügbarkeitsverlust eines Services werden die betroffenen Parteien mindestens alle 24 Stunden über einen aktuellen Status zur Störungsbeseitigung informiert.

## 6.6 Technische Maßnahmen während des Life Cycles

Produktive Serversysteme erhalten sicherheitsrelevante Konfigurationen über zentrale Managementsysteme. Nicht zwingend benötigte Dienste werden deaktiviert. Es erfolgt alle 15 Minuten eine Überprüfung der Konfigurationen. Festgestellte Abweichungen gegen die zentralen Sicherheitsrichtlinien werden unmittelbar in den Konfigurationen korrigiert.

Bereits bei der Planung aller vom TSP oder im Auftrag des TSP betriebener Systeme werden die Anforderungen aus Abschnitt 5 [BRG] angemessen berücksichtigt.

### 6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

Bei der Entwicklung aller vom TSP oder im Auftrag des TSP durchgeführter Systementwicklungsprojekte werden Sicherheitsanforderungen im Entwurfsstadium analysiert. Die gewonnenen Erkenntnisse werden als Anforderungen bei der Entwicklung festgelegt.

Die Testumgebung der D-Trust für Entwicklungs-, Test- und Staging-Systeme ist getrennt von ihren Produktionssystemen.

### 6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Ausschließlich entsprechend dem Rollenkonzept autorisiertes Personal darf Computer, Netze und andere Komponenten administrieren. Es findet eine regelmäßige Auswertung von Logfiles auf Regelverletzungen, Angriffsversuche und andere Vorfälle statt. Überwachungsmaßnahmen beginnen mit Inbetriebnahme eines Gerätes und enden mit dessen Entsorgung.

### 6.6.3 Sicherheitsmaßnahmen während des Life Cycles

Eingesetzte Geräte werden gemäß Herstellerangaben betrieben. Vor Inbetriebnahme werden sie eingehend geprüft und kommen nur zum Einsatz, wenn feststeht, dass sie nicht manipuliert wurden. Bei Verdacht auf Manipulation einer Komponente, wird eine ggf. geplante Aktion an der Komponente nicht durchgeführt und der Vorfall gemeldet. Um kurzfristig und koordiniert auf eventuelle sicherheitsrelevante Vorfälle reagieren zu können, definiert der TSP klare Eskalationsrichtlinien für die einzelnen Rollen.

Kapazitätsanforderungen und -auslastungen sowie Eignung der beteiligten Systeme werden überwacht und bei Bedarf angeglichen. Geräte oder Datenträger werden derart außer Betrieb genommen und entsorgt, dass Funktionalitäts- oder Datenmissbrauch ausgeschlossen wird. Änderungen an Systemen, Software oder Prozessen durchlaufen einen dokumentierten Change-Management-Prozess. Sicherheitskritische Änderungen werden durch den Informationssicherheitsbeauftragten geprüft. Nach Ablauf der Gültigkeit von CAs werden die privaten Schlüssel vernichtet.

Elektronische Daten oder papiergebundene Protokolle dokumentieren alle relevanten Ereignisse, die den Life-Cycle der CA sowie der ausgestellten Zertifikate und generierten Schlüssel beeinflussen und werden auf langlebigen Medien revisionssicher gespeichert. Die Medien des Unternehmens werden entsprechend ihrer Klassifizierung im Rahmen der Dokumentationsrichtlinie des TSP zuverlässig vor Schaden, Entwendung, Verlust oder Kompromittierung geschützt.

Penetrationstests werden durch eine unabhängige und fachkundige Stelle mindestens einmal pro Jahr durchgeführt. Weiterhin werden mindestens einmal pro Quartal Schwachstellenscans veranlasst. Die Ergebnisse des Penetrationstestberichts werden intern archiviert.

## 6.7 Sicherheitsmaßnahmen für Netze

Im Betrieb der CAs wird ein Netzkonzept realisiert, welches sicherstellt, dass die relevanten CA-Systeme in besonders gesicherten Netzwerkzonen betrieben werden. Die Netzwerkarchitektur des TSP beinhaltet ein mehrstufiges Konzept der Netzwerksicherheitszonen. Die Root CAs werden in der Netzwerksicherheitszone mit dem höchsten Schutzbedarf betrieben.

Zum Schutz der Prozesse des TSP werden Firewall und Intrusion Detection / Prevention Mechanismen eingesetzt, die nur explizit erlaubte Verbindungen zulassen. D-Trust betreibt Netzsegmente unterschiedlichen Schutzbedarfs und trennt dabei mitarbeiter- und internetnahe Netze sorgfältig von Servernetzwerken. Die Systeme unterliegen regelmäßigen Revisionen, die Verantwortlichen sind berichtspflichtig. Auffälligkeiten werden durch technische Systeme und organisatorische Prozesse gemeldet und in einem definierten Incidentverfahren und daran ansetzenden Prozessen behandelt.

Die Verfügbarkeit der Internetanbindung ist durch Redundanz abgesichert. Es bestehen zwei ständige Verbindungen zum Provider auf zwei unterschiedlichen Streckenführungen. Beim Ausfall des Zugangspunktes des Providers erfolgt die automatische Umschaltung auf die zweite Anbindung.

Datenverkehr mit hohem Schutzbedarf außerhalb der durch den TSP geschützten Netzwerke, für den Integrität oder Vertraulichkeit sichergestellt werden muss, wird durch kryptographische Mechanismen geschützt.

Die physische Sicherheit der durch den TSP betriebenen und genutzten Netze ist sichergestellt und wird den baulichen Gegebenheiten und ihren Veränderungen angepasst.

D-Trust hält die spezifischen Anforderungen aus [NetSec-CAB] ein.

### 6.8 Zeitstempel

Der TSP betreibt einen Zeitstempeldienst.

Die spezifischen Regelungen sind im Cloud CPS dokumentiert.

## 7. Profile von Zertifikaten, Sperrlisten und OCSP

### 7.1 Zertifikatsprofile

#### 7.1.1 Versionsnummern

Es werden Zertifikate im Format X.509v3 und gemäß EN 319 412-2, -3 bzw. -4 ausgegeben.

Die Zertifikatsseriennummer wird mit Hilfe eines kryptographisch sicheren Zufallsgenerators (CSPRNG) zufällig erzeugt und enthält eine Entropie von 128 bit.

#### 7.1.2 Zertifikatserweiterung

Die Wahl der Erweiterung ist weitestgehend produktabhängig.

CA-Zertifikate enthalten folgende *kritische* Erweiterungen („Pflichtfeld"):

| Erweiterung | OID | Parameter |
|---|---|---|
| *keyUsage* | 2.5.29.15 | *keyCertSign, cRLSign* |
| *basicConstraints* | 2.5.29.19 | *Ca=TRUE, (pathLenConstraint)* |

CA-Zertifikate können folgende *unkritische* Erweiterungen enthalten („optional"):

| Erweiterung | OID | Parameter |
|---|---|---|
| *extKeyUsage*[9,10] | 2.5.29.37 | Entsprechend [RFC 5280], [RFC 6818]<br>**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP:**<br>Für SubCA-Zertifikate wird die Erweiterung "extKeyUsage" gem. der untergeordneten EE-Zertifikatsprofile verwendet.<br>Die anyExtendedKeyUsage KeyPurposeId wird grundsätzlich nicht verwendet. |
| *authorityKeyIdentifier*[9] | 2.5.29.35 | 160-bit SHA-1 Hash des Ausstellerschlüssels |
| *subjectKeyIdentifier* | 2.5.29.14 | 160-bit SHA-1 Hash des Subject Public Key |

[9] Wird nicht in Root CA Zertifikaten verwendet.

[10] Wird ausschließlich verwendet bei QEVCP-w, QNCP-w, EVCP, OVCP und DVCP.

| Erweiterung | OID | Parameter |
|---|---|---|
| *cRLDistributionPoints* | 2.5.29.31 | Adresse(n) der CRL-Ausgabestelle(n) |
| *authorityInfoAccess*[9] | 1.3.6.1.5.5.7.1.1 | *accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation {…} accessMethod=caIssuers {1.3.6.1.5.5.7.48.2}, accessLocation {…}* |
| *certificatePolicies*[9] | 2.5.29.32 | OIDs der unterstützten CPs |
| *subjectAltName*[9] | 2.5.29.17 | Alternativer Inhabername |

Ergänzende Erweiterungen können aufgenommen werden, müssen [X.509], [RFC 5280], [RFC 6818], [ETSI EN 319 412] und [ETSI-ALG] entsprechen oder in einem referenzierten Dokument beschrieben sein.

EE-Zertifikate enthalten folgende *kritische* Erweiterungen:

| Erweiterung | OID | Parameter |
|---|---|---|
| *keyUsage* | 2.5.29.15 | Möglich sind:<br>*digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, decipherOnly*<br>und Kombinationen |

EE-Zertifikate können folgende unkritische Erweiterungen enthalten:

| Erweiterung | OID | Parameter |
|---|---|---|
| *extKeyUsage* | 2.5.29.37 | Entsprechend [RFC 5280], [RFC 6818][11]<br>**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP:**<br>nur "id-kp-serverAuth" und "id-kp-clientAuth" sind zulässig |
| *authorityKeyIdentifier* | 2.5.29.35 | 160-bit SHA-1 Hash des Ausstellerschlüssels |
| *subjectKeyIdentifier* | 2.5.29.14 | 160-bit SHA-1 Hash des Subject Public Key |
| *cRLDistributionPoints* | 2.5.29.31 | CRL-Ausgabestelle als ldap-Adresse |
| *authorityInfoAccess* | 1.3.6.1.5.5.7.1.1 | *accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation {…}*[12] *accessMethod= caIssuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}* |
| *certificatePolicies* | 2.5.29.32 | OIDs der unterstützten CPs<br>*cpsURI* |
| *subjectAltName* | 2.5.29.17 | Alternativer Inhabername<br><br>Wenn eine Emailadresse angegeben wird, muss diese als *RFC822Name* eingetragen werden. |

[11] Sonderfall im Rahmen des digitalen EU Impfnachweises davon abweichend.

[12] Wird der Status eines Zertifikats via Onlinestatusprotokoll (OCSP) bereitgestellt, so erfolgt dies über das http Protokoll.

| Erweiterung | OID | Parameter |
|---|---|---|
| *qcStatements* | *1.3.6.1.5.5.7.1.3* | QEVCP-w und QNCP-w:<br>esi4-qcStatement-1 {0 4 0 1862 1 1};<br>esi4-qcStatement-5 {0 4 0 1862 1 5};<br>esi4-qcStatement-6 {0 4 0 1862 1 6};<br>id-etsi-qct-web {0 4 0 1862 1 6 3};<br><br>QCP-l:<br>esi4-qcStatement-1 {0 4 0 1862 1 1};<br>esi4-qcStatement-5 {0 4 0 1862 1 5};<br>esi4-qcStatement-6 {0 4 0 1862 1 6};<br>id-etsi-qct-eseal {0 4 0 1862 1 6 2} ;<br><br>QCP-l-qscd:<br>esi4-qcStatement-1 {0 4 0 1862 1 1};<br>esi4-qcStatement-4 {0 4 0 1862 1 4};<br>esi4-qcStatement-5 {0 4 0 1862 1 5};<br>esi4-qcStatement-6 {0 4 0 1862 1 6};<br>id-etsi-qct-eseal {0 4 0 1862 1 6 2} ;<br><br>QCP-n-qscd:<br>esi4-qcStatement-1 {0 4 0 1862 1 1};<br>esi4-qcStatement-2 {0 4 0 1862 1 2};<br>esi4-qcStatement-4 {0 4 0 1862 1 4};<br>esi4-qcStatement-5 {0 4 0 1862 1 5};<br>esi4-qcStatement-6 {0 4 0 1862 1 6};<br>id-etsi-qct-esign {0 4 0 1862 1 6 1} ;<br><br>BTSP:<br>esi4-qtstStatement-1 {0 4 0 19422 1 1};<br><br>Bei Zertifikaten mit der Ausprägung PSD2 bei QEVCP-w, QNCP-w und QCP-l gilt zusätzlich:<br>etsi-psd2-qcStatement {0 4 0 19495 2}<br><br>mit<br>PSD2QcType ::= SEQUENCE {<br>rolesOfPSP<br>nCAName<br>nCAId } <br>Die Validierung der PSD2 spezifischen Attribute ist in Abschnitt 4.2.1 beschrieben. |

Ergänzende Erweiterungen können aufgenommen werden, müssen [X.509], [RFC 5280], [RFC 6818], [ETSI EN 319 412] und [ETSI-ALG] entsprechen oder in einem referenzierten Dokument beschrieben sein.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

**QEVCP-w, EVCP,OVCP, DVCP**

Ein Vorzertifikat (Precertificate), wie in RFC 6962 beschrieben, wird nicht als "Zertifikat" im eigentlichen Sinne betrachtet, welches den Anforderungen von RFC 5280 entspricht.

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

Die Liste der QSCDs in Deutschland wird auf der Webseite der BNetzA öffentlich zugänglich bereitgestellt. D-Trust monitort den QSCD-Zertifizierungsstatus, der von ihr verwendeten QSCDs. Sollte der QSCD-Zertifizierungsstatus der eingesetzten QSCDs kürzer sein als die

regulären Zertifikatslaufzeiten werden Kunden vorab informiert und die Zertifikate werden ab dem kritischen Zeitpunkt mit verkürzter Zertifikatslaufzeit ausgestellt.

Sollte jedoch irrtümlich ein Zertifikat auf einer QSCD mit einer Zertifikatslaufzeit ausgestellt werden, das über den gültigen QSCD-Zertifizierungsstatus hinaus gilt, wird das Subject/ der Subscriber vorab informiert und das Zertifikat wird spätestens zum Ablaufdatum des QSCD gesperrt.

Wenn dem TSP Änderungen bekannt werden, die die Gültigkeit des Zertifikats beeinträchtigen, weil z.B. die Aufsichtsstelle den QSCD-Zertifizierungsstatus entzogen hat, werden alle betroffenen Zertifikate, bei denen das „esi4-qcStatement-4" gemäß ETSI EN 319 412-5 gesetzt ist und die von dieser Änderung des betroffenen QSCD-Zertifizierungsstatus betroffen sind, gesperrt. Die betroffenen Subjects und ggf. Subscriber werden darüber unterrichtet.

**QCP-l für den digitalen EU Impfnachweis**
Siegelzertifikate, die im Rahmen des digitalen EU Impfnachweises eingesetzt werden, können im Feld extendedKeyUsage (extKeyUsage) folgende OID-Einträge erhalten:

- OID 1.3.6.1.4.1.0.1847.2021.1.1 for Test Issuers
- OID 1.3.6.1.4.1.0.1847.2021.1.2 for Vacination Issuers
- OID 1.3.6.1.4.1.0.1847.2021.1.3 for Recovery Issuers

### 7.1.3 Algorithmen-OIDs

SHA1 wird nicht verwendet.

Die spezifischen Regelungen sind im jeweiligen CPS dokumentiert.

### 7.1.4 Namensformate

In den Feldern *subject* (hier: Name des Endanwenders) und *issuer* (Name des Ausstellers) werden Namen nach [X.500] bzw. [X.509] als DistinguishedName vergeben. Es können die Attribute aus Abschnitt 3.1.4 vergeben werden. Die Kodierung erfolgt als UTF8-String bzw. PrintableString für das Attribut C (Country).

In den Feldern *SubjectAltName* (Alternativer Zertifikatsnehmername) und *Issuer-AltName* (Alternativer Ausstellername) können Namen gemäß [RFC 5280], [RFC 6818] (kodiert als IA5String) stehen.

**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP**
Die Vorgaben aus Abschnitt 7.1.4 [BRG] werden erfüllt.

**QEVCP-w, EVCP**
Es gelten die Vorgaben aus Abschnitt 9.2 [EVGL] und haben Vorrang zu den Vorgaben aus Abschnitt 7.1.4 [BRG].

### 7.1.5 Name Constraints

„NameConstraints" wird nicht benutzt.

### 7.1.6 Certificate Policy Object Identifier

„CertificatePolicies" kann die OIDs unterstützter CPs enthalten.

Weitere Regelungen sind in der CP in Abschnitt 1.1.3 dokumentiert.

### 7.1.7 Nutzung der Erweiterung "PolicyConstraints"

„PolicyConstraints" wird nicht benutzt.

### 7.1.8 Syntax und Semantik von "Policy Qualifiern"

„PolicyQualifier" können benutzt werden.

### 7.1.9 Verarbeitung der Semantik der kritischen Erweiterungen CertificatePolicies

In Dienste-, CA- und EE-Zertifikaten ist die Erweiterung *CertificatePolicies* (Zertifikatsrichtlinie) nicht kritisch. Es liegt im Ermessen der Zertifikatsnehmer und Zertifikatsnutzer, diese Erweiterung auszuwerten.

## 7.2 Sperrlistenprofile

Die Differenz zwischen dem nextUpdate-Feld und dem thisUpdate-Feld überschreitet nicht zehn Tage.

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

**CA-Zertifikate**

D-Trust gibt für gesperrte CA-Zertifikate im reasonCode Eintrag in der CRL den Sperrgrund wieder. Sollte ein Eintrag erforderlich werden, verwendet D-Trust einen der folgenden CRLReason gemäß RFC 5280, Kapitel 5.3.1, der dem Sperrgrund am besten entspricht:

- keyCompromise (1),
- cACompromise (2),
- affiliationChanged (3),
- superseded (4) oder
- cessationOfOperation (5).

**Subscriber-Zertifikate**

Der Subscriber muss einen Sperrgrund auswählen. Wählt er unspecified (0) aus, so bleibt der reasonCode Eintrag in der CRL leer. D-Trust verwendet einen der folgenden CRLReason gemäß RFC 5280, Kapitel 5.3.1:

- unspecified (0)
- keyCompromise (1),
- affiliationChanged (3),
- superseded (4) oder
- cessationOfOperation (5)

Folgender Sperrgrund wird vom TSP nachträglich als CRLReason eingetragen, wenn der Subscriber gegen die vereinbarten Terms and Conditions verstößt:

- privilegeWithdrawn (9).

Wenn nachweislich eine Schlüsselkompromittierung stattgefunden hat, diese aber im CRLReason vom Subscriber nicht korrekt dokumetiert wurde, setzt der TSP diesen Wert nachträglich auf „keyCompromise". Wenn der TSP festgestellt, dass der private Schlüssel des Zertifikats vor dem Sperrdatum, das im CRL-Eintrag für dieses Zertifikat angegeben ist, kompromittiert wurde, korrigiert der TSP nachträglich das Sperrdatum. Diese Rückdatierung ist eine Ausnahme und findet in der Regel keine Anwendung.

### 7.2.1 Versionsnummer(n)

Es werden Sperrlisten v2 gemäß [RFC 5280], [RFC 6818] erstellt. Delta-CRLs sind nicht vorgesehen.

### 7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

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

Sperrlisten können folgende unkritische Erweiterungen enthalten:

| Erweiterung | OID | Parameter |
|---|---|---|
| *cRLNumber* | 2.5.29.20 | Nummer der Sperrliste |
| *authorityKeyIdentifier* | 2.5.29.35 | 160-bit SHA-1 Hash des Ausstellerschlüssels |
| *expiredCertsOnCRL* | 2.5.29.60 | Die Erweiterung wird nur für **QCP-n-qscd, QCP-l-qscd, QCP-l, QEVCP-w, QNCP-w** verwendet. |
| *reasonCode* | 2.5.29.21 | Wenn dieses Feld vorhanden ist, dann wird ein CRLReason gemäß Kapitel 7.2 verwendet. |

## 7.3 Profile des Statusabfragedienstes (OCSP)

Der OCSP-Responder unterstützt zusätzlich zu RFC 6960 auch Positivauskünfte. („Zertifikat ist authentisch und gültig").

Der OCSP-Responder liefert folgende Antworten:

- „good"[13], wenn der Responder das Zertifikat als gültig erkennt,
- „unknown"[14], wenn der Responder den Status des Zertifikats nicht ermitteln kann und
- „revoked", wenn der Responder das Zertifikat als widerrufen erkennt.

Ist das Feld „nextUpdate" nicht gesetzt, dann zeigt der OCSP-Responder gemäß Kapitel 4.2.2.1 des RFC 6960 an, dass immer die neusten Sperrinformationen verfügbar sind.

**QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP**
Das Feld „nextUpdate" ist gesetzt. Die Differenz zwischen dem nextUpdate-Feld und dem thisUpdate-Feld überschreitet nicht 24 Stunden.

Erfolgt die OCSP-Auskunft für ein gesperrtes CA-Zertifikat, dann enthält diese den Eintrag revocationReason innerhalb der RevokedInfo des CertStatus gemäß RFC 6960. Der Inhalt des Eintrags richtet sich nach den Vorgaben aus Abschnitt 7.2.

Zertifikate werden mindestens bis zum Ablauf der Zertifikatsgültigkeit beauskunftet.

### 7.3.1 Versionsnummer(n)

Es wird OCSP v1 gemäß [RFC 6960] eingesetzt.

### 7.3.2 OCSP-Erweiterungen

Der OCSP-Responder unterstützt bei Anfragen die im Folgenden angegebene Erweiterung (Extension):

| Erweiterung | Parameter |
|---|---|
| *retrieveIfAllowed* | Falls gesetzt, wird Zertifikat in der Antwort mitgeliefert (optional). |

[13] Ist ein Zertifikat nicht ausgestellt, gibt der OCSP Responder"unknown" als Statusinformation zurück.

[14] Der OCSP-Responder überwacht die als „unknown" geprüften Anfragen nicht. Diese werden aktuell verworfen.

Der OCSP-Responder verwendet in den Antworten die im Folgenden angegebenen Erweiterungen (Extensions):

| Erweiterung | Parameter |
|---|---|
| *archiveCutOff* | Zeitraum, für den der OCSP-Responder nach Ausstellung des Zertifikats die Statusinformationen bereitstellt. |
| *certHash* | Bei Status good oder revoked wird der SHA-1 Hash-Wert des Zertifikats eingetragen. |
| *certInDirSince* | Zeitpunkt der Veröffentlichung des Zertifikats im zentralen Verzeichnisdienst. |
| *requestedCertificate* | Enthält das Zertifikat, falls *RetrieveIfAllowed* gesetzt war. |

Alle Erweiterungen sind nicht kritisch. Weitere unkritische Erweiterungen können enthalten sein.

## 8. Überprüfungen und andere Bewertungen

Revisionen, Revisionsgegenstände und Prozesse sind detailliert in der Dokumentation der D-Trust GmbH beschrieben. Das Rollenkonzept dokumentiert die Qualifikation und die Stellung des Revisors.

Die Dokumentation sowie die operativen Verfahren des TSP werden wiederkehrend durch jährliche Audits konsekutiv über den gesamten Zeitraum durch eine unabhängige Konformitätsbewertungsstelle geprüft.

Bei begründetem Interesse können diese Dokumente in den relevanten Teilen eingesehen werden.

CP, TSPS und CPS erfüllen für Zertifikate die Anforderungen

- für Produkte innerhalb der **Root CPS und CSM CPS:** gemäß [EN 319 411-1] bzw. [EN 319 411-2] bzw. BSI [TR-03145-1] einschließlich der Anforderungen aus [BRG] und [NetSec-CAB],
- für Produkte innerhalb des **Cloud CPS:** gemäß [EN 319 421], [EN 319 411-1] bzw. [EN 319 411-2] einschließlich der Anforderungen aus [BRG] und [NetSec-CAB].

Ein regelmäßiges Assessment durch einen qualifizierten und unabhängigen Dritten („competent independent party" belegt die Kompatibilität:

- für Produkte innerhalb der Root CPS und CSM CPS: gemäß [EN 319 411-1] bzw. [EN 319 411-2], welche normative Verweise auf [EN 319 401] enthalten,
- für Produkte innerhalb des Cloud CPS: gemäß [EN 319 421], [EN 319 411-1] bzw. [EN 319 411-2], welche normative Verweise auf [EN 319 401] enthalten.

Der TSP gibt Zertifikate mit einer Policy-OID-Referenz auf die oben spezifizierten Standards der jeweiligen CPS, erst nach der erfolgreich abgeschlossenen Prüfung durch eine unabhängige externe Konformitätsbewertungsstelle, aus. Es finden regelmäßige Überwachungsprüfungen statt. Sollten sich die Verfahren als nicht mehr konform zu den aktuellen Richtlinien von den oben spezifizierten Standards der jeweiligen CPS erweisen, unterlässt der TSP das Ausstellen o. g. Zertifikate bis die Richtlinienkonformität wiederhergestellt und entsprechend überprüft wurde. Diese Auditierung findet jährlich statt. Kritische Änderungen werden unterjährig ebenfalls von der Konformitätsbewertungsstelle geprüft und freigegeben.

Darüber hinaus finden regelmäßig interne Audits statt. Im Rahmen von „Self Audits" werden zur Qualitätssicherung vierteljährlich zufällig ausgewählte Stichproben von mindestens drei Prozent der Zertifikate (jedoch mindestens ein Zertifikat), die die D-Trust in dem Zeitraum gem. den Anforderungen des [BRG] und [EVGL] ausgestellt hat, geprüft und intern dokumentiert.

**EVCP, OVCP, DVCP**

Im Falle von Unstimmigkeiten in Bezug auf das geltenden nationale Recht und die [BRG] und [EVGL] wird die D-Trust das CA/Browser-Forum über die Tatsache, die Umstände und das geltende nationale Recht informieren.

## 9. Sonstige finanzielle und rechtliche Regelungen

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