

# Certification Practice Statement of the D-TRUST Root PKI Version 2.0

Date of issue  
Effective date

01/01/2017  
01/01/2017



REGISTERED TRADE  
MARK OF  
BUNDESDRUCKEREI

## Copyright notice

### **Certification Practice Statement of the D-TRUST Root PKI ©2017 D-TRUST GmbH, all rights reserved.**

Notwithstanding the rights reserved in the foregoing and unless permitted below, reproduction, storage or entering into a storage system or transmission of any part of this publication in any manner and using any process whatsoever (electronic, mechanical, photocopy, recording or in any other manner) shall not be permitted without D-TRUST's prior consent.

Notwithstanding the foregoing, reproduction and distribution of this CPS is permitted on a non-exclusive, no-cost basis on condition that (i) the foregoing copyright notice and the introductory paragraphs appear in a prominent position at the beginning of each copy and (ii) this document is repeated literally and completely, beginning with a statement naming D-TRUST GmbH as the author of the document.

Please send any requests for any other approval for reproduction or other use of this CPS of D-TRUST GmbH to:

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

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

## Document history

Version	Date	Description
2.0	01/01/2017	As part of the introduction of qualified products pursuant to EN 319 411-2 and eIDAS, the document version was raised to 2.0. The certificate policy document history up to this point in time can be found in version 1.15 from 3 October 2016.

## Contents

1.	Introduction .....	5
1.1	Overview .....	5
1.2	Name and identification of the document .....	7
1.3	PKI entities .....	7
1.4	Use of certificates .....	9
1.5	Maintenance and updating of the CPS .....	10
1.6	Terminology and abbreviations .....	11
2.	Responsibility for repositories and publications .....	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 .....	14
3.1	Name rules .....	14
3.2	Initial identity verification .....	17
3.3	Identification and authentication of applications for re-keying .....	20
3.4	Identification and authentication of revocation requests .....	20
4.	Operational requirements .....	22
4.1	Certificate application and registration .....	22
4.2	Processing the certificate application .....	23
4.3	Issuance of certificates .....	27
4.4	Certificate handover .....	27
4.5	Use of the key pair and of the certificate .....	29
4.6	Certificate renewal .....	29
4.7	Certificate renewal with key renewal .....	29
4.8	Certificate change .....	30
4.9	Revocation and suspension of certificates .....	30
4.10	Status request service for certificates .....	35
4.11	Withdrawal from the certification service .....	35
4.12	Key depositing and key restoration .....	35
5.	Non-technical security measures .....	36
5.1	Structural security measures .....	36
5.2	Procedural rules .....	36
5.3	Personnel employed .....	37
5.4	Monitoring and surveillance measures .....	38
5.5	Archiving of records .....	39
5.6	Key change at the TSP .....	40
5.7	Compromising and continuation of business on the part of the TSP .....	40
5.8	Closing the TSP down .....	41
6.	Technical security measures .....	42
6.1	Generation and installation of key pairs .....	42
6.2	Securing the private key and requirements for cryptographic modules .....	44
6.3	Other aspects of key pair management .....	46
6.4	Activation data .....	46
6.5	Security measures in the computer systems .....	47
6.6	Technical measures during the lifecycle .....	48
6.7	Security measures for networks .....	49
6.8	Time stamp .....	49
7.	Profiles of certificates, certificate revocation lists and OCSP .....	50
7.1	Certificate profiles .....	50

---

7.2	Certificate revocation list profiles.....	53
7.3	Profiles of the status request service (OCSP) .....	53
8.	Checks and other evaluations.....	55
9.	Other financial and legal provisions .....	56

## 1. Introduction

### 1.1 Overview

This document is the Certification Practice Statement (CPS) of the D-TRUST root PKI operated by D-TRUST GmbH.

#### 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.

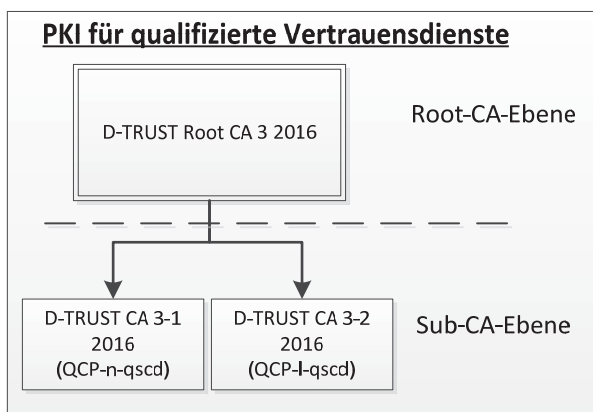
The structure of this document is closely related to the RFC 3647 Internet standard "*Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*", making it easier to read and comparable with other CPSs.

#### 1.1.3 Properties of the PKI

The PKI described here features a multi-level hierarchy. Figs. 1 and 2 show PKI set-ups for qualified and non-qualified trust services. It always consists of a chain which begins with a root CA (root authority or trust anchor) which is optionally

followed by further sub-CAs (intermediate CAs). The last sub-CA of this chain is the issuing CA which issues EE certificates.

### PKI for qualified trust services



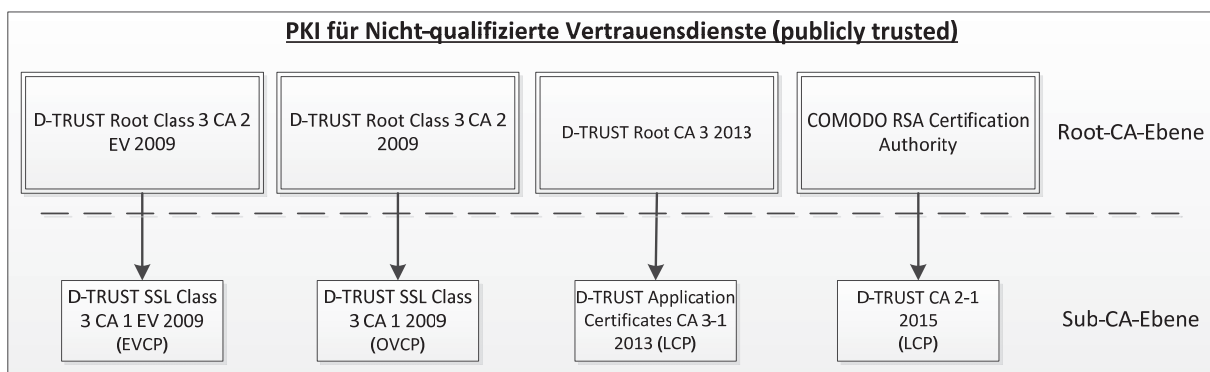
**Fig. 1 PKI hierarchy for qualified trust services**

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

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

### 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 – Organisation 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 EVCP policy level are SSL certificates. The fact that they are EV certificates can be recognised in the EE certificates by the EV policy OID (as described in section 1.2). EV certificates are not issued on smart cards.

OVCP

EE certificates of the OVCP certification level include SSL certificates and machine certificates which include the name of an organisation. 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 LCP certification level are simple personal certificates. In this case too, the name of an organisation can be included as an attribute in the certificate. LCP certificates are not issued on smart cards.

## 1.2 Name and identification of the document

Document name:	Certification Practice Statement of the D-TRUST Root PKI
Version	2.0

## 1.3 PKI entities

### 1.3.1 Certification authorities (CAs)

Certification authorities (CAs) are operated by trust service providers 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.

### 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.

### 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 end-entity'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 organisation
- ▶ 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.

**QCP-n-qscd**

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

**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.

**EVCP, OVCP, QCP-I-qscd**

Seal and SSL/TLS certificates are issued exclusively to legal entities.

**LCP**

Certificates for individuals are also issued if the subscriber and the end-entity are not identical. In this case, both parties are responsible for ensuring compliance with the subscriber agreement.

**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 Use of certificates****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. Relying parties 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<sup>1</sup>

## 1.5 Maintenance and updating of the CPS

### 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, when necessary, 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 CP

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-n-qscd, QCP-l-qscd

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

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]. In the event of inconsistencies between this document and the above-mentioned guidelines, [GL-BRO] has priority.

---

<sup>1</sup> OCSP information is signed using special OCSP service certificates.

## **1.6 Terminology and abbreviations**

### **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. Responsibility for repositories and publications

### 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 if this was requested by the subscriber
- ▶ CA certificates
- ▶ Certificate revocation lists (CRLs) and status information
- ▶ The CP
- ▶ This CPS
- ▶ The subscriber agreement for SSL certificates
- ▶ The subscriber agreement for all other certificates under this policy (general subscriber agreement)
- ▶ PKI user information for qualified trust services

### 2.3 Publication frequency

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

EVCP, OVCP, LCP

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

QCP-n-qscd, QCP-l-qscd

Published EE certificates can be retrieved until the end of their validity term plus at least ten years and until the end of the year.

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

- ▶ at least 10 years (QCP-n-qscd, QCP-l-qscd, 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

### 3.1 Name rules

#### 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.

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

In the case of certificates that were created with pseudonyms too, the TSP 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)	<p><i>Given name(s)</i> of the individual</p> <ul style="list-style-type: none"> <li>- QCP-I-qscd, EVCP, OVCP: This field is not used.</li> <li>- QCP-n-qscd, LCP: according to the proof used for identification</li> </ul>
SN (surname)	<p><i>Surname</i> of the individual</p> <ul style="list-style-type: none"> <li>- QCP-I-qscd, EVCP, OVCP: This field is not used.</li> <li>- QCP-n-qscd, LCP: according to the proof used for identification</li> </ul> <p>If pseudonyms are used, SN corresponds to CN.</p>
CN (common name)	<p><i>Common name:</i> The following variants are used:</p> <ul style="list-style-type: none"> <li>- Individuals without a pseudonym: "family name, name used".</li> <li>- Individuals with a pseudonym: "Pseudonym:PN".</li> <li>- Legal entities: official name of the organisation (company, public authority, association, etc.), if necessary, reduced to a meaningful name if the maximum number of 64 characters is exceeded.</li> </ul> <p>Special case: It is also possible to include one or more domain names in the CN. Wildcards are not permitted for SSL/TLS certificates.</p> <ul style="list-style-type: none"> <li>- 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</li> <li>- Technical components: Name of the server, service or application using the certificate</li> </ul>
PN	<i>Pseudonym:</i> identical to CN.
serialNumber	<p><i>Serial number:</i> Name suffix number to ensure unambiguity of the name (typically the application number).</p> <p>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.</p>
O (organization)	<p>Official name of the subscriber or name of the <i>organisation</i> 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.</p>
OU (organization unit)	<i>Organisation unit</i> (department, division or other unit) of the organisation.



DN component	Interpretation
OrgID (organization identifier)	QCP-I-qscd: <i>Unambiguous organisation number</i> of the organisation. The number of the commercial register as well as the VAT ID number or a number assigned by D-TRUST can be entered.
C (country)	The notation of the country to be stated corresponds to [ISO 3166] and is set up as follows: If an organisation O is listed in the DistinguishedName, the organisation's place of business in the register determines the entry in the certificate. If no organisation O is entered, the country is listed that issued the document that was used to identify the subscriber.
Street	Postal address <i>Street</i>
Locality	Postal address <i>City</i>
State	Postal address <i>(Federal) state</i>
PostalCode	Postal address <i>Postal code</i>
BusinessCategory	Business category (2.5.4.15) according to [GL-BRO]
Jurisdiction Of Incorporation Locality	Jurisdiction of the organisation according to [GL-BRO]: <i>City</i> (1.3.6.1.4.1.311.60.2.1.1)
Jurisdiction Of Incorporation State Or Province Name	Jurisdiction of the organisation: <i>(Federal) state</i> (1.3.6.1.4.1.311.60.2.1.2)
Jurisdiction Of Incorporation CountryName	Jurisdiction of the organisation according to [GL-BRO]: <i>Country</i> (1.3.6.1.4.1.311.60.2.1.3)

EVCP

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

QCP-n-qscd

Qualified certificates for individuals include, as a minimum, the subject DN components: "CommonName", "Country", "subjectSerialNumber" as well as either "GivenName" and "Surname" or "Pseudonym".

#### QCP-I-qscd

Qualified certificates for legal entities include, as a minimum, the subject DN components: "CommonName", "Country", "subjectSerialNumber" and "Organization" as well as "organizationIdentifier".

It is not necessary to use all the DN components mentioned here. Further components can be added. Additional DN components must comply with [RFC 5280] and [Co PKI].

### 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 within this PKI to the same subscriber or subject, respectively.

#### EVCP, OVCP, LCP

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 section 9.5).

#### 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 verification

### 3.2.1 Proof of ownership of the private key

Two cases are distinguished:

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

2. 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 (not applicable to QCP-I-qscd and QCP-n-qscd).

### 3.2.2 Identification and authentication of organisations

Organisations 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 319 411-2] for QCP-I-qscd. 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.

	<b>EVCP</b>	<b>OVCP</b>	<b>QCP-I-qscd</b>
CN	Register/ Non-Register/ Domain	Register/ Non-Register/ Domain	Register / Non-Register
C			
O			
OU	C confirmation/ A confirmation	C confirmation/ A confirmation	n.a.
STREET	Register/ Non-Register	Register/ Non-Register	Register/ Non-Register
L			
State			
PostalCode			
Alternative applicant (SAN)	Domain	Domain	n.a.
All other attributes	C confirmation/ A confirmation/ Dok-Ident/ out-of-band mechanisms/ Register/ Non-Register	A confirmation/ Dok-Ident/ out-of-band mechanisms	n.a.

If the application is submitted on behalf of a legal entity, the representative must (in analogy to the procedure for proving affiliation with the organisation according to section 3.2.3) prove his or her authorisation to this effect and authenticate or if, applicable, identify themselves for qualified seal cards according to QCP-I-qscd.

***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 organisation has authorised 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.

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

**EVCP, OVCP, LCP**

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 alternative names, e.g. LDAP directories, etc. as well as certificate extensions (AdditionalInformation, monetaryLimit, etc.), if any, are not checked for correctness (see also section 4.9.1).

SSL/TLS certificates according to 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 organisation concerned is determined and verified and/or confirmed using procedures according to section 3.2.3.

In the case of organisations, proof of their existence and the applicant's right to represent the organisation 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 Identification and authentication of applications for re-keying**

Re-keying is equivalent to the production of new certificates and, if applicable, tokens and keys for the same end-entity, however, the end-entity's previously validated data and documents that are still valid can be used.

Different procedures can be agreed to on a case-to-case basis and the TSP decides on their implementation if such procedures are not subject to certification according to [EN 319 411-1] or [EN 319 411-2]. The conditions of section 4.7 must be fulfilled.

## **3.4 Identification and authentication of revocation requests**

Revocation authorisation 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 authorised 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 third party authorised to revoke must give the correct password.
- ▶ All written revocation applications are checked against the revocation applicant's signature.
- ▶ Electronic revocation applications submitted via an online interface can be authorised using a secret transmitted via a previously agreed to and secure channel (e.g. SMS TAN).

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. Operational requirements

### 4.1 Certificate application and registration

#### 4.1.1 Application authorisation

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

LCP

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

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. Sub-tasks can be carried out by partners or external providers under a corresponding agreement if such partners or external providers fulfil the requirements of the CP.

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

Prior to completing the registration process, the subscriber receives the CP, CPS and a subscriber agreement and undertakes to abide by the terms and conditions thereof. The documents are published. The subscriber agreement complies with the requirements of [EN 319 411-1] and [EN 319 411-2]. The application also includes the subscriber's consent to the certificates being published or not. 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. The subscriber is always the subject of the certificate. 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 Processing the certificate application

### 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 organisations 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 authorised 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.

#### **eID**

Individuals with their place of residence in Germany authenticate themselves using a valid, official electronic ID function. Accepted documents are German ID cards or electronic residence permits issued by the Federal Republic of Germany with an electronic ID function. Documents used as proof are filed.

#### **Dok-Ident**

The contents to be verified are compared to the application data on the basis of copies (printed copies or electronically scanned documents or fax transmissions). An out-of-band mechanism 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 organisations) or registers organised under private law (DUNS, comparable business databases, government bodies organised 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.

### **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 organisation (subscriber) and stipulates that only valid data is to be transmitted which meets with the requirements of the CP. An authorised employee or representative of an organisation forwards extracts from the organisation's human resource database and/or requests generated on the basis of such data to the TSP via a secure communication channel. The organisation 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. The following items are filed:

- ▶ electronic or printed copies of the data transmitted,
- ▶ confirmation/proof of the forwarder as the organisation's "authorised employee" or "authorised representative", respectively,
- ▶ proof that such data was made available by an authorised 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 authorised signatory of the organisation confirms certificate-relevant information. This is carried out in writing, with the possibility of electronically

signed confirmation being accepted in individual cases. The authorisation to sign must become apparent either from the proof of existence of the organisation, or it must be proven in another suitable manner. Documents used as proof are filed. It can be agreed that documents used as proof are to be filed by the RA.

### **A confirmation**

Authorised employees or representatives within an organisation or trusted third parties (for instance, partners of the TSP or government bodies) confirm certain certificate-relevant information which they are authorised 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 organisations 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 organisation 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 organisation can also be verified by way of a verification letter "by registered mail with acknowledgement of receipt" to the organisation 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 organisation, 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 CP. An authorised 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**

The domain of an organisation and, if applicable, other attributes such as e-mail addresses are verified by a domain query in official registers (WHOIS and/or RDAP).

#### **OVCP, LCP**

A check is carried out as to whether the subscriber is entitled to use the domain.

#### **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.

### **E-mail**

#### **EVCP, OVCP, LCP**

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

#### **QCP-n-qscd**

E-mail addresses from individuals are not checked.

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.

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 for correctness. 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.

#### **4.2.3 Deadlines for processing certificate applications**

Not applicable

### **4.3 Issuance of certificates**

#### **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.

#### **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 handover**

#### **4.4.1 Procedure during certificate handover**

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

LCP

Soft PSEs whose private key was produced in the area of the TSP are sent, as requested by the subscriber, on a storage medium (by mail to the address shown in the application), made available for access-protected and SSL-

encrypted download or sent by e-mail (the PKCS#12 file being protected by a PIN).

#### EVCP, OVCP, LCP

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. Following revocation, the TSP can demand that the subscriber send the smart cards back to the TSP.

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 CP. Otherwise the relevant rules for remedial measures according to the applicable General Terms and Conditions [AGB] are applicable to defects and their existence.

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

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

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**

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

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

Third parties authorised 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 organisation or the party authorised to request revocation.

## 4.5 Use of the key pair and of the certificate

### 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.

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 this 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 subscriber and found to be compatible.

## 4.6 Certificate renewal

The rules laid down in sections 4.7 and 3.3 apply.

### 4.7 Certificate renewal with key renewal

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.

#### **4.7.2 Authorisation for certificate renewal**

Each subscriber who is authorised (pursuant to section 4.1.1) to submit a certificate application can apply for certificate renewal if the TSP offers a corresponding procedure for the chosen product.

#### **4.7.3 Processing an application for certificate renewal**

The rules laid down in section 4.3 apply.

#### **4.7.4 Notification of the subscriber concerning 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 rules laid down in section 4.3 apply.

#### **4.7.6 Publication of the certificate renewal by the TSP**

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

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

The rules laid down in section 4.4.3 apply.

### **4.8 Certificate change**

Certificate changes are not offered.

### **4.9 Revocation and suspension of certificates**

#### **4.9.1 Conditions for revocation**

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

#### QCP-n-qscd, QCP-l-qscd, EVCP

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

Subscribers or third parties concerned are called upon to immediately 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 organisation).

A certificate is revoked in the following cases:

- ▶ when requested by the subscriber and/or the third party concerned (for instance, the organisation 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,
- ▶ the key pair is on a signature card that contains other keys that are revoked,
- ▶ weaknesses are detected in the encryption algorithm used which constitute serious risks for the permitted applications during the certificate lifecycle,
- ▶ the hardware and software used show security shortcomings which constitute serious risks for the permitted applications during the certificate 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

The TSP operates an EV reporting unit according to [GL-BRO] to which PKI entities or software manufacturers can send, on a 24/7 basis, complaints, voice suspicion regarding cases of compromising of private keys of EV



certificates, report cases of misuse of EV certificates as well as cases of fraud and conduct in violation of the rules for EV certificates.

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

Suspected misuse of D-TRUST EV certificates can be reported to the following e-mail address:

reporting@d-trust.net.

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

Parties authorised to request revocation must identify themselves according to section 3.4.

#### 4.9.2 Authorisation for revocation

The TSP is authorised to revoke certificates.

Subscribers are always authorised 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 authorised 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 authorised to request revocation can be specified and will then always be authorised to request revocation of these certificates.

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

#### 4.9.3 Revocation request procedure

A revocation request can be generally submitted by post. If a revocation password was agreed to, revocation requests can be submitted by e-mail or by phone.

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

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

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

Parties authorised to request revocation can do so by phone on a 24/7 basis after authentication using 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.

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

#### **4.9.4 Revocation request deadlines**

The subject or subscriber is solely responsible for ensuring that they or a person authorised 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-n-qscd, QCP-l-qscd, EVCP, OVCP, LCP

Revocation is carried out following successful authorisation of the party requesting revocation by telephone or SMS TAN.

#### **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 Status request service for certificates

### 4.10.1 Operation of the status request service

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

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

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 Withdrawal from the certification service

The validity of the certificate ends on the date shown in the certificate. Key renewal can be applied for according to section 3.3.1. The request to revoke a certificate by a subscriber or party authorised to request revocation leads to revocation by the TSP. The TSP's main contractual duties are thereby completely fulfilled.

## 4.12 Key depositing and key restoration

A request can be submitted to deposit private EE keys.

According to EN 319 411-1 and EN 319 411-2, the TSP does not offer to deposit keys for certificates. 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 subscriber must apply for the key(s) to be deposited and state that the private EE key is to be re-used to create certificates for the same subscriber, subject or a certain group of individuals.

If EE keys according to 6.2.3 are to be re-used, the subscriber must prove that he is authorised to re-use these keys.

### 4.12.2 Conditions and procedures for depositing and restoring session keys

Session keys are not offered.

## 5. Non-technical security measures

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 Structural security measures

Detailed documentation is available for structural security measures 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 measures.

The CAs of the 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 rules

#### 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 authorisations in a managed process. The authorisations of the individual roles are limited to those authorisations which these roles need to fulfil their tasks. The assignment of authorisations is revised by security management on a regular basis, and authorisations 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 organisation 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 organisational measures, such as access authorisation and verification of knowledge.

## 5.2.3 Identification and authentication for individual roles

The role concept is ensured by technical and organisational measures, such as access authorisation 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 behaviour.

## 5.3 Personnel employed

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 Measures 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 Monitoring and surveillance measures**

#### **5.4.1 Monitoring access**

The TSP implements comprehensive surveillance measures (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 measures are supplemented by organisational 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 organisational measures**

Monitoring organisational measures is 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 counter-measures. 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 Archiving of records**

### **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.

### **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<sup>2</sup> years and until the end of the year<sup>3</sup>. 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.

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.

### **5.5.3 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. 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].

---

<sup>2</sup> In the case of SSL/TLS certificates: seven years

<sup>3</sup> If the token contains, in addition to the non-qualified certificates of the root PKI, further end-entity certificates (qualified certificates or qualified certificates with provider accreditation), the filing periods of such certificates will then apply.



### **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 change at the TSP**

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

## **5.7 Compromising and continuation of business on the part of the TSP**

### **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 Closing the TSP down**

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.

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 measures

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 Generation and installation of key pairs

#### 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.

EVCP, OVCP, LCP

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].

QCP-l-qscd, QCP-n-qscd

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

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

#### 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

EVCP, OVCP, LCP

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

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.

##### 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] and [GL-BRO] in their latest applicable version.

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

EE certificates are exclusively issued on the basis of keys that comply with both [ETSI-ALG] and [EN 319 411-2] 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 Securing the private key and requirements for cryptographic modules

### 6.2.1 Standards and security measures 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 organisational measures.

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.

EVCP, OVCP

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 authorised 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 CA and EE keys that meet the requirements of [EN 319 411-1] or [EN 319 411-2] are not deposited.

A request can be submitted to deposit other private EE keys. The keys are encrypted and stored in the trust service provider's high-security area and can only be decrypted by authorised individuals. Other options for depositing keys can be agreed to individually with the customer.

### 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 authorised 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 authorised persons. Further copies of the private CA key 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.

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 authorised roles and for the permitted types of use (*keyCertSign*, *cRLSign*).

Private EE keys are activated by entering the PIN.

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

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

#### **6.2.10 Destruction of private keys**

The 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 card chip is destroyed or the files containing the private EE key are deleted, the private key is then also destroyed. Destruction of keys deposited with the TSP (according to section 4.12.1) can be requested.

### 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  
39 months,

EVCP  
27 months,

LCP  
63 months.

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

If a certificate is issued for a period of more than 24 months, after this period, the customer bears 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.

EVCP, OVCP, LCP

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

If the TSP generates the keys, either a transport PIN process is used or the PINs are printed as a PIN letter that is sent or handed over to the subscriber.

#### **6.4.2 Protection of activation data**

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

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

#### **6.4.3 Other aspects of activation data**

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

### **6.5 Security measures in the computer systems**

#### **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 CP 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 perimeteric 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 checked, inspected and audited by recognised inspection and certification bodies and are suitably monitored in accordance with [EN 319 401].

## 6.6 Technical measures during the lifecycle

### 6.6.1 Security measures 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 measures in conjunction with computer management

Administration of computers, networks and other components is strictly limited to personnel authorised 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 measures 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 to the TSP manager. 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.

#### EVCP

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

### 6.7 Security measures for networks

A network concept is implemented at the CAs that ensures that the relevant CA systems are operated in particularly well-protected network zones. 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 organisational 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.

The security concept was audited by TÜV Informationstechnik GmbH as the audit and certification body accredited by the Federal Network Agency.

### 6.8 Time stamp

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

## 7. Profiles of certificates, certificate revocation lists and OCSP

### 7.1 Certificate profiles

#### 7.1.1 Version numbers

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

#### 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
<i>KeyUsage</i>	2.5.29.15	<i>keyCertSign</i> , <i>cRLSign</i>
<i>BasicConstraints</i>	2.5.29.19	<i>Ca=TRUE</i> , <i>(pathLenConstraint)</i>

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

Extension	OID	Parameter
<i>AuthorityKeyIdentifier</i>	2.5.29.35	160-bit SHA-1 hash of the issuer key
<i>SubjectKeyIdentifier</i>	2.5.29.14	160-bit SHA-1 hash of the subject public key
<i>CRLDistributionPoints</i>	2.5.29.31	Address(es) of the CRL issuing authority/authorities
<i>AuthorityInfoAccess</i>	1.3.6.1.5.5.7.1.1	<i>accessMethod=OCSP</i> <i>{1.3.6.1.5.5.7.48.1}</i> , <i>accessLocation {...}</i>  <i>accessMethod=caIssuer</i> <i>{1.3.6.1.5.5.7.48.2}</i> , <i>accessLocation {...}</i>
<i>certificatePolicies</i>	2.5.29.32	OIDs of the CPs supported
<i>SubjectAltName</i>	2.5.29.17	Alternative holder's name

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

EE certificates contain the following *critical* extensions:

Extension	OID	Parameter
<i>KeyUsage</i>	2.5.29.15	Possible are: <i>digitalSignature</i> , <i>contentCommitment</i> , <i>keyEncipherment</i> , <i>dataEncipherment</i> , <i>keyAgreement</i> , <i>encipherOnly</i> , <i>decipherOnly</i> and combinations thereof

EE certificates can include the following non-critical extensions:

Extension	OID	Parameter
<i>ExtKeyUsage</i>	2.5.29.37	Corresponding to [RFC 5280]
<i>AuthorityKeyIdentifier</i>	2.5.29.35	160-bit SHA-1 hash of the issuer key
<i>SubjectKeyIdentifier</i>	2.5.29.14	160-bit SHA-1 hash of the subject public key
<i>CRLDistributionPoints</i>	2.5.29.31	CRL issuing authority as ldap address
<i>AuthorityInfoAccess</i>	1.3.6.1.5.5.7.1.1	<i>accessMethod=OCSP</i> <i>{1.3.6.1.5.5.7.48.1}</i> , <i>accessLocation {...}</i>  <i>accessMethod= caIssuer</i> <i>{1.3.6.1.5.5.7.48.2}</i> , <i>accessLocation {...}</i>
<i>certificatePolicies</i>	2.5.29.32	OIDs of the CPs supported <i>cpsURI</i>
<i>SubjectAltName</i>	2.5.29.17	Alternative holder's name
<i>QCStatements (QCP-n-qscd and QCP-l-qscd only)</i>	<i>1.3.6.1.5.5.7.1.3</i>	<i>esi4-qcStatement-1</i> {0 4 0 1862 1 1}; <i>esi4-qcStatement-6</i> : <i>id-etsi-qct-esign</i> {0 4 0 1862 1 6 1} for QCP-n-qscd, <i>id-etsi-qct-eseal</i> {0 4 0 1862 1 6 2} for QCP-l-qscd; <i>esi4-qcStatement-5</i> {0 4 0 1862 1 5}; <i>esi4-qcStatement-4</i> {0 4 0 1862 1 4}; <i>esi4-qcStatement-2</i> {0 4 0 1862 1 2};

Further extensions can be added; they must comply with [X.509], [RFC 5280] 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.

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,
- ▶ SHA1 RSA with OID 1.2.840.113549.1.1.5.

SHA1 is not used if the CA or EE certificates are subject to certification in accordance with EN 319 411-1 or EN 319 411-2.

### 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] (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 Certificate revocation list profiles

### 7.2.1 Version number(s)

Certificate revocation lists v2 according to [RFC 5280] 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
<i>cRLNumber</i>	2.5.29.20	Number of the certificate revocation list
<i>AuthorityKeyIdentifier</i>	2.5.29.35	160-bit SHA-1 hash of the issuer key

## 7.3 Profiles of the status request service (OCSP)

In addition to RFC 2560, the OCSP responder also supports positive information.

### 7.3.1 Version number(s)

OCSP v1 according to [RFC 2560] is used.

### 7.3.2 OCSP extensions

The OCSP responder supports the extension shown below for queries:

Extension	Parameter
<i>RetrieveIfAllowed</i>	If set, the certificate is delivered in the response (optional).

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

<b>Extension</b>	<b>Parameter</b>
<i>ArchiveCutoff</i>	Period of time for which the OCSP responder makes the status information available after issuance of the certificate.
<i>CertHash</i>	In the case of the good or revoked status, the SHA-1 hash value of the certificate is entered.
<i>CertInDirSince</i>	Time of publication of the certificate in the central repository service.
<i>RequestedCertificate</i>	Contains the certificate if <i>RetrieveIfAllowed</i> was set.

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

## 8. Checks and other evaluations

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 according to [EN 319 411-1] or [EN 319 411-2] 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], 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 financial and legal provisions

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