Certification Practice Statement of the D-TRUST CSM PKI

ENGLISH

DEUTSCH

BUNDESDRUCKEREI

Certification Practice Statement of the D-TRUST CSM PKI

Version 2.3

D-TRUST
REGISTERED TRADE MARK OF BUNDESDRUCKEREI

COPYRIGHT NOTICE AND USE LICENSE

Certification Practice Statement of the D-TRUST CSM PKI
©2018 D-TRUST GmbH

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

Requests for any other use of this CPS of D-TRUST GmbH not contained in the aforementioned license are to be sent to:

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

Document history

Version	Date	Description
1.0	09/02/2015	▪ Initial version
1.1	23/02/2015	▪ Editorial changes during first-time certification according to ETSI 102 042 LCP. Several contents of the CP of D-TRUST GmbH were incorporated in the CPS.
1.2	05/10/2015	▪ Editorial changes ▪ More detailed information regarding the option to have the key material generated and delivered by the TSP ▪ Revocation now only via the online interface and by phone when a revocation password was agreed to. ▪ All new certificates are always published in the D-TRUST LDAP.
1.3	03/10/2016	▪ Change to EN 319 411-1
2.0	01/01/2017	▪ Introduction of qualified SSL/TLS certificates (QWACs) according to EN 319 411-2 and eIDAS
2.1	01/10/2017	▪ Editorial changes along with more specific details in section 6.5
2.2	28/03/2018	▪ Editorial changes and improving of the adaption with RFC 3647 ▪ Adaptation of the use license to “Creative Commons Attribution” ▪ Adaption with Mozilla Root Store Policy 2.5
2.3	05.07.2018	▪ Section 4.2.1: Domain validation methods changed ▪ Field OrgID in section 3.1.4 supplemented according to variant 3 in section 5.1.4 of EN 319 412-1 ▪ Editorial changes

Contents

1. Introduction 6
1.1 Overview 6
1.2 Document Name and Identification 8
1.3 PKI Participants 8
1.4 Certificate Usage 9
1.5 Policy Administration 10
1.6 Definitions and Acronyms 11
2. Publication and Repository Responsibilities 12
2.1 Repositories 12
2.2 Publication of information concerning certificates 12
2.3 Publication frequency 12
2.4 Directory access control 13
3. Identification and Authentication (I&A) 14
3.1 Naming 14
3.2 Initial Identity Validation 17
3.3 I&A for Re-key Requests 19
3.4 I&A for Revocation Requests 19
4. Certificate Life-Cycle Operational Requirements 21
4.1 Certificate Application 21
4.2 Certificate Application Processing 21
4.3 Certificate Issuance 25
4.4 Certificate Acceptance 25
4.5 Key Pair and Certificate Usage 26
4.6 Certificate Renewal 26
4.7 Certificate Re-key 27
4.8 Certificate Modification 28
4.9 Certificate Revocation and Suspension 28
4.10 Certificate Status Services 31
4.11 End of Subscription 31
4.12 Key Escrow and Recovery 31
5. Facility, Management, and Operational Controls 32
5.1 Physical Security Controls 32
5.2 Procedural Controls 32
5.3 Personnel Controls 33
5.4 Audit Logging Procedures 34
5.5 Records Archival 34
5.6 Key Changeover 35
5.7 Compromise and Disaster Recovery 35
5.8 CA or RA Termination 36
6. Technical Security Controls 37
6.1 Key Pair Generation and Installation 37
6.2 Private Key Protection and Cryptographic Module Engineering Controls 38
6.3 Other Aspects of Key Pair Management 39
6.4 Activation Data 40
6.5 Computer Security Controls 40
6.6 Life Cycle Security Controls 41
6.7 Network Security Controls 42
6.8 Timestamping 42
7. Certificate, CRL, and OCSP Profiles 43
7.1 Certificate Profile 43
7.2 CRL Profile 45
7.3 OCSP Profile 46

8. Compliance Audit and Other Assessment 47
9. Other Business and Legal Matters 48

1. Introduction

1.1 Overview

This document is the Certification Practice Statement (CPS) of the trust services operated by D-TRUST GmbH that are provided via the Certificate Service Manager (CSM).

1.1.1 Trust service provider

These rules are laid down in the CP.

1.1.2 About this document

This CPS defines processes and procedures within the scope of the trust services throughout the entire life of the CA and end-entity certificates (EE certificates). It determines the minimum measures that all PKI entities must fulfil.

This CPS refers to the CP (certificate policy) of D-TRUST GmbH with OID 1.3.6.1.4.1.4788.2.200.1 and to [EN 319 411-1] or [EN 319 411-2], respectively and describes the implementation of the resultant requirements.

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

The complete CPS has a legally binding effect in as far as this is permitted under German and/or European law. It contains provisions regarding obligations, warranty and liability for the PKI entities. Unless expressly stated, no warranties or guarantees in a legal sense are given on the basis of this CPS.

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

The structure of this document is closely related to the RFC 3647 Internet standard "*Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*", making it easier to read and comparable with other CPSs.

1.1.3 Properties of the PKI

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

PKI for qualified trust services

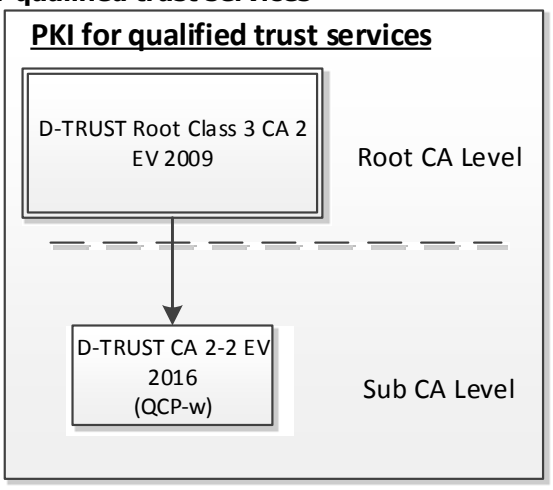

Fig. 1 PKI hierarchy for qualified trust services

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

QCP-w – Qualified website certificates (QWACs)

QCP-w

EE certificates of the certification level QCP-w are qualified SSL/TLS certificates according to [EN 319 411-2]. EV certificates are not issued on smart cards. Qualified website certificates always meet the requirements for SSL/TLS certificates pursuant to certification level EVCP according to [EN 319 411-1] which can be identified by the EV Policy OID in the EE certificates.

PKI for non-qualified trust services

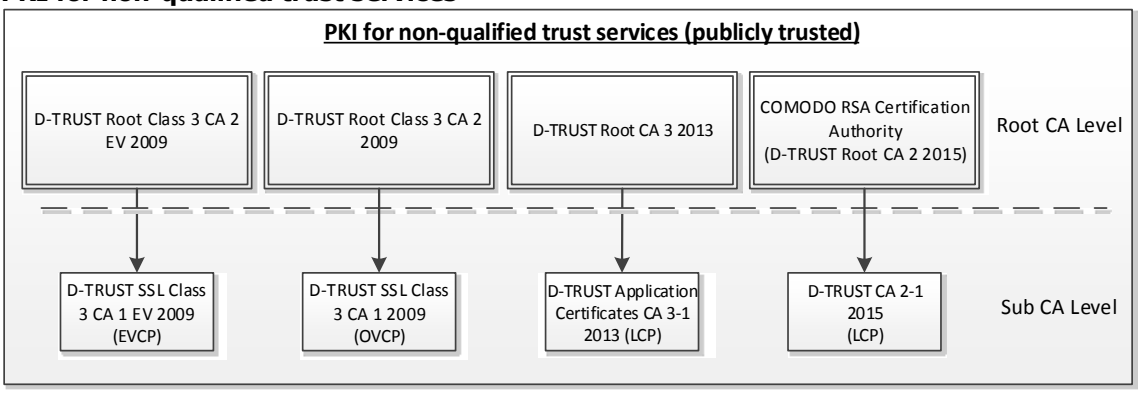

Fig. 2 PKI hierarchy for non-qualified trust services

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

LCP – Lightweight Certificate Policy

NCP – Normalized Certificate Policy

OVCP – Organization Validated Certificate Policy

EVCP – Extended Validation Certificate Policy

Although corresponding policy levels (such as EVCP+) which require a secure signature creation device (SSCD) to be used are currently not offered, subscribers are free to use an SSCD to create and store their private keys.

EVCP

EE certificates of the EV policy level are SSL/TLS certificates. The fact that they are EV certificates can be recognised in the EE certificates by the EV policy OID. EV certificates are not issued on smart cards.

OVCP

EE certificates of the OV policy level include SSL/TLS certificates and machine certificates which include the name of an organization. OV certificates are not issued on smart cards.

NCP

NCP certificates are currently not offered and will therefore not be described further in the following.

LCP

EE certificates of the LC policy level are simple personal certificates. In this case too, the name of an organization can be included as an attribute in the certificate. LCP certificates are not issued on smart cards.

1.2 Document Name and Identification

Document name:	Certification Practice Statement of the D-TRUST CSM PKI
Version	2.3

1.3 PKI Participants

1.3.1 Certification authorities (CAs)

Certification authorities (CAs) are operated by the trust service provider and issue certificates and revocation lists. The following types of certificates are possible:

- Personal certificates for individuals (EE certificate)
- Seal certificates for legal entities (EE certificate)
- Group certificates for groups of individuals, functions and IT processes (EE certificate)
- Machine certificates for IT processes and communication connections (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.

LCP

The issuing SubCA can be cross-signed by another root CA. All definitions from this CPS are also valid here.

1.3.2 Registration authorities (RAs)

The RA identifies and authenticates subscribers or subjects, and it collects and checks applications for different certification services.

The concrete tasks and obligations of the RA as 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 which are not operated by D-TRUST are currently only used for identification within the framework of certification level LCP.

1.3.3 Subscribers and end-entities (EEs)

Subscribers are individuals 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.

Subjects (end-entities (EEs)) use the private end-entity keys (EE keys). The subject's identity is linked to the certificate and the related key pair. The end-entity can be identical to the subscriber. Valid end-entities are:

- Individuals
- Legal entities
- Groups of individuals or teams
- Functions which are performed by staff of an organization
- IT processes (such as SSL server)

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 passes it on to the subscriber. Moreover, additional obligations exist under [EN 319 411-1] and [EN 319 411-2]. At the time of submitting the application at the latest, subscribers receive this CPS and the subscriber agreement as information about these obligations which they are obliged to adhere to. In the case of SSL certificates, the subscriber agreement for SSL certificates applies. The general subscriber agreement applies to all other certificates under this policy.

EVCP, OVCP, LCP

In the event that the subscriber and end-entity are not identical and the end-entity is an individual, the subscriber is responsible for ensuring that the end-entity complies with the obligations.

QCP-w, EVCP, OVCP

SSL/TLS certificates are issued exclusively to legal entities.

1.3.4 Relying parties

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

1.4 Certificate Usage

1.4.1 Permitted uses of certificates

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 which are compatible with the types of use shown in the certificate.

Relying parties are solely responsible for their acts. Certificate users are responsible for judging whether this CPS meets with the requirements of an application and whether the 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 uses of certificates

Types of use not laid down in the certificate are not permitted. The rules of the CP of D-TRUST GmbH also apply.

1.4.3 Use of service certificates

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 revocation information[1]

1.5 Policy Administration

1.5.1 Responsibility for the document

This CPS is maintained and updated by D-TRUST GmbH. The representative of management is responsible for acceptance of the document.

This CPS is checked and updated annually by the TSP. A change is indicated by a new version number of this document.

1.5.2 Contact partner/contact person/secretariat

These rules are laid down 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 CPS. The reference of a policy OID in the certificate extensions serves as the 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]).

QCP-w, EVCP

SSL/TLS certificates or their sub-CAs and root CAs comply with the requirements of the CA/Browser Forum's Guidelines for Extended Validation Certificates [GL-BRO] as well as with [EN 319 411-1] and [EN 319 411-2]. In the event of inconsistencies between this document and the guidelines above, [GL-BRO] and [EN 319 411-1] as well as [EN 319 411-2] have priority.

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

1.6 Definitions and Acronyms

1.6.1 Terms and names

These rules are laid down in the CP.

1.6.2 Abbreviations

These rules are laid down in the CP.

1.6.3 References

These rules are laid down in the CP.

2. Publication and Repository Responsibilities

2.1 Repositories

These rules are laid down in the CP.

2.2 Publication of information concerning certificates

The TSP publishes the following information:

- EE certificates
- CA certificates
- Certificate revocation lists (CRLs) and status information
- The CP
- This CPS
- The subscriber agreement for SSL/TLS certificates
- The subscriber agreement for all other certificates under this policy (general subscriber agreement).
- Cross certificates
- PKI user information for qualified trust services

2.3 Publication frequency

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

QCP-w

Published EE Certificates will remain available until the end of their validity term plus at least ten years and until the end of the year.

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

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

Certificate revocation lists are issued regularly and until the end of validity of the issuing CA certificate. Certificate revocation lists are issued and published immediately following revocations. Even if no certificates were revoked, the TSP ensures that a new certificate revocation list is created at least every 24 hours. The certificate revocation lists are retained and kept for a minimum period of one year following expiration of the validity of the CA.

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

This CPS is published and remains available for retrieval as long as the certificates that were issued on the basis of this CPS remain valid. The websites of the TSP have high availability.

2.4 Directory access control

Certificates, certificate revocation lists and this CPS can be publicly retrieved at no cost. Read 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 issued on request against proof of a legitimate interest.

3. Identification and Authentication (I&A)

3.1 Naming

3.1.1 Types of names

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

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

3.1.2 Need for telling names

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

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

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

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

3.1.3 Anonymity or pseudonyms of subscribers

Pseudonyms are used exclusively for individuals. Pseudonyms are generally assigned by the TSP.

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

3.1.4 Rules for the interpretation of different name forms

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

DN component	Interpretation
G (given name)	*Given name(s)* of the individual QCP-w, EVCP, OVCP: This field is not used. LCP: according to the proof used for identification
SN (surname)	*Surname* of the individual QCP-w, EVCP, OVCP: This field is not used. LCP: according to the proof used for identification If pseudonyms are used, SN corresponds to CN.

CN (common name)	*Common name:* The following variants are used: Individuals without a pseudonym: "family name, name used". Individuals with a pseudonym: "Pseudonym:PN". Legal entities: official name of the organization (company, public authority, association, etc.), if necessary, reduced to a meaningful name if the maximum number of 64 characters is exceeded. Special case: It is also possible to include one or more domain names in the CN. QCP-w, EVCP: Wildcards are not permitted for SSL/TLS certificates. Function or group of individuals: Name of the function or group of individuals preceded by the abbreviation "GRP:" in order to indicate that this is a group certificate Technical components: Name of the server, service or application using the certificate
PN	*Pseudonym*: identical to CN.
serialNumber	*Serial number*: Name suffix number to ensure unambiguity of the name (typically the application number). Special case for EV certificates according to [GL-BRO]: Register number if assigned, date of registration or establishment. Other product-specific uses of the field are possible.
O (organization)	Official name of the subscriber or name of the *organization* to which the end-entity belongs or to which he or she is connected (company, public authority, association, etc.) according to the proof of existence; if necessary, reduced to a meaningful name if the maximum number of 64 characters is exceeded.
OU (organization unit)	*Organization unit* (department, division or other unit) of the organization.
OrgID (organization identifier)	QCP-w: *Unambiguous organization number* of the organization. The number of the commercial register as well as the VAT ID number or a number assigned by D-TRUST can be entered. The number assigned by D-TRUST is based on variant 3 in section 5.1.4 of EN 319 412-1 and is composed as follows: DT: DE-1234567890 (DT: D-TRUST; DE: Germany; random number that is unambiguously assigned to the organization).
C (country)	The notation of the country to be stated corresponds to [ISO 3166] and is set up as follows: If an organization O is listed in the DistinguishedName, the organization's place of business in the register determines the entry in the certificate. If no organization O is entered, the country is listed that issued the document that was used to identify the subscriber.
Street	Postal address *Street*

Locality	Postal address *City*
State	Postal address *(Federal) state*
PostalCode	Postal address *Postal code*
BusinessCategory	Business category (2.5.4.15) according to [GL-BRO]
Jurisdiction Of Incorporation Locality	Jurisdiction of the organization according to [GL-BRO]: *City* (1.3.6.1.4.1.311.60.2.1.1)
Jurisdiction Of Incorporation State Or Province Name	Jurisdiction of the organization: *(Federal) state* (1.3.6.1.4.1.311.60.2.1.2)
Jurisdiction Of Incorporation CountryName	Jurisdiction of the organization according to [GL-BRO]: *Country* (1.3.6.1.4.1.311.60.2.1.3)

QCP-w, EVCP

SSL/TLS certificates include, as a minimum, the subject DN components: "Organization", "CommonName", "subjectAlternativName", "BusinessCategory", "Jurisdiction of Incorporation or Registration", "subjectSerialNumber", "Locality", "State" as well as "Country", "StreetAddress" and "Postal Code".

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

3.1.5 Unambiguity of names

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

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

3.1.6 Recognition, authentication and the role of brand names

The subscriber is liable for compliance with intellectual property rights in the application and certificate data (see Certificate Policy of D-TRUST GmbH, section 9.5).

QCP-w, EVCP

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

3.2 Initial Identity Validation

3.2.1 Proof of ownership of the private key

Two cases are distinguished:

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

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

3.2.2 Identification and authentication of organizations

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

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

On the different certification levels, the verification procedures described are applied as follows to the DN components according to section 3.1.4 plus further attributes, if necessary and applicable. The procedures shown in the table below are described in section 4.2.1.

<table>
<tr><th></th><th>QCP-w, EVCP</th><th>OVCP</th></tr>
<tr><td>CN</td><td>Register/
Non-Register/

Domain/
CAA</td><td>Register/
Non-Register/

Domain/
CAA</td></tr>
<tr><td>C</td><td rowspan="2">Register/
Non-Register/

Domain</td><td rowspan="2">Register/
Non-Register/

Domain</td></tr>
<tr><td>O</td></tr>
<tr><td>OU</td><td>C confirmation/
A confirmation</td><td>C confirmation/
A confirmation</td></tr>
<tr><td>STREET</td><td rowspan="4">Register/
Non-Register</td><td rowspan="4">Register/
Non-Register</td></tr>
<tr><td>L</td></tr>
<tr><td>State</td></tr>
<tr><td>PostalCode</td></tr>
<tr><td>Alternative applicant (SAN)</td><td>Domain/
CAA</td><td>Domain/
CAA</td></tr>
<tr><td>All other attributes</td><td>C confirmation/
A confirmation/ Dok-Ident/
out-of-band mechanisms/
Register/
Non-Register</td><td>A confirmation/ Dok-Ident/
out-of-band mechanisms</td></tr>
</table>

If the application is submitted on behalf of a legal entity, the representative must (in analogy to the procedure for proving affiliation with the organization according to section 3.2.3) prove his or her authorization to this effect and also furnish proof of his or her identity.

Documents in non-Latin characters are not accepted.

3.2.3 Identification and authentication of individuals

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

LCP

Subscribers applying for certificates for other individuals must furnish proof of their authority to submit such applications. The subscriber's data is verified.

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

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

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

Documents in non-Latin characters are not accepted.

3.2.4 Non-verified information concerning the subscriber

Verification of the subscriber's information is carried out or skipped according to sections 3.2.2, 3.2.3 and 4.2.1. In the case of alternative names, only the e-mail addresses or their domain components are generally verified. Other certificate contents, e.g. LDAP directories, etc. as well

as certificate extensions (AdditionalInformation, monetaryLimit, etc.), if any, are not checked for correctness.

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

3.2.5 Verification of authority to apply

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

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

3.2.6 Criteria for interoperability

See section 1.5.3.

3.3 I&A for Re-key Requests

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

3.3.1 Routine re-keying applications

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

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

3.3.2 Re-keying after revocation

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

3.4 I&A for Revocation Requests

Revocation authorization is verified as follows:

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

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

LCP

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

Revocation procedures are defined in section 4.9.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Application authorization

Applications can only be submitted by individuals and legal entities (or their authorized representatives).

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

QCP-w, EVCP

Subscribers must fulfil the requirements of [GL-BRO].

CA certificates are exclusively issued to legal entities.

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

4.1.2 Registration process and responsibilities

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

QCP-w, EVCP

Prior to completing the registration process, the subscriber receives the CP and CPS as well as 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]. Proof is kept electronically or in printed form. The subscriber agreement corresponds to the requirements of [GL-BRO].

LCP

The subscriber receives the 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 or not. If the subscriber is not the subject, the subscriber must prove that the obligations under this document and the subscriber agreement have been transferred to the subject.

4.2 Certificate Application Processing

4.2.1 Identification and authentication procedure

The identification and registration process described herein must be completely carried out and all necessary proofs must be provided.

Individuals 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.

Individuals must be unambiguously identified. In addition to the full name, further attributes (such as place and date of birth or other applicable individual parameters) must be used to prevent individuals 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 relevant register information must be verified.

Identification is carried out according to section 3.2.3.

The TSP defines the following verification methods:

Pers-Ident
Using a valid ID document, the individual must prove his or her identity in person before an RA or an authorized identification partner (e.g. PostIdent service provided by Deutsche Post AG or Identity Trust Management AG) who fulfils the requirements of 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. Documents used as proof are filed. It can be agreed that documents used as proof are to be filed by the RA.

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 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. It can be agreed that documents used as proof are to be filed by the RA.

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 (registration courts, German Federal Central Tax Office, professional associations under public law or equivalent organizations) or registers organized under private law (DUNS, 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. Documents used as proof are filed. It can be agreed that documents used as proof are to be filed by the RA.

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

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 CPS. An authorized employee or representative of an organization forwards extracts from the organization's human resource 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 subject about the latter's obligations under the subscriber agreement as well as possible revocation options, if applicable. 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 representative", 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.

It can be agreed that documents used as proof are to be filed by the RA.

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 accepted in individual cases. The authorization to sign must become apparent either from the proof of existence of the organization, or it must be proven in another suitable manner. The authorized signatory can appoint a deputy in writing (see "A confirmation"). Documents used as proof are filed. It can be agreed that documents used as proof are to be filed by the RA.

A confirmation
Authorized employees or representatives 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 accepted in individual cases. Documents used as proof are filed. It can be agreed that documents used as proof are to be filed by the RA.

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 individuals can, for instance, be provided to the TSP in the form of bank transfer, direct debit or payment by credit card. The TSP trusts the bank whose customer the organization and/or individual is. Verification by telephone by the TSP via a public telephone directory is also permitted.

In order to identify individuals, the TSP can send a letter "by registered mail with acknowledgement of receipt" to the subscriber, with the signature on the receipt being compared to the signature on the stored proof documents or in the application documents.

The subject's affiliation with an organization can also be verified by way of a verification letter "by registered mail with acknowledgement of receipt" to the organization to the attention of the subject. 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.

It can be agreed that documents used as proof are to be filed by the RA.

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 CPS. An authorized employee or representative 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 corresponding to HR-DB apply. It can be agreed that documents used as proof are to be filed by the RA.

Domain
With a view to the right to use the domain and the control thereof, an organization is validated using the following methods.

QCP-w, EVCP, OVCP, LCP
According to [BRG version 1.5.7] section 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact as well as [BRG version 1.5.7] section 3.2.2.4.4 Constructed Email to Domain Contact and [BRG version 1.5.7] section 3.2.2.4.6 Agreed-Upon Change to Website.

The following domain validation methods can be used until 31 July 2018:
according to [BRG version 1.5.4] 3.2.2.4.5 Domain Authorization Document and [BRG version 1.5.4] section 3.2.2.4.1 Validating the Applicant as a Domain Contact.

QCP-w, EVCP
In the case of SSL/TLS certificates, the domain name is additionally checked against blacklists of known phishing domains and other blacklists. Domain names not subject to a registration obligation as well as top-level domains are not permitted.

The results of the enquiry are filed.

CAA
CAA stands for Certification Authority Authorization. With this Resource Record (according to RFC6844), it is defined which CA is authorized to issue SSL certificates for that domain.

When it receives the application and immediately before activating the certificate, D-TRUST checks the domains named with a view to a corresponding CAA entry. Validated domains can be used for certificate generation if the CAA entry is empty or if D-TRUST has been entered by the domain holder as the CA.

Valid values are dtrust.de, d-trust.de, dtrust.net, d-trust.net, D-Trust Gmbh as well as D-Trust.

D-TRUST cannot issue TLS certificates if a different CA is stated in the CAA Resource Record.

E-mail
It must be possible to unambiguously assign the domain used in a registered e-mail address to the registered organization.

If this is not the case, the TSP sends an e-mail to the e-mail address to be confirmed, and receipt of this e-mail must be confirmed (exchange of secrets). The results of the enquiry are filed.

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

4.2.2 Acceptance or rejection of certificate applications

In the event that any inconsistency occurs during identity verification by the RA or the TSP or during the check of the data in the certificate application or in the ID card and proof documents that cannot be fully resolved, the application will be rejected.

Agreement can be reached so that the TSP adapts certificate applications on the basis of the agreed attributes.

Other reasons for rejection include:

- Suspected violation of name rights of third parties;
- Non-adherence to deadlines for proof of data;
- Payment arrears of the applicant in relation to the TSP or

- Circumstances justifying suspicion that the issuance of a certificate could discredit the operator of the CA.

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 to ensure that they match the stored documents. Such check does not have to be carried out by the TSP if contractual agreements are in place with partners where commissioned, independent persons make the requests available to the TSP for production. 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.

4.2.3 Deadlines for processing certificate applications

Not applicable

4.3 Certificate Issuance

4.3.1 Procedure of the TSP for the issuance of certificates

The corresponding certificates are produced in the high-security area of the trust service provider.

Use of the correct time during certificate production is ensured.

The TSP either files the complete application documentation in accordance with section 5.5 in an auditable manner, or the TSP concludes agreements with partners pursuant to which the application documents and/or requests have to be filed in a safe manner and completely until the expiration of the period according to section 5.5.2.

EVCP, OCP-w, OVCP

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

4.3.2 Notification of the subscriber that the certificate was issued

The subscriber does not receive separate notification of completion of the certificate.

4.4 Certificate Acceptance

4.4.1 Procedure during certificate handover

LCP

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

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

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

In the event that the subscriber detects errors in his certificates or in conjunction with the function of the keys and tokens, he must communicate this to the TSP without delay. The certificates are then 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 functions 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, the delivery constituting a service rather than a work within the meaning of German civil law.

4.4.2 Publication of the certificate by the TSP

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

The status can be retrieved via OCSP after production.

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

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

4.5 Key Pair and Certificate Usage

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

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

QCP-n-qscd, QCP-l-qscd

After expiry of the validity period or after revocation of the certificate, the associated private keys may no longer be used.

The provisions in section 1.4 apply to subscribers.

4.5.2 Use of the public key and of the certificate by relying parties

The certificates of the D-TRUST CSM PKI can be used by all relying parties. They can, however, only be relied upon if:

- the certificates are used in line with the types of use shown there (key use, extended key use, restricting extensions, if applicable),
- verification of the certificate chain can be carried out successfully right through to a trusted root certificate,
- the check of the status of the certificates via the status request service (OCSP) had a positive outcome, and

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

4.6 Certificate Renewal

The rules laid down in sections 4.7 and 3.3 apply.

4.7 Certificate Re-key

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

Certificate renewal is generally not performed for CA keys.

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

4.7.1 Conditions for certificate renewal

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

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

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

LCP

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

4.7.2 Authorization for certificate renewal

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

4.7.3 Processing an application for certificate renewal

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

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

4.7.4 Notification of the subscriber concerning the issuance of a new certificate

The rules laid down in section 4.3.2 apply.

4.7.5 Procedure in conjunction with the issuance of a certificate renewal

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

4.7.6 Publication of the certificate renewal by the TSP

The rules laid down in section 4.4.2 apply.

4.7.7 Notification of other PKI entities concerning the renewal of the certificate

The rules laid down in section 4.4.3 apply.

4.8 Certificate Modification

Certificate changes are not offered.

4.9 Certificate Revocation and Suspension

4.9.1 Conditions for revocation

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

QCP-q, EVCP

The procedures of the TSP additionally fulfil the requirements of [EN 319 411-2] and [GL-BRO].

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

A certificate is revoked in the following cases:

- when requested by the subscriber and/or the third party concerned (for instance, the organization named in the certificate),
- if information in the certificate is invalid,
- if the TSP discontinues its activities and if such activities are not continued by another TSP.

Notwithstanding the foregoing, the TSP can cause revocation if:

- the private key of the issuing or of a higher-level CA was compromised,
- weaknesses are detected in the encryption algorithm used which constitute serious risks for the permitted applications during the certification lifecycle,
- the hardware and software used show security shortcomings which constitute serious risks for the permitted applications during the certification lifecycle,
- unambiguous assignment of the key pair to the subscriber is no longer ensured,
- a certificate was obtained on the basis of false data or was otherwise 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.

EVCP, OVCP

Pursuant to [GL-BRO], the TSP offers PKI entities or software manufacturers an additional 24x7 service for EV/OV TLS certificates which 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 conformities.

Within 24 hours, the TSP begins addressing the events reported according to [GL-BRO] which can lead to revocation of the OV/EV certificates concerned.

This kind of security incident with D-Trust security certificates can be described and reported according to CP section 9.13.

Any revocation is 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.

4.9.2 Authorization for revocation

The TSP is authorized to revoke certificates.

Subscribers are always authorized to have their certificates revoked. Agreements can be made with subscribers pursuant to which they waive this right.

In the event that a certificate contains information regarding the subscriber's power to represent a third party, such third party is also authorized to request revocation of the certificate concerned. The body (for instance, a professional chamber) responsible for other information regarding an individual (such as the information "tax advisor") can also request revocation of the certificate concerned when the basis for such information about the individual ceases to exist following its 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.

Otherwise any individual will be deemed to be authorized to request revocation from the TSP if such individual mentions the correct revocation password.

4.9.3 Revocation request procedure

Revocation can be generally carried out by subscribers and/or their authorized representative via the agreed online interface(s).

Subjects must generally send revocation requests to the technical contact of the RA who then triggers a revocation order at the TSP via the agreed online interface. Unambiguous identification of the technical contact of the RA in relation to the online interface of the TSP is mandatory.

If a revocation password was agreed to, revocation requests can be submitted by telephone during nation-wide working days in Germany between 9am and 5pm.

Revocation number: +49 (0)30 / 25 93 91 - 602

QCP-w, OVCP, EVCP

Parties authorized to request revocation can do so on a 24/7 basis after authentication by their agreed revocation password.

Revocation number: +49 (0)30 / 25 93 91 – 601

Other revocation methods can be agreed to.

Certificate revocation requests submitted by e-mail must contain an unambiguous description of the certificate to be revoked and should hence include the following details:

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

Revocation is carried out in the TSP's sphere of responsibility. Notwithstanding this, the TSP can subcontract part of its tasks. The revocation service can be performed by third parties acting on the basis of the requirements of the TSP.

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

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

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

4.9.4 Revocation request deadlines

The subject or subscriber are solely responsible to ensure that they or a person authorized to request revocation on their behalf immediately request revocation as soon as reasons for revocation become known. The procedure which promises fastest processing of the revocation request must be used.

4.9.5 Time span for the processing of a revocation request by the TSP

The TSP processes revocation requests on nation-wide German working days between 9am and 5pm. Revocation requested by telephone is carried out immediately. Revocation requests received by e-mail and letter are processed the next working day at the latest.

QCP-w, EVCP, OVCP

Revocation is carried out following successful authorization of the party requesting revocation by telephone or via the online interface.

LCP

Revocation requests submitted via the online interface are carried out within 24 hours.

4.9.6 Methods available for checking revocation information

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

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

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

4.9.7 Publication frequency of certificate revocation lists

See section 2.3.

4.9.8 Maximum latency time for certificate revocation lists

Certificate revocation lists are published immediately following their generation.

4.9.9 Online availability of revocation information

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

4.9.10 Need for online verification of revocation information

There is no obligation for an online verification of revocation information; however, section 4.5.2 applies.

4.9.11 Other forms for notification of revocation information

None.

4.9.12 Special requirements in the case of compromising of the private key

None.

4.9.13 Conditions for suspension

Certificate suspension is not offered.

4.10 Certificate Status Services

4.10.1 Operation of the status request service

The status request 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.

The system time of the OCSP responder is synchronised daily with the official time via DCF77.

4.10.2 Availability of the status request service

The status request service is available 24/7.

4.10.3 Optional services

None.

4.11 End of Subscription

The validity of the certificate ends on the date shown in the certificate. Key renewal can be applied for according to section 3.3. The request to revoke a certificate by a subscriber or party authorized to request revocation leads to revocation by the TSP. The TSP's main contractual duties are thereby completely fulfilled.

4.12 Key Escrow and Recovery

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

4.12.1 Conditions and procedures for depositing and restoring private keys

The TSP does not offer key depositing.

4.12.2 Conditions and procedures for depositing and restoring session keys

The TSP does not offer key depositing.

5. Facility, Management, and Operational Controls

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

5.1 Physical Security Controls

Detailed documentation is available for structural security controls and the relevant parts of this can be made available for inspection to any party proving a relevant interest in such disclosure. The security concept has been audited by an independent audit and certification body. Auditing and certification are regularly repeated in accordance with [EN 319 411-1] and [EN 319 411-2].

Furthermore, TÜV-IT has certified that the trust service provider of D-TRUST GmbH applies and implements the "Infrastructure measures for high protection requirements – level 3" ["Infrastrukturmaßnahmen für hohen Schutzbedarf – Level 3"] (according to the catalogue of audit criteria for "Trusted Site Infrastructure") in its security area. This TÜV-IT certificate for a "Trusted Site Infrastructure" evaluates all infrastructure-relevant aspects. This audit is repeated every two years. The above-mentioned certificate confirms that D-TRUST GmbH fulfils this demanding security standard for its non-technical security controls.

The CAs of the CSM PKI which is the subject matter of this document are operated by the TSP under the same conditions as the CAs of D-TRUST GmbH for the issuance of qualified certificates.

5.2 Procedural Controls

5.2.1 Role concept

Documentation includes a role concept where TSP management assigns employees to one or more roles and they receive the 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.
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 organization 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, as a minimum, required for particularly security-critical operations. This is ensured by technical and organizational controls, such as access authorization and verification of knowledge.

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

5.2.3 Identification and authentication for individual roles

The role concept is ensured by technical and organizational controls, such as access authorization and verification of knowledge. Before being allowed to access any security-critical applications, the employee concerned must have been successfully authenticated. Event logs enable the identification of employees who performed past actions; the 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 acts.

5.3 Personnel Controls

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

5.3.1 Requirements in terms of qualification, experience and reliability

The TSP ensures that persons employed in the area of the certification service have the knowledge, experience and skills necessary for this activity.

The identity, reliability and professional qualifications of employees are verified prior to commencing their work. Regular and demand-driven training ensures competency in the respective fields of activity as well as general information security. Training and proficiency check results are documented.

5.3.2 Security screening

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

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

5.3.3 Training

The TSP trains certification service personnel.

5.3.4 Frequency of training and information

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

5.3.5 Frequency and sequence of job rotation

Role changes are documented. The corresponding employees are trained.

5.3.6 Controls in the case of unlawful acts

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

5.3.7 Requirements for freelance staff

Not applicable; no freelance staff are employed.

5.3.8 Documentation handed over

Comprehensive process instructions and procedures for all production steps 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 in the production process.

5.4 Audit Logging Procedures

5.4.1 Monitoring access

The TSP implements comprehensive surveillance controls (for instance, video surveillance) in order to warrant the security of its certification services and the underlying IT systems and documents.

The monitoring and surveillance controls are supplemented by organizational rules. Visitor rules, for instance, require visitors to be announced and registered by their names at least 24 hours before their visit. While in the area of the trust service provider's premises, visitors must at all times be accompanied by an employee of the TSP.

5.4.2 Monitoring organizational controls

Monitoring organizational controls another part of the security concept.

This includes a regular risk analysis that provides a comprehensive analysis of threats to the TSP's operation and defines requirements and countermeasures. It also includes an analysis of the residual risk where the appropriateness of the residual risk is identified and, if appropriate, accepted.

Furthermore, all relevant assets are correctly identified, and the corresponding changes to these assets are checked or, if applicable, released by the TSP staff commissioned 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 (including subsequent applications), documents concerning procedures (CP, CPS), certificates, revocation documentation, electronic files and reports/logs regarding the certificate lifecycle. 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.

Furthermore, security-relevant events are suitably recorded. The system time is synchronised daily with the official time via DCF77.

5.5.2 Archiving times for data

Application and verification documents as well as data concerning the certificate lifecycle and the certificates themselves are filed for a period of at least ten[2] years and until the end of the year. The period begins after the expiration of the term of validity of the certificate that was issued last on the basis of these documents.

If applicable, this also includes the corresponding system reports/logs that were generated as part of the stated events.

Furthermore, security-relevant events are suitably recorded. The system time is synchronised daily with the official time via DCF77.

[2] In the case of SSL/TLS certificates: seven years

5.5.3 Archive protection

The archive 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. The documentation is set up immediately so that subsequent changes will be discovered. European and German data protection requirements are adhered to.

5.5.5 Request for time stamping of records

The TSP operates a time stamping service in accordance with [eIDAS].

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 TSP.

5.6 Key Changeover

In due time before a CA expires, new CA keys are generated, and new CA instances set up and published.

5.7 Compromise and Disaster Recovery

5.7.1 Treatment of incidents and cases of compromising

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

5.7.2 Restoring after compromising of resources

The security concept describes the performance of recovery procedures.

5.7.3 Compromising of the private CA key

In the event of compromising or communication of uncertainty of algorithms or associated parameters by the issuers of the relevant catalogues according to section 6.1.6, the TSP initiates the following:

- The CA certificates as well as their certificates already issued and not yet expired are revoked.
- Subscribers affected are informed about the incident and its effects.
- The respective supervisory body is informed and the incident is published on the websites of the TSP including a statement that any certificates that were issued by this CA are no longer valid.

The analysis of the reasons for compromising is used, if possible, to design suitable measures in order to prevent future cases of compromising. Taking the reasons for compromising into consideration, new CA signature keys are generated and new CA certificates issued.

5.7.4 Ways of continuing business following compromising and disaster

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 compromising.

5.8 CA or RA Termination

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. Private CA keys which are concerned are destroyed.

In the event of a planned discontinuation of its operations, the TSP informs all end-entities, subscribers and third party in advance.

The repository service and application documents are 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 handed over either to another TSP or to Bundesdruckerei GmbH.

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

On completion of operations, the functionality of the CAs will be discontinued so that certification is no longer possible.

D-TRUST has a continuously updated termination plan.

6. Technical Security Controls

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

6.1 Key Pair Generation and Installation

6.1.1 Generation of key pairs

CA keys are generated in a "FIPS 140-2 Level 3"-compliant hardware security module (HSM). The HSM is located in the high-security area of the trust service provider. The role concept and hence the 4-eyes principle are compulsory for key generation. Whenever CA keys are generated, an independent auditor is always present or, following key generation, the auditor can use a video recording in order to verify the correctness of the key generation process. The generation of CA keys is also documented in accordance with [EN 319 411-1] or [EN 319 411-2], respectively.

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

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

6.1.2 Delivery of private keys to subscribers

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

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

6.1.3 Delivery of public keys to the TSP

Certificate requests can be submitted by subscribers for an existing key pair in the form of a PKCS#10 request which must be signed with the corresponding private key. The PKCS#10 request contains the public key. The corresponding response returns the complete certificate.

6.1.4 Delivery of public CA keys to relying parties

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

6.1.5 Key lengths

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

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

6.1.6 Determining the key parameters and quality control

QCP-w, EVCP, OVCP, LCP

CA and EE certificates are issued on the basis of keys that comply with [ETSI-ALG] in its latest applicable version in as far as compatibility in the use environment is ensured.

QCP-w, EVCP

CA and EE certificates are exclusively issued on the basis of keys that comply not only with [ETSI-ALG] but also with [EN 319 411-1] or [EN 319 411-2], respectively, and [GL-BRO] in their latest applicable version.

The signature and encryption algorithms are mentioned in section 7.1.3.

6.1.7 Key uses

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Standards and security controls for cryptographic modules

The cryptographic modules used by the TSP work perfectly. Throughout their entire lifecycle (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.

LCP

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

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

6.2.2 Multi-person access protection for private keys (n of m)

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

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

6.2.3 Depositing private keys (key escrow)

Private EE keys are not deposited by the TSP.

6.2.4 Backup of private keys

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 protection measures as the production system. Restoring private keys also requires two authorized persons. Further copies of the private CA keys do not exist.

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

6.2.5 Archiving of private keys

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 restoring purposes. Adherence to the 4-eyes principle is compulsory. Private CA keys exported to/imported from another HSM are protected by encryption.

6.2.7 Storage of private keys in cryptographic modules

The private CA keys are contained in encrypted form in the HSM.

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

6.2.8 Activation of private keys

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

Private EE keys are activated by entering the secret.

6.2.9 Deactivation of private keys

The private CA keys are deactivated by disconnecting the connection between the HSM and the application.

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

6.2.10 Destruction of private keys

The private CA keys are deleted when their term of validity expires. This is accomplished by deleting 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.

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

6.2.11 Assessment of cryptographic modules

The TSP operates suitable hardware-based and software-based key generators in order to warrant the quality of the EE keys. The HSMs used are FIPS 140-2 Level 3-compliant.

6.3 Other Aspects of Key Pair Management

6.3.1 Archiving of public keys

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

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

OVCP
Max. 825 days

QCP-w, EVCP
Max. 825 days

LCP
63 months

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

6.4 Activation Data

6.4.1 Generation and installation of activation data

The activation data of the CA keys is requested by the HSM. The PIN is assigned during the bootstrap procedure. Adherence to the 4-eyes principle is compulsory.

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

LCP
If EE keys are generated by the TSP, the PIN is either sent or handed over to the subscriber in a PIN letter or made available to the subscriber via a secured SSL connection or online interface. If the subscriber is not the subject, the subscriber is responsible for the secure delivery of the PIN to the subject.

6.4.2 Protection of activation data

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

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

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer Security Controls

6.5.1 Specific technical security requirements for 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 CPS and [EN 319 411-1] or [EN 319 411-2], respectively, and, in the case of EV certificates, with [GL-BRO].

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. 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.

6.5.2 Assessment of computer security

The computers, networks and other components used for the CA keys are regularly checked, inspected and audited by recognised inspection and certification 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 prioritised. 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 case of failures where one service is no longer available, the parties affected by this will be informed every 24 hours on the current status of trouble-shooting.

6.6 Life Cycle Security Controls

6.6.1 Security controls during development

During the course of all system development projects carried out by or on behalf of the TSP, security requirements are analysed already during the draft design phase. The results are defined as requirements for development.

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 analysed with a view to rule violations, attempted attacks and other incidents. Monitoring and surveillance measures begin when a device is set into operation and end when it is disposed of.

6.6.3 Security controls during the lifecycle

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 beyond any doubt that they were not manipulated. Sealing of hardware and software checks are, for instance, used in order to be able to detect manipulation and attempted manipulation during any activity or inspection. In the case of suspected manipulation of a component, any action planned will not be carried out and the incident is reported. In order to enable immediate and co-ordinated response to any security-relevant incidents, the TSP defines clear-cut escalation rules for the individual roles.

Capacity requirements and utilisation as well as the suitability of the systems involved are monitored and adapted as required. Devices exchanged or obsolete data media are 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 changes are checked by the security officer. After the 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 lifecycle 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 regularly by an independent and competent body. Weak point scans are also regularly carried out.

QCP-w, EVCP

The events specified in [GL-BRO] are, as a minimum, logged in an auditable form.

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. Detailed documentation is available for the network concept and the relevant parts of this can be made available for inspection to any party proving a relevant interest in such disclosure.

In order to protect the processes of the TSP, firewalls and intrusion detection/prevention mechanisms are used, for instance, that allow explicitly permitted connections only. The TSP operates network segments with different protection requirements and separates networks for employees and Internet uses on the one hand from server networks on the other. 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.

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.

6.8 Timestamping

The TSP operates a time stamping service. However, time stamps are not offered within the scope of this CPS.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version numbers

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

7.1.2 Certificate extensions

The selection of the extension is primarily 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
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	Address(es) of the CRL issuing authority/authorities
AuthorityInfoAccess	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	2.5.29.32	OIDs of the CPs supported
SubjectAltName	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: *digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, decipherOnly* and combinations thereof

EE certificates can include the following non-critical extensions:

Extension	OID	Parameter
ExtKeyUsage	2.5.29.37	Corresponding to [RFC 5280], [RFC 6818]
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
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	*accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation {…}* *accessMethod= caIssuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}*
certificatePolicies	2.5.29.32	OIDs of the CPs supported *cpsURI*
SubjectAltName	2.5.29.17	Alternative holder's name
QCStatements (QCP-w only)	*1.3.6.1.5.5.7.1.3*	esi4-qcStatement-1 {0 4 0 1862 1 1}; esi4-qcStatement-5 {0 4 0 1862 1 5};

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.

7.1.3 Algorithm OIDs

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

- RSA with OID 1.2.840.113549.1.1.1.
- RSA-PSS mit OID 1.2.840.113549.1.1.10.

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

- SHA512 RSA with OID 1.2.840.113549.1.1.13,
- SHA256 RSA with OID 1.2.840.113549.1.1.11.

7.1.4 Name formats

In the *subject* (here: name of the subject) and *issuer* (name of the issuer) fields, names are assigned according to [X.501] 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 *Issuer-AltName* (alternative issuer name) fields can contain names according to [RFC 5280], [RFC 6818] (coded as IA5String).

7.1.5 Name constraints

"NameConstraints" is not used.

7.1.6 Certificate Policy Object Identifier

"CertificatePolicies" can contain the OID of CPs supported.

Additional rules are laid down in the CP.

7.1.7 Use of the "PolicyConstraints" extension

"PolicyConstraints" is not used.

7.1.8 Syntax and semantics of "PolicyQualifiers"

"PolicyQualifiers" can be used.

7.1.9 Processing the semantics of the critical CertificatePolicies extension

In 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 Profile

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

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

7.3 OCSP Profile

In addition to RFC 6960, the OCSP responder also supports positive information.

7.3.1 Version number(s)

OCSP v1 according to [RFC 6960] is used.

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 Assessment

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.

This documentation is audited by an independent audit and certification body on a regular basis. Relevant parts of these documents can be inspected against proof of a legitimate interest.

The CP and CPS fulfil the requirements for certificates in accordance with [EN 319 411-1] or [EN 319 411-2], respectively, including the requirements of [BRG] and [NetSec-CAB]. Regular assessment by a qualified and competent independent party pursuant to [EN 319 411-1] or [EN 319 411-2], respectively, serves as proof of compatibility.

The TSP does not issue certificates with a policy OID reference to [EN 319 411-1] and [EN 319 411-2] until after initial and successfully completed auditing by an independent external certification body. Regular follow-up audits are conducted. When procedures and processes are found to be no longer in conformity with the current guidelines of [EN 319 411-1] or [EN 319 411-2], respectively, the TSP discontinues the issuance of the above-mentioned certificates until conformity with the guidelines is restored and has been audited accordingly.

This audit takes place annually.

Regular internal audits are additionally carried out.

9. Other Business and Legal Matters

With regard to the corresponding provisions, see section 9 in the CP as well as additionally the General Terms and Conditions [AGB].

BUNDESDRUCKEREI

Certification Practice Statement der D-TRUST CSM PKI

Version 2.3

Erscheinungsdatum 05.07.2018
Datum des Inkrafttretens 05.07.2018

D-TRUST EINE MARKE DER BUNDESDRUCKEREI

COPYRIGHT UND NUTZUNGSLIZENZ

Certification Practice Statement der D-TRUST CSM PKI

©2018 D-TRUST GmbH

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

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

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

Dokumentenhistorie

Version	Datum	Beschreibung
1.0	09.02.2015	▪ Initialversion
1.1	23.02.2015	▪ Editorische Änderungen im Rahmen der Erstzertifizierung gemäß ETSI 102 042 LCP. Es wurden diverse Inhalte aus der CP der D-TRUST GmbH in das CPS überführt.
1.2	05.10.2015	▪ Editorische Änderungen ▪ Konkretisierung der Möglichkeit das Schlüsselmaterial durch den TSP erzeugen und ausliefern zu lassen ▪ Sperrung nur noch über Online-Schnittstelle und wenn ein Sperrpasswort vereinbart wurde telefonisch ▪ Alle neuen Zertifikate werden immer im LDAP der D-TRUST veröffentlicht
1.3	03.10.2016	▪ Umstellung auf EN 319 411-1
2.0	01.01.2017	▪ Einführung von qualifizierten SSL-/TLS-Zertifikaten (QWACs) gemäß EN 319 411-2 und eIDAS
2.1	01.10.2017	▪ Editorische Änderungen und Konkretisierung des Kapitels 6.5
2.2	28.03.2018	▪ Editorische Änderungen und eine Überarbeitung der Kompatibilität mit RFC 3647 ▪ Anpassung Nutzungslizenz an „Creative Commons Attribution" ▪ Angleichung an die Mozilla Root Store Policy 2.5
2.3	05.07.2018	▪ Änderung der Domain-Validierungsmethoden in 4.2.1 ▪ Feld OrgID in Abschnitt 3.1.4 wurde gemäß Variante 3 aus Kapitel 5.1.4 der EN 319 412-1 ergänzt. ▪ Redaktionelle Anpassungen

Inhaltsverzeichnis

1. Einleitung 6
1.1 Überblick 6
1.2 Name und Kennzeichnung des Dokuments 8
1.3 PKI-Teilnehmer 8
1.4 Verwendung von Zertifikaten 10
1.5 Pflege und Aktualisierung des CPS 10
1.6 Begriffe und Abkürzungen 11
2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen 12
2.1 Verzeichnisse 12
2.2 Veröffentlichung von Informationen zu Zertifikaten 12
2.3 Häufigkeit von Veröffentlichungen 12
2.4 Zugriffskontrollen auf Verzeichnisse 13
3. Identifizierung und Authentifizierung 14
3.1 Namensregeln 14
3.2 Initiale Überprüfung der Identität 17
3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying) 19
3.4 Identifizierung und Authentifizierung von Sperranträgen 20
4. Betriebsanforderungen 21
4.1 Zertifikatsantrag und Registrierung 21
4.2 Verarbeitung des Zertifikatsantrags 21
4.3 Ausstellung von Zertifikaten 25
4.4 Zertifikatsübergabe 26
4.5 Verwendung des Schlüsselpaars und des Zertifikats 26
4.6 Zertifikatserneuerung (certificate renewal) 27
4.7 Zertifikatserneuerung mit Schlüsselerneuerung 27
4.8 Zertifikatsänderung 28
4.9 Sperrung und Suspendierung von Zertifikaten 28
4.10 Statusabfragedienst für Zertifikate 31
4.11 Austritt aus dem Zertifizierungsdienst 32
4.12 Schlüsselhinterlegung und –wiederherstellung 32
5. Nicht-technische Sicherheitsmaßnahmen 33
5.1 Bauliche Sicherheitsmaßnahmen 33
5.2 Verfahrensvorschriften 33
5.3 Eingesetztes Personal 34
5.4 Überwachungsmaßnahmen 35
5.5 Archivierung von Aufzeichnungen 35
5.6 Schlüsselwechsel beim TSP 36
5.7 Kompromittierung und Geschäftsweiterführung beim TSP 36
5.8 Schließung des TSP 37
6. Technische Sicherheitsmaßnahmen 38
6.1 Erzeugung und Installation von Schlüsselpaaren 38
6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module 39
6.3 Andere Aspekte des Managements von Schlüsselpaaren 41
6.4 Aktivierungsdaten 41
6.5 Sicherheitsmaßnahmen in den Rechneranlagen 42
6.6 Technische Maßnahmen während des Life Cycles 42
6.7 Sicherheitsmaßnahmen für Netze 43
6.8 Zeitstempel 44
7. Profile von Zertifikaten, Sperrlisten und OCSP 45
7.1 Zertifikatsprofile 45

7.2 Sperrlistenprofile 47
7.3 Profile des Statusabfragedienstes (OCSP) 48
8. Auditierungen und andere Prüfungen 49
9. Sonstige finanzielle und rechtliche Regelungen 50

1. Einleitung

1.1 Überblick

Dieses Dokument ist das Certification Practice Statement (CPS) der von D-TRUST GmbH betriebenen Vertrauensdienste, die über den Certificate Service Manager (CSM) bereitgestellt werden.

1.1.1 Vertrauensdiensteanbieter

Diese Regelungen sind in der CP festgehalten.

1.1.2 Über dieses Dokument

Dieses CPS definiert Abläufe und Vorgehensweisen 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.

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

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

Das gesamte CPS ist rechtsverbindlich, soweit dies im Rahmen der deutschen bzw. europäischen Gesetzgebung zulässig ist. Es enthält Aussagen über Pflichten, Gewährleistung und Haftung für die PKI-Teilnehmer. Soweit nicht ausdrücklich genannt, erfolgen auf Basis dieses CPS keine Zusicherungen oder Garantien im Rechtssinne.

Die Kenntnis der in dieser CPS beschriebenen Zertifizierungsverfahren und -regeln sowie der rechtlichen Rahmenbedingungen erlaubt es Zertifikatnutzern Vertrauen in die Komponenten dieser PKI und PKI-Teilnehmern aufzubauen und Entscheidungen zu treffen, inwieweit das durch die PKI gewährte Vertrauens- und Sicherheitsniveau für Anwendungen geeignet ist.

Die Struktur dieses Dokumentes ist eng an den Internet-Standard RFC 3647 „Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework" angelehnt, um eine einfache Lesbarkeit und Vergleichbarkeit mit anderen CPSs zu erreichen.

1.1.3 Eigenschaften der PKI

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

PKI für qualifizierte Vertrauensdienste

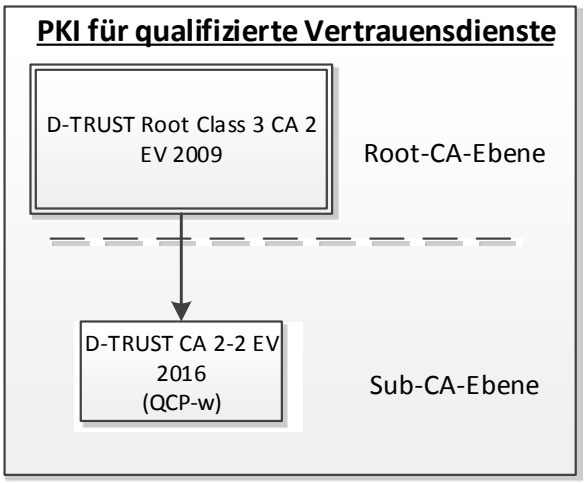

Abbildung 1 PKI-Hierarchie für qualifizierte Vertrauensdienste

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

QCP-w – Qualifizierte Webseitenzertifikate (QWACs)

QCP-w

EE-Zertifikate des Zertifizierungslevels QCP-w sind qualifizierte SSL-/TLS-Zertifikate gemäß [EN 319 411-2]. EV-Zertifikate werden nicht auf Chipkarten ausgegeben. Qualifizierte Webseitenzertifikate erfüllen immer auch die Anforderungen an SSL/TLS-Zertifikate nach dem Zertifizierungslevel EVCP gemäß [EN 319 411-1], was an der EV-Policy-OID in den EE-Zertifikaten erkennbar ist.

PKI für nicht-qualifizierte Vertrauensdienste

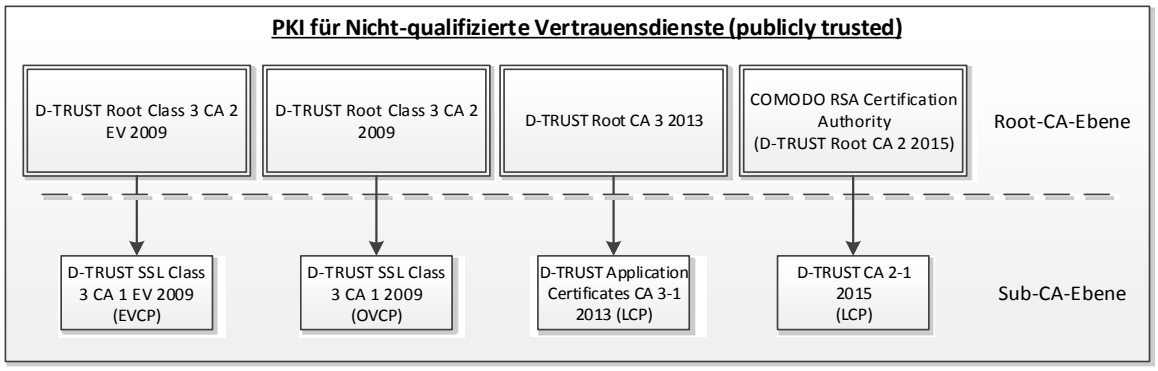

Abbildung 2 PKI-Hierarchie für nicht-qualifizierte Vertrauensdienste

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

LCP – Leightweight Certificate Policy

NCP – Normalized Certificate Policy

OVCP – Organisation Validated Certificate Policy

EVCP – Extended Validation Certificate Policy

Derzeit werden entsprechende Zertifizierungslevel (z.B. EVCP+), die die Verwendung einer sicheren Signaturerstellungseinheit (SSEE) voraussetzen nicht angeboten. Dennoch steht es dem Zertifikatnehmer frei, eine SSEE für die Erzeugung und Aufbewahrung seiner privaten Schlüssel zu verwenden.

EVCP

EE-Zertifikate des Zertifizierungslevels EVCP sind SSL-/TLS-Zertifikate. Dass es sich um EV-Zertifikate handelt, ist in den EE-Zertifikaten an der EV-Policy-OID erkennbar. EV-Zertifikate werden nicht auf Chipkarten ausgegeben.

OVCP

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

NCP

NCP-Zertifikate werden derzeit nicht angeboten. Daher wird im Folgenden auf die weitere Beschreibung verzichtet.

LCP

EE-Zertifikate des Zertifizierungslevels LCP sind einfache Personenzertifikate. Auch hier kann der Name einer Organisation als Attribut in das Zertifikat aufgenommen werden. LCP-Zertifikate werden nicht auf Chipkarten ausgegeben.

1.2 Name und Kennzeichnung des Dokuments

Dokumentname:	Certification Practice Statement der D-TRUST CSM PKI
Version	2.3

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (CA)

Zertifizierungsstellen (Certification Authority – CA) werden vom Vertrauensdiensteanbieter betrieben und stellen Zertifikate sowie Sperrlisten aus. Möglich sind folgende Arten von Zertifikaten:

- Personenzertifikate für natürliche Personen (EE-Zertifikat),
- Siegelzertifikate für juristische Personen (EE-Zertifikat),
- Gruppenzertifikate für Personengruppen, Funktionen und IT-Prozesse (EE-Zertifikat),
- Maschinenzertifikate für IT-Prozesse und Kommunikationsverbindungen (EE-Zertifikat)
- 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.

LCP

Die ausstellende SubCA kann von einer anderen Root-CA cross-signiert werden. Sämtliche Festlegungen aus dieser CPS sind auch hier gültig.

1.3.2 Registrierungsstellen (RA)

Die RA identifiziert und authentifiziert Zertifikatnehmer (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 D-TRUST betrieben werden, werden derzeit nur für die Identifizierung im Rahmen des Zertifizierungslevel LCP eingesetzt.

1.3.3 Zertifikatnehmer (ZNE) und Endanwender (EE)

Zertifikatnehmer (*subscriber*) sind natürliche oder juristische Personen, die EE-Zertifikate beantragen und innehaben. Der Zertifikatnehmer 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 Zertifikatnehmer identisch sein. Zulässige Endanwender sind:

- natürliche Personen,
- juristische Personen,
- Personengruppen oder Teams,
- Funktionen, die durch Mitarbeiter einer Organisation ausgefüllt werden und
- IT-Prozesse (z. B. SSL-Server).

Die Verantwortung für Schlüssel und Zertifikat trägt der Zertifikatnehmer, wenn das Schlüsselmaterial vom Zertifikatnehmer erzeugt wurde bzw. sobald dieses durch den Vertrauensdiensteanbieter an ihn übergeben wurde. Darüber hinaus ergeben sich nach [EN 319 411-1] bzw. [EN 319 411-2] weitere Pflichten. Spätestens zum Zeitpunkt der Antragstellung wird der Zertifikatnehmer über diese Pflichten durch die Bereitstellung dieses CPS und der Verpflichtungserklärung (subscriber agreement) informiert und muss sich zu deren Einhaltung verpflichten. Für SSL Zertifikate gilt die Verpflichtungserklärung für SSL Zertifikate. Für alle anderen Zertifikate unter dieser Policy gilt die allgemeine Verpflichtungserklärung.

EVCP, OVCP, LCP

Sind Zertifikatnehmer und Endanwender nicht identisch und der Endanwender eine natürliche Person, ist der Zertifikatnehmer für die Einhaltung der Pflichten durch den Endanwender verantwortlich.

QCP-w, EVCP, OVCP

SSL-/TLS-Zertifikate werden ausschließlich für juristische Personen ausgestellt.

1.3.4 Zertifikatnutzer (ZNU)

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

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.

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

Zertifikatnutzer handeln auf eigene Verantwortung. Es liegt in der Verantwortung des Zertifikatnutzers, einzuschätzen, ob dieses 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 Zertifikaten

Andere Verwendungsarten als die im Zertifikat festgelegten, sind nicht zulässig. Weiterhin gelten die Regelungen der CP der D-TRUST GmbH.

1.4.3 Verwendung von Dienstezertifikaten

Der TSP verwendet Dienstezertifikate zur Erbringung von Vertrauensdiensten 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 Sperrauskünften[1]

1.5 Pflege und Aktualisierung des CPS

1.5.1 Zuständigkeit für das Dokument

Dieses CPS wird durch die D-TRUST GmbH gepflegt und aktualisiert. Der Beauftragte der Geschäftsführung übernimmt die Abnahme des Dokuments.

Dieses CPS wird jährlich durch den TSP überprüft und ggf. aktualisiert. Eine Änderung wird durch eine neue Versionsnummer dieses Dokumentes kenntlich gemacht.

1.5.2 Ansprechpartner/Kontaktperson/Sekretariat

Diese Regelungen sind in der CP festgehalten.

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 dieser CPS nicht widersprechen. Die Referenz einer Policy-OID in den

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

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

QCP-w, EVCP

SSL-/TLS-Zertifikate, bzw. deren Sub- sowie Root-CAs kommen den Anforderungen des CA/Browser Forum Guidelines for Extended Validation Certificates [GL-BRO] und [EN 319 411-1] sowie [EN 319 411-2] nach. Im Falle von Inkonsistenzen zwischen diesem Dokument und den genannten Guidelines gelten vorrangig die [GL-BRO] und [EN 319 411-1] sowie [EN 319 411-2].

1.6 Begriffe und Abkürzungen

1.6.1 Begriffe und Namen

Diese Regelungen sind in der CP festgehalten.

1.6.2 Abkürzungen

Diese Regelungen sind in der CP festgehalten.

1.6.3 Referenzen

Diese Regelungen sind in der CP festgehalten.

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Diese Regelungen sind in der CP festgehalten.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Der TSP veröffentlicht folgende Informationen:

- EE-Zertifikate,
- CA-Zertifikate,
- Sperrlisten (CRLs) und Statusinformationen,
- die CP,
- dieses CPS,
- die Verpflichtungserklärung für SSL-/TLS-Zertifikate,
- die Verpflichtungserklärung für alle anderen Zertifikate unter dieser Policy (allgemeine Verpflichtungserklärung),
- Cross-Zertifikate
- die PKI-Nutzerinformation für qualifizierte Vertrauensdienste.

2.3 Häufigkeit von Veröffentlichungen

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

QCP-w

Veröffentlichte EE-Zertifikate bleiben bis zum Ende ihrer Gültigkeit sowie mindestens für zehn Jahre und bis zum Jahresende abrufbar.

CA-Zertifikate werden nach ihrer Erstellung veröffentlicht und:

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

nach Ablauf der Gültigkeit der CA vorgehalten.

Sperrlisten werden regelmäßig und bis zum Ende der Gültigkeit des ausstellen-den CA-Zertifikats ausgestellt. Sperrlisten werden unmittelbar nach Sperrungen erstellt und veröffentlicht. Auch wenn keine Sperrungen erfolgen, stellt der TSP sicher, das mindestens alle 24 Std. eine neue Sperrliste ausgestellt wird. Die Sperrlisten werden mindestens ein Jahr nach Ablauf der Gültigkeit der CA vor-gehalten.

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

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

2.4 Zugriffskontrollen auf Verzeichnisse

Zertifikate, Sperrlisten und dieses CPS können öffentlich und unentgeltlich abgerufen werden. 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 ausgegeben werden.

3. Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

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

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

3.1.2 Notwendigkeit für aussagefähige Namen

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

Eine eindeutige Zuordnung des Zertifikats zum Zertifikatnehmer (bei Zertifikaten für natürliche Personen auch zum Endanwender) ist gegeben.

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

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

3.1.3 Anonymität oder Pseudonyme von Zertifikatnehmern

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

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

3.1.4 Regeln für die Interpretation verschiedener Namensformen

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

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

DN-Bestandteil	Interpretation
CN (common name)	*Gebräuchlicher Name:* Folgende Varianten werden verwendet: Natürlichen Personen ohne Pseudonym: „Familienname, Rufname". Natürliche Personen mit Pseudonym: „Pseudonym:PN". Juristische Personen: offizielle Bezeichnung der Organisation (Firma, Behörde, Verein etc.), ggf. sinnvolle Abkürzung bei Überschreiten der Zeichenbegrenzung von 64 Zeichen. Sonderfall: ein oder mehrere Domainnamen können ebenfalls in den CN aufgenommen werden. QCP-w, EVCP: Wildcards sind nicht zulässig bei SSL-/TLS-Zertifikaten. Funktion oder Personengruppe: Name der Funktion oder Personengruppe mit dem vorangestellten Abkürzung „GRP:" als Hinweis, dass es sich um ein Gruppenzertifikat handelt Technische Komponenten: Name des Servers, des Dienstes oder der Applikation, der/die das Zertifikat benutzt.
PN	*Pseudonym*: ist identisch zu CN.
serialNumber	*Seriennummer*: Namenszusatznummer, welche die Eindeutigkeit des Namens sicherstellt (i.d.R. die Antragsnummer). Sonderfall bei EV-Zertifikate gemäß [GL-BRO]: Registernummer falls vergeben, Datum der Registrierung oder Gründung. Produktspezifisch kann das Feld anderweitig verwendet werden.
O (organization)	Offizielle Bezeichnung des Zertifikatnehmers oder Bezeichnung der *Organisation*, der der Endanwender angehört oder damit verbunden ist (Firma, Behörde, Verein etc.) entsprechend Existenznachweis, ggf. sinnvolle Abkürzung bei Überschreiten der Zeichenbegrenzung von 64 Zeichen.
OU (organization unit)	*Organisationseinheit* (Abteilung, Bereich oder andere Unterteilung) der Organisation.
OrgID (organization identifier)	QCP-w: *Eindeutige Organisationsnummer* der Organisation. Es kann die Nummer des Handelsregistereintrags sowie die Umsatzsteueridentnummer oder eine von D-TRUST vergebene Nummer eingetragen werden. Die von D-TRUST vergebene Nummer ist an das Format gemäß Variante 3 aus Kapitel 5.1.4 der EN 319 412-1 angelehnt und setzt sich wie folgt zusammen: DT:DE-1234567890 (DT: D-TRUST; DE: Deutschland; zufällige Nummer, die der Organisation eindeutig zugeordnet wird).

DN-Bestandteil	Interpretation
C (country)	Das aufzuführende Land wird gemäß [ISO 3166] notiert und ergibt sich wie folgt: Ist eine Organisation O im DistinguishedName aufgeführt, so bestimmt der im Register benannte Sitz der Organisation den Eintrag im Zertifikat. Ist keine Organisation O eingetragen, so wird das Land aufgenommen, dass das Dokument ausgestellt hat, mit dem der Zertifikatnehmer identifiziert wurde.
Street	Postalische Adresse *Straße*
Locality	Postalische Adresse *Ort*
State	Postalische Adresse *(Bundes-)Land*
PostalCode	Postalische Adresse *Postleitzahl*
BusinessCategory	Business Category (2.5.4.15) gemäß [GL-BRO]
Jurisdiction Of Incorporation Locality	Gerichtsstand der Organisation gemäß [GL-BRO]: *Ort* (1.3.6.1.4.1.311.60.2.1.1)
Jurisdiction Of Incorporation State Or Province Name	Gerichtsstand der Organisation: *(Bundes-)Land* (1.3.6.1.4.1.311.60.2.1.2)
Jurisdiction Of Incorporation CountryName	Gerichtsstand der Organisation gemäß [GL-BRO]: *Land* (1.3.6.1.4.1.311.60.2.1.3)

QCP-w, EVCP

SSL-/TLS-Zertifikate enthalten mindestens die subject-DN-Bestandteile „Organization", „CommonName", „subjectAlternativName", „BusinessCategory", „Jurisdiction of Incorporation or Registration", „subjectSerialNumber", „Locality", „State" sowie „Country", „StreetAddress" und „Postal Code".

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

3.1.5 Eindeutigkeit von Namen

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

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

3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen

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

QCP-w, EVCP

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

3.2 Initiale Überprüfung der Identität

3.2.1 Nachweis für den Besitz des privaten Schlüssels

Es werden zwei Fälle unterschieden:

a) Schlüsselpaare von Zertifikatnehmern werden im Verantwortungsbereich des TSP produziert. Mit der Übergabe der Token oder Soft-PSE (LCP) und ggf. PIN-Briefe gemäß Abschnitt 4.4.1 an die Zertifikatnehmer durch den TSP wird sichergestellt, dass die privaten Schlüssel in den Besitz der Zertifikatnehmer gelangen.

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

3.2.2 Identifizierung und Authentifizierung von Organisationen

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

Für die Teilnehmeridentifizierung und die Antragsprüfung gelten die Vorgaben aus [EN 319 411-1] je nach Anwendbarkeit LCP, EVCP oder OVCP oder aus [EN 319 411-1] und [EN 319 411-2] für QCP-w. Die Prüfung erfasst alle DN-Bestandteile.

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

	QCP-w, EVCP	OVCP
CN	Register/ Non-Register/ Domain/ CAA	Register/ Non-Register/ Domain/ CAA
C	Register/ Non-Register/ Domain	Register/ Non-Register/ Domain
O		
OU	Z-Bestätigung/ A-Bestätigung	Z-Bestätigung/ A-Bestätigung
STREET	Register/ Non-Register	Register/ Non-Register
L		
State		
PostalCode		

	QCP-w, EVCP	OVCP
Alternativer Antragsteller (SAN)	Domain/ CAA	Domain/ CAA
Alle weiteren Attribute	Z-Bestätigung/ A-Bestätigung/ Dok-Ident/ out-of-band-Mechanismen/ Register/ Non-Register	A-Bestätigung/ Dok-Ident/ out-of-band-Mechanismen

Wird der Antrag im Auftrag einer juristischen Person gestellt, muss der Vertreter (analog zu dem Verfahren für die Organisationszugehörigkeit aus Abschnitt 3.2.3) seine diesbezügliche Berechtigung nachweisen und sich authentifizieren.

Nachweise in nicht lateinischer Schrift werden nicht akzeptiert.

3.2.3 Identifizierung und Authentifizierung natürlicher Personen

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

LCP

Zertifikatnehmer die für andere natürliche Personen Zertifikate beantragen, müssen ihre Berechtigung zur Antragstellung nachweisen. Die Überprüfung der Daten bezieht sich auf den Zertifikatnehmer.

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

	LCP
G	HR-DB / Dok-Ident / Pers-Ident
SN	
CN	HR-DB / Register / Non-Register / Domain
C	
O	Register / Non-Register / Z-Bestätigung / A-Bestätigung/
OU	Z-Bestätigung / A-Bestätigung
STREET	n.a.
L	
State	
PostalCode	
Alternativer Antragsteller (SAN)	Domain / E-Mail-Adresse

	LCP
Alle weiteren Attribute	A-Bestätigung/ Dok-Ident/ out-of-band-Mechanismen

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

Nachweise in nicht lateinischer Schrift werden nicht akzeptiert.

3.2.4 Ungeprüfte Angaben zum Zertifikatnehmer

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

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

3.2.5 Prüfung der Berechtigung zur Antragstellung

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

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

3.2.6 Kriterien für die Interoperabilität

Siehe Abschnitt 1.5.3.

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

Eine Schlüsselerneuerung ist gleichbedeutend mit der erneuten Produktion von Zertifikaten ggf. Token und Schlüsseln für denselben Endanwender. Schlüsselerneuerungen werden nur für OVCP- und LCP-Zertifikate, aber nicht für SSL-Zertifikate gemäß EVCP oder QCP-w angeboten. Bei diesen Zertifikaten muss der gesamte Identifizierungs- und Registrierungsprozess wie bei einem Erstantrag durchlaufen werden, ggf. können aber bereits vorliegende Nachweisdokumente wiederverwendet werden, wenn sie nach [GL-BRO] noch verwertbar sind.

3.3.1 Routinemäßige Anträge zur Schlüsselerneuerung

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

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

3.3.2 Schlüsselerneuerung nach Sperrungen

Schlüsselerneuerung auf Basis eines gesperrten Zertifikats wird nicht angeboten.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Sperrberechtigung wird wie folgt geprüft:

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

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

LCP

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

Sperrverfahren werden in Abschnitt 4.9 definiert.

4. Betriebsanforderungen

4.1 Zertifikatsantrag und Registrierung

4.1.1 Berechtigung zur Antragstellung

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

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

QCP-w, EVCP

Zertifikatnehmer müssen den Anforderungen aus [GL-BRO] entsprechen.

CA-Zertifikate werden ausschließlich an juristische Personen ausgegeben.

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

4.1.2 Registrierungsprozess und Zuständigkeiten

Der TSP gewährleistet die Einhaltung des Registrierungsprozesses. Die entsprechenden Aufgaben können von vertraglich gebundenen Partnern oder externen Anbietern übernommen werden, die die Maßgaben von CP und CPS nachweislich erfüllen.

QCP-w, EVCP

Dem Zertifikatnehmer liegen vor Abschluss des Registrierungsprozesses CP und CPS sowie eine Verpflichtungserklärung (Subscriber Agreement) vor, zu deren Einhaltung sich der Zertifikatnehmer verpflichtet. Die Dokumente werden veröffentlicht. Die Verpflichtungserklärung entspricht den Vorgaben aus [EN 319 411-1] und [EN 319 411-2]. Nachweise werden elektronisch oder papierbasiert hinterlegt. Die Verpflichtungserklärung entspricht dem „Subscriber Agreement" gemäß den Vorgaben aus [GL-BRO].

LCP

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

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Der beschriebene Identifizierungs- und Registrierungsprozess muss vollständig durchlaufen und alle nötigen Nachweise dabei erbracht werden.

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 Schlüsselmaterial sowie PINs abgeschlossen sein.

Natürliche Personen müssen eindeutig identifiziert werden. Um Verwechslungen zu vermeiden, müssen ggf. weitere Attribute wie Geburtsort, Geburtsdatum oder andere anwendbare individuelle Merkmale aufgenommen werden. Werden juristische Personen im Zertifikat benannt oder sind sie Zertifikatnehmer, müssen deren vollständiger Name und rechtlicher Status sowie ggf. relevante Registerinformationen geprüft werden.

Die Identifizierung findet gemäß Abschnitt 3.2.3 statt.

Der TSP definiert die folgenden Prüfverfahren:

Pers-Ident
Die natürliche Person muss sich von einer RA oder einem zugelassenen Identifizierungspartner (z.B. PostIdent der Deutschen Post AG oder identity Trust Management AG), der die Maßgaben des CPS erfüllt, 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. Nachweise werden hinterlegt. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

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, Handelsregisterauszüge oder vergleichbare Auszüge, die nicht älter als ein halbes Jahr sind, Promotions-, Habilitations-, Ernennungsurkunden sowie Dokumente vergleichbaren Ranges.
Nachweise werden hinterlegt. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt 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 (Registergerichte, Bundeszentralamt für Steuern, berufsständischen Körperschaften öffentlichen Rechts oder vergleichbare) oder privatrechtliche Register (DUNS, 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. Nachweise werden hinterlegt. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

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. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

HR-DB
Der TSP schließt vertragliche Vereinbarungen mit einer Organisation (Zertifikatnehmer) und vereinbart, dass nur valide Daten übermittelt werden, die die Vorgaben des CPS erfüllen. 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 Zertifikatnehmer den Endanwender über dessen Pflichten aus der Verpflichtungserklärung und ggf. Sperrmöglichkeiten 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 Zertifikatnehmer in die Verpflichtungs-erklärung eingewilligt hat.

Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

Z-Bestätigung
Ein Zeichnungsberechtigter der Organisation bestätigt zertifikatsrelevante Informationen. Dies geschieht schriftlich, in Einzelfällen können elektronisch signierte Bestätigungen akzeptiert werden. Die Zeichnungsberechtigung muss entweder aus dem Existenznachweis der Organisation ersichtlich sein oder anderweitig nachgewiesen werden. Der Zeichnungs-berechtigte kann schriftlich einen Vertreter benennen (siehe A-Bestätigung). Nachweise werden hinterlegt. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

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, in Einzelfällen können elektronisch signierte Bestätigungen akzeptiert werden. Nachweise werden hinterlegt. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

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 Zertifikatnehmer 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 ist auch eine telefonische Nachfrage über ein öffentliches Telefonverzeichnis seitens des TSP.

Zur Identifizierung natürlicher Personen kann eine postalische Sendung mittels "Einschreiben mit Rückschein" vom TSP an den Zertifikatnehmer 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.

Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

Körperschaften
Der TSP schließt vertragliche Vereinbarungen mit Körperschaften des öffentlichen Rechts und vereinbart, dass nur Daten übermittelt werden, die die Vorgaben des CPS 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. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

Domain
Eine Organisation wird nach folgenden Verfahren hinsichtlich eines Domain-Nutzungsrechts beziehungsweise dessen Kontrolle geprüft.

QCP-w, EVCP, OVCP, LCP

gemäß [BRG Version 1.5.7] 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact sowie [BRG Version 1.5.7] Kapitel 3.2.2.4.4 Constructed Email to Domain Contact und [BRG Version 1.5.7] 3.2.2.4.6 Agreed-Upon Change to Website.

Die folgenden Domain-Validierungsmethoden können bis zum 31.07.2018 angewendet werden: gemäß [BRG Version 1.5.4] 3.2.2.4.5 Domain Authorization Document sowie [BRG Version 1.5.4] Kapitel 3.2.2.4.1 Validating the Applicant as a Domain Contact.

QCP-w, EVCP

Bei SSL-/TLS-Zertifikaten wird zusätzlich eine Überprüfung des Domainnamens gegen bekannte Phishing Domains und anderen Blacklists durchgeführt. Nicht registrierungspflichtige Domainnamen sowie Top-Level-Domain sind nicht zulässig.

Die Ergebnisse der Abfrage werden hinterlegt.

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

D-TRUST prüft sowohl bei Antragsannahme als auch unmittelbar vor Freischaltung des Zertifikats enthaltene Domains auf einen entsprechenden CAA-Eintrag. Geprüfte Domains können zur Zertifikatserstellung verwendet werden, wenn entweder der CAA-Eintrag leer ist oder D-Trust als CA vom Domaininhaber eingetragen wurde.

Zulässige Werte sind dtrust.de, d-trust.de, dtrust.net, d-trust.net, D-Trust GmbH sowie D-Trust.

D-TRUST kann keine TLS-Zertifikate ausstellen, wenn in dem CAA Ressource Record eine andere CA aufgeführt ist.

E-Mail
Die Domain, die in einer eingetragenen E-Mail-Adresse verwendet wird, muss der eingetragenen Organisation eindeutig zuzuordnen sein.

Ist dies nicht der Fall, schickt der TSP an die zu bestätigende E-Mail-Adresse eine E-Mail, deren Empfang bestätigt werden muss (Geheimnisaustausch). Die Ergebnisse der Abfrage werden hinterlegt.

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

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Treten bei der Prüfung der Identität durch die RA oder den TSP oder der Prüfung auf Korrektheit der Daten im Zertifikatsantrag oder den Ausweis- und Nachweisdokumenten Unstimmigkeiten auf, die nicht restlos ausgeräumt werden können, wird der Antrag abgelehnt.

Es kann vereinbart werden, dass Zertifikatsanträge gemäß den vereinbarten Attributen durch den TSP angepasst werden.

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 oder
- Umstände, die den Verdacht begründen, dass eine Zertifikatsausstellung den Betreiber der CA in Misskredit bringt.

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 Übereinstimmung mit den hinterlegten Nachweisen überprüft. Diese Überprüfung entfällt für den TSP, wenn vertragliche Vereinbarungen mit Partnern bestehen, bei denen beauftragte, unabhängige Personen die Requests dem TSP zur Produktion zur Verfügung stellen. 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.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

entfällt

4.3 Ausstellung von Zertifikaten

4.3.1 Vorgehen des TSP bei der Ausstellung von Zertifikaten

Im Hochsicherheitsbereich des Trustcenters werden die entsprechenden Zertifikate ausgefertigt.

Dabei wird sichergestellt, dass bei der Zertifikatserstellung 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.

EVCP, OCP-w, OVCP

Die D-Trust GmbH verwendet bei der Ausstellung von TLS-Zertifikaten Certificate Transparency (CT) gemäß RFC 6962. Der Standard sieht die Veröffentlichung aller durch die CA ausgestellten TLS-Zertifikate in mindestens drei revisionssicheren Logs externer Anbieter vor.

4.3.2 Benachrichtigung des Zertifikatnehmers über die Ausstellung des Zertifikats.

Es erfolgt keine gesonderte Benachrichtigung des Zertifikatnehmers nach der Fertigstellung des Zertifikats.

4.4 Zertifikatsübergabe

4.4.1 Verhalten bei der Zertifikatsübergabe

LCP

Soft-PSEs, deren privater Schlüssel im Bereich des TSP erstellt wurde, werden zum zugriffsgeschützen und SSL-verschlüsselten Download bzw. SSL-geschützter Schnittstelle (CSM) bereitgestellt oder per E-Mail gesendet (die PKCS#12-Datei ist mit einer PIN geschützt).

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

Kundenspezifisch können abweichende Verfahren vereinbart werden.

Entdeckt der Zertifikatnehmer Fehler in seinen Zertifikaten oder bei der Funktion der Schlüssel und Token, so hat er dies dem TSP unverzüglich mitzuteilen. Die Zertifikate werden gesperrt.

Fehlerhafte Angaben in den Zertifikaten gelten nur insoweit als vertraglicher Mangel im Sinne des Gesetzes, soweit der TSP nach diesem 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

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

Der Status ist nach Produktion über OCSP abrufbar.

4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats

Sperrberechtigte Dritte nach Abschnitt 4.9.2 werden schriftlich benachrichtigt und erhalten das Sperrpasswort, sofern nichts anderes mit der Organisation oder dem Sperrberechtigten Dritten vereinbart wurde.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatnehmer

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

QCP-n-qscd, QCP-l-qscd

After expiry of the validity period or after revocation of the certificate, the associated private keys may no longer be used.

Für Zertifikatnehmer gelten die Bestimmungen aus Abschnitt 1.4.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatnutzer

Die Zertifikate der D-TRUST CSM PKI können von allen Zertifikatnutzern verwendet werden. Es kann jedoch nur dann darauf vertraut werden, wenn

- die Zertifikate entsprechend den dort vermerkten Nutzungsarten (Schlüsselverwendung, erweiterte Schlüsselverwendung, ggf. einschränkende Extentions) benutzt werden,
- die Verifikation der Zertifikatskette bis zu einem vertrauenswürdigen Root-Zertifikat erfolgreich durchgeführt werden kann,
- der Status der Zertifikate über den Statusabfragedienst (OCSP) positiv geprüft wurde und
- alle weiteren in Vereinbarungen oder an anderer Stelle angegebenen Vorsichtsmaßnahmen getroffen wurden, eventuelle Einschränkungen im Zertifikat und jegliche anwendungsspezifische Vorkehrungen seitens des Zertifikatnutzers berücksichtigt und als kompatibel erkannt wurden.

4.6 Zertifikatserneuerung (certificate renewal)

Es gelten die Anforderungen aus Abschnitt 4.7 und 3.3.

4.7 Zertifikatserneuerung mit Schlüsselerneuerung

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

Bei CA-Schlüsseln wird keine Zertifikatserneuerung durchgeführt.

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

4.7.1 Bedingungen für eine Zertifikatserneuerung

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

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

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

LCP

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

4.7.2 Berechtigung zur Zertifikatserneuerung

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

4.7.3 Bearbeitung eines Antrags auf Zertifikatserneuerung

Zertifikatnehmer, die berechtigt sind, Anträge auf Zertifikatserneuerung zu stellen, nutzen eine produktspezifisch bereitgestellte Onlineschnittstelle des TSP zur Antragstellung.

Über die entsprechenden Schnittstellen gestellte Anträge werden automatisiert auf Berechtigung und Inhalt geprüft.

4.7.4 Benachrichtigung des Zertifikatnehmers über die Ausgabe eines neuen Zertifikats

Es gelten die in Abschnitt 0 festgelegten Regelungen.

4.7.5 Verhalten bei der Ausgabe einer Zertifikatserneuerung

Das erzeugte Zertifikat wird über die bereitgestellte Online-Schnittstelle zur Verfügung gestellt. Weiterhin gelten die in Abschnitt 4.4.1 festgelegten anwendbaren Regelungen.

4.7.6 Veröffentlichung der Zertifikatserneuerung durch den TSP

Es gelten die in Abschnitt 4.4.2 festgelegten Regelungen.

4.7.7 Benachrichtigung anderer PKI-Teilnehmer über die Erneuerung des Zertifikats

Es gelten die in Abschnitt 4.4.3 festgelegten Regelungen.

4.8 Zertifikatsänderung

Zertifikatsänderungen werden nicht angeboten.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Bedingungen für eine Sperrung

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

QCP-w, EVCP
Die Verfahren des TSP erfüllen zusätzlich die Bedingungen aus [EN 319 411-2] und [GL-BRO].

Zertifikatnehmer oder betroffenen Dritte sind aufgefordert, die Sperrung 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 Zertifikatnehmers zu einer Organisation).

Die Sperrung eines Zertifikats wird bei folgenden Ereignissen durchgeführt:

- auf Verlangen des Zertifikatnehmers bzw. betroffenen Dritten (z.B. die im Zertifikat genannte Organisation),
- Ungültigkeit von Angaben im Zertifikat,
- wenn der TSP seine Tätigkeit beendet und diese nicht von einem anderen TSP fortgeführt wird.

Unabhängig davon kann der TSP Sperrungen veranlassen, wenn:

- der private Schlüssel der ausstellenden oder einer übergeordneten CA kompromittiert 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 zum Zertifikatnehmer nicht mehr gegeben ist,
- ein Zertifikat aufgrund falscher Angaben erwirkt oder anderweitig missbraucht wurde,
- 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.

EVCP, OVCP

Der TSP bietet PKI-Teilnehmern oder Software-Herstellern gemäß [GL-BRO] für EV/OV TLS-Zertifikate 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.

Innerhalb von 24 Stunden beginnt der TSP mit der Bearbeitung der Vorfälle gemäß [GL-BRO], was die Sperrung der betroffenen OV/EV-Zertifikate auslösen kann.

Diese Art von zu prüfenden Sicherheitsvorfällen bei Sicherheitszertifikaten bei D-TRUST können gemäß CP Abschnitt 9.13 beschrieben und gemeldet werden.

Sperrungen enthalten eine Angabe des Zeitpunkts der Sperrung und werden nicht rückwirkend erstellt. Weiterhin kann eine Sperrung nicht rückgängig gemacht werden.

Sperrberechtigte müssen sich gemäß Abschnitt 3.4 authentifizieren.

4.9.2 Berechtigung zur Sperrung

Der TSP ist sperrberechtigt.

Der Zertifikatnehmer hat stets die Berechtigung zur Sperrung seiner Zertifikate. Es können Vereinbarungen getroffen werden, in denen der Zertifikatnehmer auf dieses Recht verzichtet.

Enthält ein Zertifikat Angaben über die Vertretungsvollmacht des Zertifikatnehmers für eine dritte Person, so kann auch die dritte Person eine Sperrung des betreffenden Zertifikates verlangen. Die für sonstige Angaben zur Person (z.B. die Angabe „Steuerberater“) zuständige Stelle (z.B. zuständige Kammer) kann ebenfalls eine Sperrung des betreffenden Zertifikates verlangen, wenn die Voraussetzungen für die Angaben zur Person nach Aufnahme in das Zertifikat entfallen. Zusätzliche Sperrberechtigte Dritte können benannt werden und haben dann stets die Berechtigung zur Sperrung dieser Zertifikate.

Im Übrigen gilt jede Person als sperrberechtigt gegenüber dem TSP, soweit sie das zutreffende Sperrpasswort mitteilt.

4.9.3 Verfahren für einen Sperrantrag

Sperrungen können grundsätzlich über die vereinbarte Online-Schnittstelle(n) durch den Zertifikatnehmer bzw. seinen autorisierten Vertreter durchgeführt werden.

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

Soweit ein Sperrpasswort vereinbart wurde, können Sperranträge telefonisch an bundeseinheitlichen Arbeitstagen in der Zeit von 9 - 17 Uhr gestellt werden.

Sperrnummer: +49 (0)30 / 25 93 91 - 602

QCP-w, OVCP, EVCP

Sperrberechtigte können telefonisch sperren, an 24 Stunden am Tag und 7 Tagen der Woche und müssen sich mit ihrem vereinbarten Sperrpasswort authentifizieren.

Sperrnummer: +49 (0)30 / 25 93 91 – 601

Andere Sperrverfahren können vereinbart werden.

Ein Antrag per E-Mail zur Sperrung eines Zertifikats muss eindeutig das zu sperrende Zertifikat beschreiben und muss daher folgende Angaben enthalten:

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

Sperrungen finden im Verantwortungsbereich des TSP statt. Ungeachtet dessen kann der TSP Teilaufgaben an vertraglich gebundene Dritte weiter geben. Die Sperrdienstleistung kann von Dritten übernommen werden, die nach den Maßgaben des TSP handeln.

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

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

Die Authentifizierung der Sperrberechtigten erfolgt gemäß Abschnitt 3.4.

4.9.4 Fristen für einen Sperrantrag

Der Endanwender oder Zertifikatnehmer muss in eigener Verantwortung dafür sorgen, dass er oder eine für ihn sperrberechtigte Person unverzüglich die Sperrung beantragt, sobald Gründe zur Sperrung bekannt werden. Dabei ist dasjenige Verfahren zu nutzen, welches die schnellste Bearbeitung des Sperrantrags erwarten lässt.

4.9.5 Zeitspanne für die Bearbeitung des Sperrantrags durch den TSP

Sperranträge werden vom TSP an bundeseinheitlichen Arbeitstagen in der Zeit von 9 - 17 Uhr bearbeitet. Telefonisch eintreffende Sperranträge werden unmittelbar ausgeführt. Per E-Mail und per Briefpost eintreffende Sperranträge werden spätestens am folgenden Arbeitstag bearbeitet.

QCP-w, EVCP, OVCP

Die Sperrung erfolgt umgehend nach erfolgreicher Autorisierung des Sperrantragstellers per Telefon oder über die Online-Schnittstelle.

LCP

Sperrverlangen über die Onlineschnittstelle werden innerhalb von 24 Stunden umgesetzt.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Aktuelle Sperrinformationen sind in Sperrlisten vorgehalten, die über das Protokoll LDAP oder über den in Abschnitt 2.1 angegebenen Link abgerufen werden können. Zusätzlich steht ein

OCSP-Dienst zur Verfügung. Die Erreichbarkeit dieser Dienste wird in Form von URLs in den Zertifikaten angegeben. Ferner können Sperrinformationen über die Webseite des TSP (siehe Abschnitt 2.1) bezogen werden. Delta-CRLs werden nicht genutzt.

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

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

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Siehe Abschnitt 2.3.

4.9.8 Maximale Latenzzeit für Sperrlisten

Sperrlisten werden unmittelbar nach ihrer Erzeugung veröffentlicht.

4.9.9 Online-Verfügbarkeit von Sperrinformationen

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

4.9.10 Notwendigkeit zur Online-Prüfung von Sperrinformationen

Es gibt keine Pflicht zur Online-Prüfung von Sperrinformationen, es gilt jedoch Abschnitt 4.5.2.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Keine.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Keine.

4.9.13 Bedingungen für eine Suspendierung

Suspendierungen von Zertifikaten werden nicht angeboten.

4.10 Statusabfragedienst für Zertifikate

4.10.1 Funktionsweise des Statusabfragedienstes

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 beschrieben.

Die Systemzeit des OCSP-Responder wird über DCF77 täglich gegen die offizielle Zeit synchronisiert.

4.10.2 Verfügbarkeit des Statusabfragedienstes

Der Statusabfragedienst ist 24 Stunden an 7 Tagen der Woche verfügbar.

4.10.3 Optionale Leistungen

Keine.

4.11 Austritt aus dem Zertifizierungsdienst

Die Gültigkeit eines Zertifikats endet mit dem im Zertifikat vermerkten Termin. Schlüsselerneuerung kann gemäß Abschnitt 3.3 beantragt werden. Der Sperrauftrag zu einem Zertifikat durch Zertifikatnehmer oder Sperrberechtigte Dritte löst die Sperrung durch den TSP aus. Die vertraglichen Hauptleistungspflichten des TSP sind damit vollständig erfüllt.

4.12 Schlüsselhinterlegung und –wiederherstellung

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

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel

Schlüsselhinterlegung wird nicht vom TSP angeboten.

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Schlüsselhinterlegung wird nicht vom TSP angeboten.

5. Nicht-technische Sicherheitsmaßnahmen

Die Beschreibungen dieses Kapitels beziehen sich auf die CAs, die bei der D-TRUST GmbH im Rahmen von [EN 319 411-1] und [EN 319 411-2] betrieben werden.

5.1 Bauliche Sicherheitsmaßnahmen

Für die baulichen Sicherheitsmaßnahmen liegt eine detaillierte Dokumentation vor, die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann. Das Sicherheitskonzept wurde durch eine anerkannte Prüf- und Bestätigungsstelle geprüft. Die Prüfung und Bestätigung wird gemäß [EN 319 411-1] und [EN 319 411-2] regelmäßig wiederholt.

Ferner wurde dem Sicherheitsbereich des Trustcenters der D-TRUST GmbH durch den TÜV-IT die Anwendung und Umsetzung der „Infrastrukturmaßnahmen für hohen Schutzbedarf – Level 3" beurkundet (gemäß Prüfkriterienkatalog für „Trusted Site Infrastructure"). Mit diesem TÜV-IT-Zertifikat „Trusted Site Infrastructure" werden alle Infrastruktur-relevanten Aspekte bewertet. Diese Prüfung wird alle zwei Jahre wiederholt. Das genannte Zertifikat bestätigt der D-TRUST GmbH diesen hohen Sicherheitsstandard der nicht-technischen Sicherheitsmaßnahmen.

Die CAs der hier behandelten CSM-PKI werden vom TSP unter den gleichen Bedingungen betrieben wie die CAs der D-TRUST GmbH zur Ausstellung qualifizierter Zertifikate.

5.2 Verfahrensvorschriften

5.2.1 Rollenkonzept

Teil der Dokumentation ist ein Rollenkonzept, in dem Mitarbeiter einer oder mehreren 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.

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 Vier-Augen-Prinzip durchgeführt werden. Dies wird durch technische und organisatorische Maßnahmen wie beispielsweise Zutrittsberechtigungen und Abfrage von Wissen durchgesetzt.

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

5.2.3 Identifikation und Authentifizierung für einzelne Rollen

Das Rollenkonzept wird durch technische und organisatorische Maßnahmen, wie beispielsweise Zutrittsberechtigungen und Abfrage von Wissen, durchgesetzt. Die durchführende Person muss sich, bevor sie Zugriff auf sicherheitskritische Anwendungen erhält, erfolgreich authentifizieren. Über Event-Logs kann die durchführende Person nachträglich einer Aktion zugeordnet werden; sie ist rechenschaftspflichtig.

5.2.4 Rollenausschlüsse

Das Rollenkonzept sieht diverse Rollenausschlüsse vor, um Interessenskonflikte zu verhindern, das Mehraugenprinzip zu erzwingen und schädliches Handeln vorzubeugen.

5.3 Eingesetztes Personal

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

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

Der TSP gewährleistet, dass die im Bereich des Zertifizierungsdienstes tätigen Personen über die für diese Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen.

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.

5.3.2 Sicherheitsprüfungen

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

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

5.3.3 Schulungen

Der TSP schult Personen, die im Zertifizierungsdienst tätig sind.

5.3.4 Häufigkeit von Schulungen und Belehrungen

Der TSP schult Personen, die im Zertifizierungsdienst tätig sind zu Beginn ihres Einsatzes 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.

5.3.7 Anforderungen an freie Mitarbeiter

Entfällt; freie Mitarbeiter werden nicht eingesetzt.

5.3.8 Ausgehändigte Dokumentation

Umfangreiche Verfahrensanweisungen definieren für alle Produktionsschritte 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 im Produktionsbetrieb nicht abgewichen werden kann.

5.4 Überwachungsmaßnahmen

5.4.1 Überwachung des Zutritts

Der TSP betreibt umfangreiche Überwachungsmaßnahmen (beispielsweise durch Videoüberwachung) zur Absicherung der Zertifizierungsdienstleistungen und deren zugrunde liegenden IT-Systemen und Dokumenten.

Die Überwachungsmaßnahmen werden durch organisatorische Regelungen ergänzt. Beispielsweise sieht die Besucherregelung unter anderem vor, dass Besucher mindestens 24 Stunden vor dem Besuch namentlich angemeldet sein müssen. Im Bereich des Trustcenters müssen Besucher stets in Begleitung eines Mitarbeiters des TSP sein.

5.4.2 Überwachung von organisatorischen Maßnahmen

Ein weiterer Bestandteil ist die Überwachung von organisatorischen Maßnahmen.

Hierzu gehört eine regelmäßige Risikoanalyse, die die Bedrohung für den Betrieb des TSP umfassend analysiert sowie Anforderungen und Gegenmaßnahmen definiert. Ferner ist eine Restrisikoanalyse enthalten, in der die Vertretbarkeit des Restrisikos aufgezeigt und ggf. akzeptiert wird.

Weiterhin werden relevante Assets angemessen erfasst, sowie entsprechende Änderungen dieser Assets überprüft bzw. wenn anwendbar durch das vom Management beauftragte Personal des TSP freigegeben.

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen

Es wird zwischen Aufzeichnungen in elektronischer Form und papierbasierten unterschieden.

Archiviert werden die vollständigen Antragsunterlagen (auch Folgeanträge), Dokumente zu Verfahrensrichtlinien (CP, 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.

Weiterhin werden sicherheitsrelevante Ereignisse entsprechend aufgezeichnet. Die Systemzeit wird über DCF77 täglich gegen die offizielle Zeit synchronisiert.

5.5.2 Aufbewahrungsfristen für archivierte Daten

Dokumente zur Antragstellung und Prüfung sowie die Daten zum Zertifikatslebenszyklus sowie die Zertifikate selbst werden mindestens zehn[2] Jahre und bis zum Jahresende aufbewahrt. Die Frist beginnt nach Ablauf der Gültigkeit des Zertifikates, das zuletzt auf der Basis dieser Dokumente ausgestellt wurde.

Wenn anwendbar, umfasst dies auch die entsprechenden Systemprotokolle, die im Rahmen der genannten Ereignisse entstehen.

[2] Bei SSL-/TLS-Zertifikate: sieben Jahre

Weiterhin werden sicherheitsrelevante Ereignisse entsprechend aufgezeichnet. Die Systemzeit wird über DCF77 täglich gegen die offizielle Zeit synchronisiert.

5.5.3 Sicherung des Archivs

Das Archiv befindet sich in gesicherten Räumen und unterliegt dem Rollen- und Zutrittskontrollkonzept 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].

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 TSP.

5.6 Schlüsselwechsel beim TSP

Eine angemessene Zeit vor Ablauf einer CA werden neue CA-Schlüssel generiert, neue CA-Instanzen aufgesetzt und veröffentlicht.

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.

5.7.2 Wiederherstellung nach Kompromittierung von Ressourcen

Das Sicherheitskonzept beschreibt die Durchführung von Recovery-Prozeduren.

5.7.3 Kompromittierung des privaten CA-Schlüssels

Im Fall einer Kompromittierung oder der Bekanntgabe von Unsicherheit von Algorithmen oder assoziierten Parametern durch die Herausgeber der maßgeblichen Kataloge nach Abschnitt 0, veranlasst der TSP folgendes:

- betroffenen CA-Zertifikate sowie deren ausgestellte und bisher nicht ausgelaufene Zertifikate werden gesperrt,
- involvierte Zertifikatnehmer werden über den Vorfall und dessen Auswirkungen informiert,

- die zuständige Aufsichtsstelle wird 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.

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 Geschäftsweiterführung nach Kompromittierung und Desaster

In einem Notfall entscheidet der TSP je nach Art des Vorfalls, ob ein Recovery des in Abschnitt 0 beschriebene Backups der CA durchgeführt oder bei Kompromittierung gemäß Abschnitt 0 verfahren wird.

5.8 Schließung des TSP

Bei Beendigung der Dienste von CAs informiert der TSP alle Zertifikatnehmer 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 gesperrt. 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 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 wird alle Funktionalität der CAs eingestellt, so dass eine Zertifizierung nicht mehr möglich ist.

D-TRUST verfügt über einen fortlaufend aktualisierten Beendigungsplan.

6. Technische Sicherheitsmaßnahmen

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

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

CA-Schlüssel werden in einem „FIPS 140-2 Level 3" konformen Hardware Security Module (HSM) erzeugt. Das HSM befindet sich im Hochsicherheitsbereich des Trustcenters. Bei der Schlüsselerzeugung wird die Durchsetzung des Rollenkonzepts und somit das 4-Augen-Prinzip erzwungen. Bei der Erzeugung von CA-Schlüsseln ist stets 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 gemäß[EN 319 411-1] bzw. [EN 319 411-2] dokumentiert.

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

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

6.1.2 Lieferung privater Schlüssel an Zertifikatnehmer

Werden die privaten Schlüssel beim TSP erzeugt, werden sie gemäß Abschnitt 4.4.1 zugestellt. In diesem Fall erfolgt die Speicherung der privaten Schlüssel beim TSP bis zur Auslieferung in einer sicheren Umgebungen.

Da keine Schlüsselhinterlegung angeboten wird, wird der private Schlüssel nach der Auslieferung an den Zertifikatnehmer beim TSP gelöscht.

6.1.3 Lieferung öffentlicher Schlüssel an den TSP

Zertifikatsanforderungen können von Zertifikatnehmern zu einem vorhandenem Schlüsselpaar per PKCS#10-Request gestellt werden, der mit dem entsprechenden privaten Schlüssel signiert werden muss. Der PKCS#10-Request enthält den öffentlichen Schlüssel. Die entsprechende Response gibt das vollständige Zertifikat zurück.

6.1.4 Lieferung öffentlicher CA-Schlüssel an Zertifikatnutzer

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

6.1.5 Schlüssellängen

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

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

6.1.6 Festlegung der Schlüsselparameter und Qualitätskontrolle

QCP-w, EVCP, OVCP, LCP

CA- und EE-Zertifikate werden auf Grundlage von Schlüsseln ausgestellt, die [ETSI-ALG] in der aktuell gültigen Fassung entsprechen, soweit Kompatibilität im Verwendungsumfeld gewährleistet ist.

QCP-w, EVCP

CA- und EE-Zertifikate werden ausschließlich auf Grundlage von Schlüsseln ausgestellt, die zusätzlich zu [ETSI-ALG] auch [EN 319 411-1] bzw. [EN 319 411-2] und [GL-BRO] in der aktuell gültigen Fassung entsprechen.

Signatur- und Verschlüsselungsalgorithmus sind im Abschnitt 0 genannt.

6.1.7 Schlüsselverwendungen

Private Root-CA-Schlüssel werden ausschließlich zum Signieren von CA-Zertifikaten und Sperrlisten verwendet. Alle anderen privaten CA-Schlüssel werden zum Signieren von CA-Zertifikaten, 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).

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

Die vom TSP eingesetzten kryptographischen Module funktionieren einwandfrei. 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 evaluiert wurde.

LCP

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

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

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

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

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

6.2.3 Hinterlegung privater Schlüssel (key escrow)

Private EE-Schlüssel werden vom TSP nicht hinterlegt.

6.2.4 Backup privater Schlüssel

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.

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

6.2.5 Archivierung privater Schlüssel

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.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Die privaten CA-Schlüssel liegen verschlüsselt im HSM vor.

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

6.2.8 Aktivierung privater Schlüssel

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

Private EE-Schlüssel werden durch Eingabe des Geheimnisses aktiviert.

6.2.9 Deaktivieren privater Schlüssel

Die privaten CA-Schlüssel werden durch Beendigung der Verbindung zwischen HSM und Anwendung deaktiviert.

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

6.2.10 Zerstörung privater Schlüssel

Nach Ablauf der Gültigkeit der privaten CA-Schlüssel werden diese gelöscht. 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.

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

6.2.11 Beurteilung kryptographischer Module

Der TSP betreibt geeignete hard- und softwarebasierte Schlüsselgeneratoren um die Qualität der EE-Schlüssel zu sichern. Die eingesetzten HSM sind FIPS 140-2 Level 3 konform.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

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

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

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

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

OVCP
Max. 825 Tage

QCP-w, EVCP
Max. 825 Tage

LCP
63 Monate

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

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation von Aktivierungsdaten

Die Aktivierungsdaten der CA-Schlüssel werden durch das HSM abgefragt. PIN-Vergabe erfolgt während der Bootstrap-Prozedur. Ein 4-Augen-Prinzip wird erzwungen.

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

LCP

Erzeugt der TSP die EE-Schlüssel, wird entweder die PIN in einem PIN-Brief an den Zertifikatnehmer versandt bzw. übergeben oder dem Zertifikatnehmer über eine gesicherte SSL-Verbindung bzw. Onlineschnittstelle zur Verfügung gestellt. Der Zertifikatnehmer ist für die sichere Zustellung der PIN an den Endanwender verantwortlich, wenn Zertifikatnehmer und Endanwender voneinander abweichen.

6.4.2 Schutz von Aktivierungsdaten

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

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

6.4.3 Andere Aspekte von Aktivierungsdaten

Nicht anwendbar.

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 zum CPS und [EN 319 411-1] bzw. [EN 319 411-2] und im Fall von EV-Zertifikaten zu [GL-BRO] 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. Abweichungen hiervon werden vom TSP angemessen dokumentiert und ggf. im Risikomanagement des TSP adressiert.

Zertifikatnehmer und Zertifikatnutzer müssen vertrauenswürdige Computer und Software verwenden.

6.5.2 Beurteilung von Computersicherheit

Die für die CA-Schlüssel eingesetzten Computer, Netze und andere Komponenten wurden durch anerkannte Prüf- und Bestätigungsstellen regelmäßig 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 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

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.

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 zweifelsfrei feststeht, dass sie nicht

manipuliert wurden. Durch Versiegelung der Hardware und Softwarechecks beispielsweise werden Manipulationen und Manipulationsversuche bei jeder Aktion oder Revision erkennbar. 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. Ausgetauschte Geräte oder obsolete 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 Sicherheitsbeauftragten 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 regelmäßig durchgeführt. Weiterhin werden regelmäßig Schwachstellenscans veranlasst.

QCP-w, EVCP

Es werden mindesten die in [GL-BRO] geforderten Ereignisse auditierbar geloggt bzw. protokolliert.

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. Für das Netzkonzept liegt eine detaillierte Dokumentation vor, die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann.

Zum Schutz der Prozesse des TSP werden beispielsweise Firewall und Intrusion Detection / Prevention Mechanismen eingesetzt, die nur explizit erlaubte Verbindungen zulassen. Der TSP betreibt Netzsegmente unterschiedlichen Schutzbedarfs und trennt dabei Mitarbeiter- und Internet-nahe 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.

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.

6.8 Zeitstempel

Der TSP betreibt einen Zeitstempeldienst. Zeitstempel werden im Rahmen dieses CPS jedoch nicht angeboten.

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.

7.1.2 Zertifikatserweiterungen

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
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	Adresse(n) der CRL-Ausgabestelle(n)
AuthorityInfoAccess	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	2.5.29.32	OIDs der unterstützten CPs
SubjectAltName	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: *digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, decipherOnly* und Kombinationen

EE-Zertifikate können folgende unkritische Erweiterungen enthalten:

Erweiterung	OID	Parameter
ExtKeyUsage	2.5.29.37	Entsprechend [RFC 5280], [RFC 6818]
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 {…}* *accessMethod= caIssuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}*
certificatePolicies	2.5.29.32	OIDs der unterstützten CPs *cpsURI*
SubjectAltName	2.5.29.17	Alternativer Inhabername
QCStatements (nur QCP-w)	*1.3.6.1.5.5.7.1.3*	esi4-qcStatement-1 {0 4 0 1862 1 1}; esi4-qcStatement-5 {0 4 0 1862 1 5}.

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.

7.1.3 Algorithmen-OIDs

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

- RSA mit OID 1.2.840.113549.1.1.1.
- RSA-PSS mit OID 1.2.840.113549.1.1.10.

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

- SHA512 RSA mit OID 1.2.840.113549.1.1.13,
- SHA256 RSA mit OID 1.2.840.113549.1.1.11.

7.1.4 Namensformate

In den Feldern *subject* (hier: Name des Endanwenders) und *issuer* (Name des Ausstellers) werden Namen nach [X.501] 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 Zertifikatnehmername) und *Issuer-AltName* (Alternativer Ausstellername) können Namen gemäß [RFC 5280], [RFC 6818] (kodiert als IA5String) stehen.

7.1.5 Name Constraints

„NameConstraints" wird nicht benutzt.

7.1.6 Certificate Policy Object Identifier

„CertificatePolicies" kann den OID unterstützter CPs enthalten.

Weitere Regelungen sind in der CP enthalten.

7.1.7 Nutzung der Erweiterung „PolicyConstraints"

„PolicyConstraints" wird nicht benutzt.

7.1.8 Syntax und Semantik von „PolicyQualifiers"

„PolicyQualifiers" können benutzt werden.

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung von CertificatePolicies

In CA- und EE-Zertifikaten ist die Erweiterung *CertificatePolicies* (Zertifikatsrichtlinie) nicht kritisch. Es liegt im Ermessen der Zertifikatnehmer und Zertifikatnutzer, diese Erweiterung auszuwerten.

7.2 Sperrlistenprofile

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

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

7.3 Profile des Statusabfragedienstes (OCSP)

Der OCSP-Responder unterstützt zusätzlich zu RFC 6960 auch Positivauskünfte.

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).

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. Auditierungen und andere Prüfungen

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 wird regelmäßig durch eine unabhängige Prüf- und Bestätigungsstelle geprüft. Bei begründetem Interesse können diese Dokumente in den relevanten Teilen eingesehen werden.

CP und CPS erfüllen für Zertifikate die Anforderungen gemäß [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" gemäß [EN 319 411-1] bzw. [EN 319 411-2] belegt die Kompatibilität.

Der TSP gibt Zertifikate mit einer Policy-OID-Referenz auf [EN 319 411-1] und [EN 319 411-2] erst nach der initialen und erfolgreich abgeschlossenen Prüfung durch einen unabhängigen externen Zertifizierer aus. Es finden regelmäßige Wiederholungsprüfungen statt. Sollten sich die Verfahren als nicht mehr konform zu den aktuellen Richtlinien von [EN 319 411-1] bzw. [EN 319 411-2] erweisen, unterlässt der TSP das Ausstellen o. g. Zertifikate bis die Richtlinienkonformität wiederhergestellt und entsprechend überprüft wurde.

Diese Auditierung findet jährlich statt.

Darüber hinaus finden regelmäßig interne Audits statt.

9. Sonstige finanzielle und rechtliche Regelungen

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