Certificate Policy of D-TRUST GmbH

ENGLISH

DEUTSCH

Teil der Bundesdruckerei-Gruppe

Certificate Policy (CP) of D-Trust GmbH
Version 4.5

Teil der Bundesdruckerei-Gruppe

COPYRIGHT NOTICE AND LICENSE

Certificate Policy of D-Trust GmbH
©2023 D-Trust GmbH

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

All other rights reserved.

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

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

The English version is a translation, the contents of which match the German version of the CP.
Please note that only the German version of this CP is authoritative.

Document History

Version	Date	Description
2.0	2015-02-23	▪ As part of the reorganization of the Certificate Policy of D-Trust GmbH, the document version was raised to 2.0. The Certificate Policy document history up to this point in time can be found in version 1.12 from 17 November 2014. ▪ Contents that refer to specific implementation have been shifted to the respective CPS. Each certificate clearly shows the CPS under which the certificate in question was created.
2.1	2015-10-05	▪ Editorial changes and reference to certificates without a CPS entry
2.2	2016-10-03	▪ Change to EN 319 411-1
3.0	2017-01-01	▪ Introduction of qualified products according to EN 319 411-2 and eIDAS
3.1	2017-04-01	▪ Introduction of a qualified time-stamp service according to EN 319 421
3.2	2017-10-01	▪ Editorial changes and reference to the German Trust Services Act (VDG)
3.3	2018-03-28	▪ Editorial changes and adaptation to Mozilla Root Store Policy 2.5 ▪ Adaptation of the use license to "Creative Commons Attribution" ▪ Addition of OID for the PKI of E.ON SE and Uniper
3.4	2018-05-08	▪ Adaptation of section 9.4 to the amended data protection legislation of 25 May 2018.
3.5	2018-07-05	▪ Addition of OID for the telematics infrastructure for the health sector (HPC) ▪ Adaptation to the requirements of the Baseline Requirements of the CA/Browser Forum, version 1.5.7, 29 April 2018
3.6	2018-10-11	▪ Section 1.5.2 updated according to Ballot SC6 (Part 2)
3.7	2018-11-30	▪ This CP complies with the requirements of Mozilla Policy 2.6.1 ▪ Full annual review of the CP ▪ Editorial changes
3.8	2019-05-15	▪ Addition of PSD2-specific abbreviations ▪ Full annual review of the CP ▪ Editorial changes
3.9	2019-05-22	▪ Addition of the qualified seal certificate with PSD2 extension without QSCD in section 1.1.3
3.10	2019-10-23	▪ Change in sales processes for trust services ▪ Section 2.5 amended ▪ Addition of OID for the Device PKI CPS in section 1.1.3 ▪ Editorial changes
3.11	2020-03-19	▪ Introduction of domain-validated TLS certificates (DVCP) according to EN 319 411-1 and BRG ▪ Full annual review of the CP ▪ Section 2.5: Reference to WCAG guideline ▪ This CP complies with the requirements of BRG 1.6.7 and Mozilla Policy 2.7
3.12	2020-04-28	▪ Integration of new sub-CAs for issuing EV and OV certificates, see section 1.1.3. ▪ Introduction of certificates for the administration PKI (V-PKI)

Version	Date	Description
3.13	2020-06-17	▪ More detailed information in section 1.5.2 and additional information in section 1.6.2.
3.14	2020-08-20	▪ Introduction of an OID for administration-PKI (V-PKI) certificates in section 1.1.3
4.0	2020-11-10	▪ Introduction of a high-level Practice Statement (TSPS, V1.0) for the following CPS documents: CSM CPS, Root CPS and Cloud CPS, see section 1.1.2 ▪ Amendments in section 9
4.1	2021-04-23	▪ Introduction of the new D-TRUST OV OID in section 1.1.3 ▪ Addition of the CA/Browser Forum OIDs for the policy level of TLS certificates ▪ References updated in section 1.6.3 ▪ Full annual review of the CP
4.2	2021-06-18	▪ Update in the context of the BR Self Assessment ▪ Additional information in sections 9.6, 9.9 and 9.16
4.3	2022-04-14	▪ Informative introduction of the NCP policy level ▪ Renaming of the QCP-w policy level to QEVCP-w and introduction of the QNCP-w policy level ▪ Full annual review of the CP
4.4	2022-11-14	▪ References updated in section 1.6.3 ▪ Additional information in section 1.4.2 ▪ Editorial changes
4.5	2023-02-14	▪ Introduction of a new OID in section 1.1.3 ▪ Editorial changes ▪ Adaptation of the BRG and EVGL version in section 1.6.3

Contents

1. Introduction 6
1.1 Overview 6
1.2 Document name and identification 10
1.3 PKI entities 10
1.4 Certificate usage 11
1.5 Policy administration 12
1.6 Definitions and acronyms 13
2. Publication and Repository Responsibility 20
2.1 Repositories 20
2.2 Publication of certificate informatio333n 20
2.3 Publication frequency 20
2.4 Repository access control 20
2.5 Access to and use of services 20
3. Identification and Authentication 21
4. Operational Requirements 21
5. Facility, Management and Operational Controls 21
6. Technical Security Controls 21
7. Profiles of Certificates, Certificate Revocation Lists and OCSP 21
7.1 Certificate profiles 21
7.2 CRL profiles 21
7.3 OCSP profiles 21
8. Compliance Audit and Other Assessments 22
9. Other Business and Legal Matters 22
9.1 Prices 22
9.2 Financial responsibilities 22
9.3 Confidentiality of business data 23
9.4 Protection of personal data 23
9.5 Industrial property and copyrights 24
9.6 Representations and guarantees 24
9.7 Disclaimers 26
9.8 Limitations of liability 26
9.9 Damages 27
9.10 Validity of the CP and termination of validity 28
9.11 Individual communications to and agreements with PKI entities 28
9.12 Amendments 28
9.13 Dispute resolution provisions 29
9.14 Reporting security incidents with certificates 29
9.15 Place of jurisdiction 29
9.16 Miscellaneous provisions 29
9.17 Other provisions 30

1. Introduction

1.1 Overview

This document describes the Certificate Policy (hereinafter referred to as CP) of the trust services operated by D-Trust GmbH.

1.1.1 Trust service provider (TSP)

The trust service provider (TSP) – also in the legal sense – is

D-Trust GmbH
Kommandantenstr. 15
10969 Berlin.

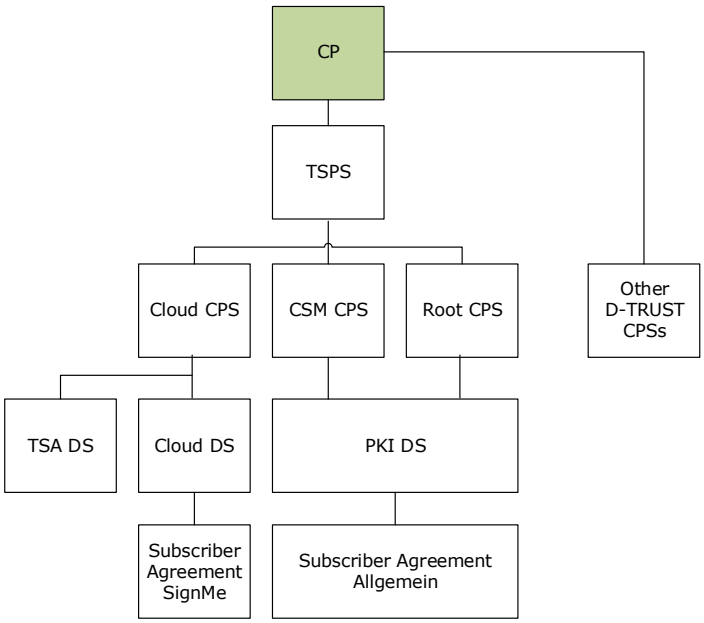
The TSP can outsource sub-tasks to partners or external providers.

The TSP, represented by its management or their agents, is responsible for compliance with the procedures as contemplated in this document and/or any statutory or certification-related requirements for the TSP.

D-Trust GmbH also issues certificates for its own purposes while complying with the relevant statutory or certification-related requirements.

1.1.2 About this document

The following diagram shows the document hierarchy used by D-Trust GmbH. The green marking highlights the document which you are currently reading. At present, the three CPSs named are subject to the TSPS. Other CPSs are directly subject to the CP. They will be gradually added below the TSPS.



This CP contains the requirements for the PKI and hence determines the certification process during the entire term of the end-entity certificates (EE certificates) as well as interaction between and the rights and obligations of PKI entities[1].

The complete CP 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. As regards warranties or representations, this CP contains only the warranties or representations expressly granted for this area.

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

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

1.1.3 Properties of the PKI and notation

These rules are described in the Certification Practice Statement (CPS) that belongs to the certificate.

Under this policy, D-Trust GmbH offers various products that meet the requirements of the Certificate Policy in terms of their special product properties. Whenever possible, services are offered as barrier-free services.

Compliance with these requirements is described in a CPS which can be assigned to a product or product group.

D-Trust GmbH uses several CPS documents. Which CPS belongs to which certificate can be found in the "cpsURI" field in each end-entity certificate.

Trust services that are also called "qualified" are qualified trust services within the meaning of eIDAS. Trust services that are not called "qualified" are non-qualified trust services within the meaning of eIDAS.

If no CPS is stored in the certificate in question, the TSP decides on the implementation of the rules required in this CP. Certificates which do not contain a CPS are <u>not</u> subject to certification within the meaning of EN 319 411-1, EN 319 411-2 or eIDAS.

Services that are operated with certificates without a CP (PolicyOID) and/or CPS entry (cpsURI) are <u>not</u> trust services in the real sense within the meaning of eIDAS, but are services for technical processes.

The OID entered shows that the certificate belongs to this policy:

Qualified personal certificates on a qualified signature creation device
The following D-Trust OID is assigned for certificates of certification class EN 319 411-2 QCP-n-qscd: 1.3.6.1.4.1.4788.2.150.1

[1] This footnote is only relevant for the German version.

Qualified certificates for the health-sector telematics infrastructure
The following D-Trust OID is assigned for certificates of certification class EN 319 411-2 QCP-n-qscd: 1.3.6.1.4.1.4788.2.211.1

Qualified seal certificates on a qualified signature creation device
The following D-Trust OID is assigned for certificates of certification class EN 319 411-2 QCP-l-qscd: 1.3.6.1.4.1.4788.2.150.2

Qualified seal certificates without a qualified signature creation device
The following D-Trust OID is assigned for certificates of certification class EN 319 411-2 QCP-l: 1.3.6.1.4.1.4788.2.150.5

Qualified website certificates (TLS)
The following D-Trust OID is assigned for certificates of certification class EN 319 411-2 QEVCP-w[2]: 1.3.6.1.4.1.4788.2.150.4

The following D-Trust OID is assigned for certificates of certification class EN 319 411-2 QNCP-w : 1.3.6.1.4.1.4788.2.150.3

For PTC website certificates (TLS)
The D-Trust EV OID is assigned for EV certificates in accordance with EN 319 411-1 and [EVGL]: 1.3.6.1.4.1.4788.2.202.1

CA/Browser Forum EV OID: 2.23.140.1.1

The D-Trust OID is assigned for EV certificates from the sub-CA "VR IDENT EV SSL CA 2020" according to EN 319 411-1 and [EVGL]: 1.3.6.1.4.1.4788.2.230.1[3]

CA/Browser Forum EV OID: 2.23.140.1.1

The D-Trust OID is assigned for OV certificates in accordance with EN 319 411-1: 1.3.6.1.4.1.4788.2.200.1 The following D-TRUST policy OID is assigned to all OV certificates from the sub-CA "TRUST BR CA CA 1-20-1 2020" according to EN 319 411-1: 1.3.6.1.4.1.4788.2.202.2

CA/Browser Forum OV OID: 2.23.140.1.2.2

The D-Trust OID is assigned for OV certificates from the sub-CA "VR IDENT SSL CA 2020" according to EN 319 411-1: 1.3.6.1.4.1.4788.2.230.2[4]

CA/Browser Forum OV OID: 2.23.140.1.2.2

The D-Trust OID is assigned for DV certificates in accordance with EN 319 411-1 and BRG: 1.3.6.1.4.1.4788.2.202.3

CA/Browser Forum DV OID: 2.23.140.1.2.1

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

[3] The "VR IDENT EV SSL CA 2020" sub-CA has been revoked.

[4] The "VR IDENT SSL CA 2020" sub-CA has been revoked.

For PTC certificates
The following D-Trust OID is assigned for certificates of certification class EN 319 411-1 LCP: 1.3.6.1.4.1.4788.2.200.2

The following D-Trust OID is assigned for certificates of certification class EN 319 411-1 NCP: 1.3.6.1.4.1.4788.2.200.3

The following D-Trust OID is assigned for certificates of E.ON SE PKI certification class EN 319 411-1 LCP: 1.3.6.1.4.1.4788.2.210.1

The following D-Trust OID is assigned for certificates of E.ON SE PKI certification class EN 319 411-1 NCP: 1.3.6.1.4.1.4788.2.210.2

The following D-Trust OID is assigned for certificates of Uniper PKI certification class EN 319 411-1 LCP: 1.3.6.1.4.1.4788.2.212.1

The following D-Trust OID is assigned for certificates of Uniper PKI certification class EN 319 411-1 NCP: 1.3.6.1.4.1.4788.2.212.2

Advanced certificates of the Cloud PKI
The private keys for certificates from the Cloud PKI remain in the protected environment of the trust service provider. The following OIDs are additionally assigned for such certificates.

The following D-Trust OID is additionally assigned for certificates of certification class EN 319 411-1 LCP: 1.3.6.1.4.1.4788.2.200.2

Qualified certificates of the Cloud PKI
The private keys for certificates from the Cloud PKI remain in the protected environment of the trust service provider. The following OIDs are additionally assigned for such certificates.

The following D-Trust OID is additionally assigned for certificates of certification class EN 319 411-2 QCP-n-qscd: 1.3.6.1.4.1.4788.2.100.1

The following D-Trust OID is additionally assigned for certificates of certification class EN 319 411-2 QCP-l-qscd: 1.3.6.1.4.1.4788.2.100.2

The following D-Trust OID is additionally assigned for the qualified time-stamp service according to EN 319 421 BTSP: 1.3.6.1.4.1.4788.2.100.3

Advanced certificates (Fortgeschrittene Zertifikate)

The policy OID 0.4.0.127.0.7.3.6.1.1.4.4 is assigned by BSI and the policy OID 1.3.6.1.4.1.4788.2.201.2 is assigned by D-Trust to certificates of the V-PKI (Administration PKI) of certification class TR-03145-1

The following D-Trust OID is assigned for machine certificates of certification class TR-03145: 1.3.6.1.4.1.4788.2.400.1.

The following D-Trust OID is assigned for certificates without a certification class: 1.3.6.1.4.1.4788.2.500[5,6]

For certificates without a certification class with inherited properties from certified products[7]

For personal certificates with inherited properties from certified products, the following D-Trust Policy OID is assigned: 1.3.6.1.4.1.4788.2.600.1

The following D-Trust OID is assigned for certificates that are issued exclusively for test purposes: 1.3.6.1.4.1.4788.2.2.2[5]

Certificates that have the properties of a product or a product group of the previously listed policies are available at the following link:

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

1.2 Document name and identification

Document name:	Certificate Policy of D-Trust GmbH
Identifier (OID):	This document has the D-Trust OID: 1.3.6.1.4.1.4788.2.200.1
Version	4.5

1.3 PKI entities

1.3.1 Certification authorities (CAs)

Certification authorities (CAs) issue both certificates and certificate revocation lists. The following types of certificates are possible:

- Personal certificates for natural persons (EE certificate)
- Seal certificates for legal entities (EE certificate)
- Group certificates for groups of individuals, functions and IT processes (EE certificate)
- Certificates for web servers (TLS certificates/EE certificate) that serve a technical purpose but which can also suitably authenticate the end-entity (subject) system
- Certificates for devices or machines that serve a purely technical purpose. Certificate contents are not verified in this case.

[5]These are certificates that are used purely for technical applications or for test purposes. These are hence NOT trust services within the meaning of eIDAS.

[6] This OID can include other service-specific sub-levels.

[7] Certificates with these OIDs are always issued in conjunction with other certified products. For both certificates, certain properties (for instance, distinguished name) are used unchanged and the same procedures (for instance, application, identification process) are used.

- Certification authorities (lower-level CA certificates of the TSP)
- Service certificates for legal entities (EE certificates as well as service certificates for time stamps) under which also the qualified time stamp is issued.

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.

In its capacity as a TSP, the certification authority operates services as contemplated in Chapter III of Regulation (EU) No 910/2014 in conjunction with (52) of the recitals (service for remote signatures).

1.3.2 Registration authorities (RAs)

These rules are described in the CPS that belongs to the certificate.

1.3.3 Subscribers and end-entities (EEs)

These rules are described in the CPS that belongs to the certificate.

1.3.4 Relying parties (RPs)

Relying parties are natural persons or legal entities using the certificates of D-Trust GmbH and having access to the services of the TSP.

1.4 Certificate usage

1.4.1 Permitted certificate usage

Certificates that are subject to this Certificate Policy can be generally used for all purposes. The subscriber is responsible for using the certificates in such a manner that their use complies with the applicable statutory provisions. This applies in particular to adherence to the applicable export and import regulations.

Other rules are described in the CPS that belongs to the certificate.

1.4.2 Forbidden certificate usage

Certificates may not be used for services or systems that, in the case of disruption or failure, lead to considerable tangible or intangible damage or danger to life and limb.

This includes, for instance, nuclear power plants, chemical production plants or aviation systems and especially services and systems related to critical infrastructures.

Deviating provisions can be agreed to in writing with the trust service provider and on a case-to-case basis.

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

1.4.3 Service certificate usage

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

The types of use include:

- CA certificates for CA and certificate issuance

- Signing status information[8]
- Signing time stamps[9]

1.5 Policy administration

1.5.1 Responsibility for the document

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

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

Contact details:

D-Trust GmbH
CP and CPS editorial unit
Kommandantenstr. 15

10969 Berlin, Germany

Phone: +49 (0)30 259391 0
E-mail: info@d-trust.net

1.5.2 Reporting security incidents with certificates

The subscriber should revoke the certificate in the fastest way possible. The fastest way for the subscriber to revoke a certificate is to use unambiguous authentication via the online interface.

The TSP provides the following contacts for reporting security incidents with certificates (e.g. in the event of suspected misuse):

EVCP, OVCP, DVCP, QEVCP-w, and QNCP-w (TLS certificates)

The following website is available to report problems with TLS certificates and CA certificates that are suitable for issuing TLS certificates:

https://www.d-trust.net/en/support/reporting-certificate-problem

The "Certificate Problem Report" form must be used to report and describe the security incident with certificates.

Within 24 hours of receiving the Certificate Problem Report, D-Trust GmbH will contact both the issuer of the Certificate Problem Report and the subscriber (preliminary report). The Certificate Problem Report must be completed in full and must be fully understandable.

- In the event than an urgent security incident is identified with an end-entity certificate (subscriber certificate/TLS certificate), the certificate will be revoked within 24 hours.
- As soon as a justified, however, not urgent reason for revocation is identified with an end-entity certificate (subscriber certificate), the certificate will be revoked within five days.
- As soon as a justified reason for revocation is identified for a subordinate CA, revocation will take place within seven days.

D-Trust GmbH, the subscriber and the party requesting revocation together determine the specific time of revocation.

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

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

The reasons for revoking certificates are listed in the Baseline Requirements (BRG) of the CA/Browser Forum, see section 4.9. Certificate revocation and suspension.

QCP-n, QCP-l

If a security breach or loss of integrity is detected in D-Trust qualified trust services that has a significant impact on the trust service provided and the personal data stored there, the TSP will notify the competent supervisory authority and/or other competent authorities in accordance with Article 19(2) of Regulation (EU) No 910/2014 within 24 hours of becoming aware of such breach or loss of integrity.

If the security breach or loss of integrity is likely to adversely affect a natural person or legal entity for whom/which the trust service was provided, the TSP will also notify such natural person or legal entity of the security breach or loss of integrity.

Suspected abuse should be reported to the following e mail address: support@d-trust.net.

NCP, LCP, V-PKI

In all other cases, such as S/MIME the following e-mail address is available: support@d-trust.net

1.5.3 Compatibility of CPs of external CAs with this CP

This CP describes the minimum requirements which all PKI entities must fulfil.

Both in CA and in EE certificates, further CPs can be referenced via policy OIDs which do not contradict this CP. The reference of a policy OID in the certificate extensions serves as the CA's 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).

1.6 Definitions and acronyms

1.6.1 Definitions and names

CA certificate	The certificate issued for a certification authority for the signature key of the CA.
CA Root Inclusion Prozess	Inclusion of CAs in software application components of verifying third-party manufacturers.
Certification Authority (CA)	Instance of the root PKI, see section 1.3.1.
Certificate policy	Certificate Policy (CP), see section 1.1.
Certification Practice Statement (CPS)	Declaration of implementation by the CA
Certificate Service Manager (CSM)	A D-Trust service for creating and managing certificates.
Certification service provider	Provider of certification services, is used in the same sense as the term trust service provider.
Cross-certificate	Certificate that is used in order to confirm that other CAs are trusted.
D-TRUST Root CA	Root certificate authority, see section 1.3.1.

D-TRUST Root PKI	PKI operated by D-Trust GmbH.
Distinguished Name	A technical name made up of several name parts which clearly describes in certificates the issuing CA and/or the subscriber within the root PKI. The distinguished name is defined in detail in standard [X.501].
EE certificate	See end-entity certificate.
Electronic seal	The electronic seal serves as proof that an electronic document was issued by a legal entity and proves the origin and integrity of the document.
End-entity/Subject	The identity of the end-entity/subject is linked to the certificate and the pertinent key pair, see also section 1.3.3.
End-entity certificate	Certificate that may not be used to certify other certificates or CRLs.
EV certificates	Certificate with extended validation of the subscriber
Federal Network Agency	Bundesnetzagentur
HR-DB	Human-resources database (of an organization)
Other third parties	Natural persons or legal entities who, for instance, request revocation of a certificate.
Postident Basic	Identification method, offered by Deutsche Post AG.
Publicly trusted (PT) services	are trust services according to the specifications of the Certificate Consumer members of the CA Browser/Forum in combination with the specifications of the CA Browser/Forum.
Publicly Trusted Certificate (PTC)	is a certificate issued by a publicly trusted (PT) service.
Qualified trust service	Electronic service according to Art. 3 (17) eIDAS
Qualified certificate	A certificate issued by a qualified trust service provider that fulfils the requirements of Annex I of eIDAS
Registration authority	Registration authority (RA), part of the PKI that identifies the entities, refer to section 1.3.2.
Relying party *(Relying Party)*	An individual or a legal entity who/that uses certificates, see section 1.3.4.
Repository service	PKI service for online requests for information, such as certificates and revocation lists, usually carried out via LDAP protocol.

Revocation	The revocation of a certificate is irreversible.
Root Store	Storage of trusted root CA certificates in software application components of verifying third-party manufacturers.
Signature card	Processor smartcard that can be used to generate electronic signatures and for other PKI applications.
sign-me	A service provided by D-Trust GmbH for remotely triggered signature processes
seal-me	A service provided by D-Trust GmbH for remotely triggered seal processes
Soft PSE	Software Personal Security Environment, also referred to as software token, contains the EE key pair, the EE certificate as well as the certificate of the issuing CA authority
Status request service	PKI service for online requests regarding the status of a certificate (OCSP).
Subordinate CA (sub-CA) or intermediate CA	A lower-level CA that issues EE certificates and/or further CA certificates.
Subscriber *(Subscriber)*	*Subscriber*, a natural person or legal entity who/that applies for and holds EE certificates, see section 1.3.3.
Third parties concerned	If a certificate contains details of subscriber's powers of representation for third parties, these are referred to as “third parties concerned”.
Third party authorized to revoke	A natural person or legal entity authorized to revoke certificates.
Token	Medium for certificates and key material.
Trust center	The security zone on the premises of D-Trust GmbH
Trust service	Electronic service according to Art. 3 (16) eIDAS
Trust service provider (TSP)	Provider of trust services according to Art. 3 (19) eIDAS
VideoIdent	Identification method, offered by Identity TM AG

1.6.2 Acronyms

BAFIN	Federal Financial Supervisory Authority
BDSG	German Federal Data Protection Act

BRG	Baseline Requirements Guidelines
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
CA	Certification Authority
Cloud CPS	Certification Practice Statement of the D-TRUST Cloud PKI
CN	Common Name
CP	Certificate Policy of D-Trust GmbH
CPS	Certification Practice Statement
CSM CPS	Certification Practice Statement of the D-TRUST CSM PKI
CRL	Certificate Revocation List
DN	Distinguished Name
DSGVO	General Data Protection Regulation
DVCP	Domain Validation Certificate Policy
EBA	European Banking Authority
EVCP	Extended Validation Certificate Policy
FIPS	Federal Information Processing Standard
FQDN	Fully qualified domain name
HSM	Hardware Security Module
ISO	International Organization for Standardization
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
NCA	National Competent Authority
NetSec-CAB	Network Security Requirements- CA/Browser Forum
NCP	Normalized Certificate Policy
NCP+	Normalized Certificate Policy requiring a secure user device
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVCP	Organizational Validation Certificate Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PSD2	Payment Services Directive 2
PSE	Personal Security Environment

PSP	Payment Service Provider
PSP_AI	Account Information Service Provider
PSP_AS	Account Servicing Payment Service Provider
PSP_IC	Payment Service Provider Issuing Card-based payment instruments
PSP_PI	Payment Initiation Service Provider
PUK	Personal Unblocking Key
QCP	Qualified Certificate Policy
QCP-l	Qualified Certificate Policy for Legal Persons
QCP-n	Qualified Certificate Policy for Natural Persons
QCP-w	Qualified Certificate Policy for Qualified Website Authentication
QSCD	Qualified Signature Creation Device
QSealC	Qualified electronic Seal Certificate
QWAC	Qualified Website Authentication Certificate
RA	Registration Authority
RFC	Request for Comment
Root CPS	Certification Practice Statement of the D-TRUST Root PKI
RTS	Regulatory Technical Standard for PSD2 strong customer authentication and common and secure open standards of communication
SSCD	Secure Signature Creation Device
SUD	Secure User Device
TLS	Transport Layer Security, also known under the previous name Secure Sockets Layer (SSL)
TSP	Trust Service Provider
TSPS	Trust Service Practice Statement
URL	Uniform Resource Locator
UTF8	Unicode Transformation Format-8
V-PKI	Administration PKI

1.6.3 References

[AGB]	General Terms and Conditions of D-Trust GmbH, latest version
[BRG]	Baseline Requirements of the CA/Browser Forum, CA/Browser Forum, version 1.8.6, 2022-12-14

[CP V-PKI BSI]	"Security guidelines of the administration root certification authority" version 3.2 dated 9 January 2003 and the related amendments dated 29 January 2013 issued by the Federal Office for Information Security. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/VerwaltungsPKIVPKI/Dokumente/dokumente_node.html
[CPS]	Certification Practice Statement of the D-TRUST PKI, D-Trust GmbH, latest version. The applicable CPS is referenced in the respective certificate.
[eHealth Network]	eHealth Network Guidelines Technical Specifications for Digital Green Certificates; Volume 1; V1.0.5 (2021-04-21); Technical Specifications for Digital Green Certificates; Volume 5; Public Key Certificate Governance; V1.02 (2021-05-12)
[eIDAS]	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[ETSI-ALG]	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites; ETSI TS 119 312 V1.3.1 (2019--02)
[EN 319 401]	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers; ETSI EN 319 401 V2.2.1 (2018-04)
[EN 319 411-1]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements; ETSI EN 319 411-1 V1.2.2 (2018-04)
[EN 319 411-2]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates; ETSI EN 319 411-2 V2.2.2 (2018-04)
[EN 319 412]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures; ETSI EN 319 412-1 V1.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons; ETSI EN 319 412-2 V2.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons; ETSI EN 319 412-3 V1.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates; ETSI EN 319 412-4 V1.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements; ETSI EN 319 412-5 V2.2.3 (2020-01)

[EN 319 421]	Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers issuing Time-Stamps; ETSI EN 319 421 V1.1.1 (2016-03)
[EN 319 422]	Electronic Signatures and Infrastructures (ESI);Time-stamping protocol and time-stamp token profiles; ETSI EN 319 422 V1.1.1 (2016-03)
[EVGL]	Guidelines for the Issuance and Management of Extended Validation Certificates, CA/Browser Forum, Version 1.8.0, 2022-11-30
HADDEX Sanktionsliste	https://www.awr-portal.de/SubBoy/pdf.jsp?site=ReadMe&lang=en
[ISO 3166]	ISO 3166-1:1997: Codes for the representation of names of countries and their subdivisions - Part 1: Country codes
[NetSec-CAB]	CA/Browser Forum Network and Certificate System Security Requirements, version 1.7, 05 April 2021
[RFC 2247]	Using Domains in LDAP/X.500 Distinguished Names, January 1998
[RFC 3647]	Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, November 2003
[RFC 5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008
[RFC 6818]	Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, January 2013
[RFC 6960]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013
[RFC 6962]	Certificate Transparency, June 2013
[TR-03145-1]	Secure CA operation, Part 1: Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level "high", Version 1.1
[TR-02102-1]	"Cryptographic methods: Recommendations and Key Lengths", version 2020-01
[VDG]	Trust Services Act (Trust Services Act of 18 July 2017 (Federal Gazette I, p. 2745), last revised by Article 2 of the Law of 18 July 2017 (Federal Gazette I, p. 2745)
[X.501]	ITU-T RECOMMENDATION X.501, Information Technology – Open Systems Interconnection – The Directory: Models, Version October 2019
[X.509]	ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, October 2019

2. Publication and Repository Responsibility

2.1 Repositories

The TSP publishes CRLs and certificates in the LDAP[10] repository at: ldap://directory.d-trust.net

The complete certificate-specific link can be found on the certificate itself.

CA certificates, this CP, the TSPS, the CPS and the Subscriber Agreement are published on the D-Trust GmbH websites and can be requested or downloaded in PDF format using the following link in the repository: https://www.d-trust.net/en/support/repository

The repository also contains test websites for TLS certificates as well as other demo certificates for other products via which the certificate status can be retrieved.

The TSP provides an online service (OCSP) that can be used to request the revocation status of D-Trust certificates. The link can be found on the certificate. End-entities/subjects can also query the status of their certificates on the following website:

https://www.d-trust.net/en/support/ocsp-request

Different procedures for transmitting the Subscriber Agreement can be agreed to on a customer-specific basis.

2.2 Publication of certificate information

These rules are described in the respective CPS that belongs to the certificate.

2.3 Publication frequency

These rules are described in the respective CPS that belongs to the certificate.

2.4 Repository access control

Certificates, revocation lists, TSPS, CPS and CPs can be publicly retrieved 24/7 and at no cost. Read only access is unrestricted. Changes in repository and web contents are carried out exclusively by the TSP.

The relevant parts of other non-public documents can be issued on request against proof of a legitimate interest.

2.5 Access to and use of services

D-TRUST's services are offered to the public and are accessible to all. In principle, they can be used by anyone who has agreed to the General Terms and Conditions, the Subscriber Agreement, the Certificate Policy and the Certification Practice Statement of D-Trust GmbH applicable to the respective service (in short: Terms & Conditions). D-Trust GmbH is committed to offering low-barrier services.

The Web Content Accessibility Guidelines (WCAG) of the W3C primarily serve as a guideline for developing largely barrier-free Internet content.

[10] Certificates and revocation lists are retrieved using LDAPv3 according to RFC4511 without Security Layer.

3. Identification and Authentication

Identification and authentication of D-Trust certificates are carried out according to product and customer-specific requirements as well as the requirements for the respective certification (e.g. eIDAS, EN 319 411-1 or EN 319 411-2).

These rules are described in the respective CPS that belongs to the certificate.

4. Operational Requirements

The operational requirements for D-Trust certificates are subject to product and customer-specific requirements as well as the requirements for the respective certification (e.g. eIDAS, EN 319 411-1 or EN 319 411-2).

These rules are described in the respective CPS that belongs to the certificate.

5. Facility, Management and Operational Controls

The TSP sets up facility, management and operational controls that meet with the requirements of [EN 319 411-1], [EN 319 411-2], [EVGL] and [eIDAS].

These rules are described in the respective CPS that belongs to the certificate.

6. Technical Security Controls

The TSP sets up technical security controls that meet with the requirements of [EN 319 411-1], [EN 319 411-2], [EVGL] and [eIDAS]. The latest information on the signature and encryption algorithms used can be found in the CPS section 7.1.3.

Subscribers and relying parties must use trusted computers and software.

These rules are described in the respective CPS that belongs to the certificate.

7. Profiles of Certificates, Certificate Revocation Lists and OCSP

7.1 Certificate profiles

The certificates issued by the CAs of the D-Trust PKI meet the requirements of the ITU [X.509], IETF [RFC 5280] and IETF [RFC 6818] standards, as well as ETSI [ETSI EN 319 412]. Deviations are described, when necessary, in a referenced document.

QCP, QEVCP-w and QNCP-w
The issued qualified certificates meet the requirements of [eIDAS], Annexes I, III and IV.

EVCP
The issued EV certificates meet the requirements of [EVGL].

The profiles are described in the respective CPS that belongs to the certificate.

7.2 CRL profiles

The certificate revocation lists issued meet the requirements of ITU [X.509], IETF [RFC 5280] and IETF [RFC 6818] standards.

The profiles are described in the respective CPS that belongs to the certificate.

7.3 OCSP profiles

This status query service complies with the [RFC 6960] standard.

The profiles are described in the respective CPS that belongs to the certificate.

8. Compliance Audit and Other Assessments

These rules are described in the respective CPS that belongs to the certificate.

9. Other Business and Legal Matters

9.1 Prices

9.1.1 Certificate prices

Remuneration for the services described in this document is laid down in the price list or the respective agreement.

9.1.2 Prices for access to certificates

Certificate requests in the repository service are free of charge.

9.1.3 Prices for revocation or status information

Revocation and the retrieval of status information are free of charge.

Revoked certificates are not replaced.

9.1.4 Prices for other services

If offered, refer to the price list or the respective agreement.

If the acquisition or temporary loan of hardware or software, especially card readers, has been agreed, this will be deemed compensated by payment of the agreed prices, including the required simple user license.

9.1.5 Rules for cost refunds

The respective agreements with the customer or the General Terms and Conditions [AGB] apply.

9.2 Financial responsibilities

9.2.1 Insurance cover

D-Trust GmbH has the means and the financial stability required to operate trust services in a suitable manner.

The TSP meets the requirement pursuant to Article 24 (2) lit. c (eIDAS) in conjunction with section 10 of the German Trust Services Act (VDG, *Vertrauensdienstgesetz*) and, with a view to damage pursuant to Article 13, has taken out liability insurance pursuant to section 10 VDG (€250,000 for each case of damage caused by a liability-triggering event). Non-qualified trust services are covered by business liability insurance.

The TSP meets the requirements of [EVGL] 8.4.

9.2.2 Other resources for maintaining operations and compensation for damage

No stipulation.

9.2.3 Insurance or warranty for end users

No stipulation.

9.3 Confidentiality of business data

9.3.1 Definition of confidential business data

The confidentiality of information can be agreed to unless this is already defined in applicable law.

9.3.2 Business data not treated as confidential

All information in issued and published certificates as well as the data referred to in section 0 is deemed to be public.

9.3.3 Responsibilities for the protection of confidential business data

In certain cases, the TSP can be obliged to employ suitable technical and organizational measures to protect data provided to it and deemed to be confidential business data against disclosure and illicit access, and further not to use such data for other unintended purposes or to disclose it to third parties only in as far as such obligation does not violate the law. As part of organizational measures, the employees working for the TSP will be obliged to maintain confidentiality regarding the data in as far as permitted by law.

9.4 Protection of personal data

9.4.1 Data protection concept

The TSP works on the basis of a data protection concept that determines the protection of confidential personal data. The TSP meets the requirements of the Federal Data Protection Act (BDSG) as well as the General Data Protection Regulation (GDPR).

9.4.2 Definition of personal data

Art.4 (1) GDPR is applicable.

9.4.3 Data not treated as confidential

Confidential data does not include such data that must be published in order to fulfil its purpose (certificate revocation lists, status information, published certificates).

9.4.4 Responsibilities for data protection

The TSP warrants compliance with data protection legislation. All of the TSP's employees are obliged to observe data protection. The company's data protection officer conducts internal control while external control is carried out by the Berlin Commissioner for Data Protection and Freedom of Information.

9.4.5 Information concerning and consent to the use of personal data

No later than at the time of application, the subscriber will be informed of which personal data will be contained in the certificate. Certificates are only published after the subscriber has agreed to this at the time of application.

If nothing to the contrary is laid down in law, subscribers consent to the use of their personal data, at the latest at the time of application, or have obtained the consent of any third parties concerned by this point in time.

Any personal data that is no longer needed to provide the service will be immediately deleted. Personal data which is needed for certificate proof is subject to the deadlines foreseen in section 5.5.2 of the CPS.

9.4.6 Information pursuant to legal or government requirements

The TSP, as a company under private law, is subject to the General Data Protection Regulation, the Federal Data Protection Act and the laws of the Federal Republic of Germany. Information is disclosed accordingly.

Information is disclosed when required by law pursuant to sec. 8 (2) VDG.

With a view to information requests pursuant to the Federal Data Protection Act, subjects should contact the offices in charge pursuant to the Federal Data Protection Act.

9.4.7 Other conditions for information

Information other than the type of information described in section 9.4.6 is not disclosed.

9.5 Industrial property and copyrights

9.5.1 TSP

The applicability and content of copyrights and other IP rights are based on the general statutory provisions.

9.5.2 Subscriber

The subscriber undertakes to comply with intellectual property rights in the application and certificate data.

9.6 Representations and guarantees

9.6.1 Scope of services by the TSP

Agreements, if any, and the General Terms and Conditions [AGB] apply together with this CP. With a view to any warranties or representations, this CP and the relevant CPS contain only those warranties or representations expressly granted for this area.

The TSP ensures that the procedures described in the relevant CPS or TSPS, respectively are implemented and adhered to.

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

The TSP ensures the unambiguous identification of the subscriber and/or (according to the agreement) the end-entity and the allocation of the public key to the end-entity according to the applicable requirements. The TSP ensures that a name (DistinguishedName in the subject field) used in certificates is always unambiguous within the D-Trust PKI and beyond the life cycle of the certificate and that it is always assigned to the same subscriber. This ensures the unambiguous identification of the subscriber on the basis of the name (subject) used in the certificate.

The TSP operates the CAs and makes the repository service and the revocation information available.

EVCP

The TSP does not provide any guarantees in the legal sense according the German Civil Code, however, it does observe the provisions according to section 7.1 [EVGL] with a view to "Legal Existence","Identity","Right to Use Domain Name", "Authorization for EV Certificate","Accuracy of Information", "Subscriber Agreement", "Status", "Revocation" and warrants adherence hereto.

Moreover, the TSP provides reporting mechanisms pursuant to section 4.9.3 [BRG]. The reporting mechanisms allow subscribers, relying parties, suppliers of application software and other third parties concerned to report suspicious certificates to the TSP. The TSP then follows up on this suspicion (e.g. fraud, phishing, etc.).

Replacement of signature-creation devices

D-Trust GmbH reserves the right to replace signature-creation devices before the end of the respective period of use if this is necessary in order to comply with applicable laws or safeguard the legitimate interests of D-Trust GmbH or is otherwise required for an important reason, especially if a replacement becomes necessary for security reasons. D-Trust GmbH will duly take the interests of the customer into consideration.

Support and advice

To the extent that support and advisory services are provided, D-Trust GmbH will select the employees assigned to this matter and offer support and advice during normal business hours on Monday through Friday, 7am to 6pm, except on national holidays, by way of first-level support through online or telephone contact, unless otherwise agreed. Where required and in order to provide support and advisory services, D-Trust GmbH will be permitted to inspect the corresponding documents or data, or the required information will be provided.

The TSP can outsource sub-tasks to partners or external providers. The TSP ensures in such cases that the provisions of the CP and the CPS are observed.

9.6.2 Scope of services of the RA

The TSP operates registration authorities (RAs). The RA performs identification and registration. The General Terms and Conditions [AGB] apply as well as the provisions of this CP.

9.6.3 Subscriber's representations and guarantees

Agreements, if any, and the General Terms and Conditions [AGB] apply together with this CP.

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

The subscriber agrees to the Subscriber Agreement containing the subscriber's representations and guarantees.

EVCP, OVCP, DVCP, NCP, LCP, V-PKI

The subscriber undertakes to inform the end-entity of its rights and obligations. The Subscriber Agreement meets with the requirements of [EVGL] and [BRG].

EVCP

The Subscriber Agreement meets with the requirements of section 10.3 [EVGL].

9.6.4 Representations and guarantees of the certificate user

The relying party's representations and guarantees are not laid down in this CP. There is no contractual relationship between the TSP and the relying party. Otherwise, the General Terms and Conditions [AGB] and the statutory provisions are applicable.

9.7 Disclaimers

9.7.1 TSP's disclaimer

The agreements entered into and the General Terms and Conditions [AGB] apply.

EVCP

If EV certificates are issued, the following provisions pursuant to section 18 [EVGL] are additionally applicable:

If the TSP has issued the EV certificate without deviations pursuant to this Certificate Policy, the TSP will not be liable for damage caused with the certificate.

The TSP expressly does not assume any liability, especially for damage that is caused by the use or non-use of certificates without certification or by incorrect use of electronic signatures for which the customer is liable.

Any impairment of the functioning of the certificate storage medium, which results from using unsuitable hardware or software, falls under the customer’s sphere of risk.

9.8 Limitations of liability

9.8.1 Limitation of liability

D-Trust GmbH’s liability for the products offered within the scope of the certification and trust services is limited according to the information in the product description.

Furthermore, the respective agreements, if any, and the General Terms and Conditions [AGB] apply.

9.8.2 Liability for slight negligence

Notwithstanding section 9.8.1, D-Trust GmbH’s liability in the case of slightly negligent breaches of duty are limited to the direct average damages that are foreseeable and typical for the type of goods and the certification and trust services. This also applies in the case of any slightly negligent breaches of duty on the part of legal representatives or vicarious agents. D-Trust is not liable to entrepreneurs for any slightly negligent violation of insignificant contractual obligations.

9.8.3 No limitation of liability in special cases

The aforesaid limitation of liability does not apply to product liability claims by the customer. Furthermore, the limitation of liability does not apply to physical injury, damage to health or death of the customer caused by reasons for which D-Trust GmbH is responsible. Section 9.8.1 remains unaffected by the foregoing.

9.8.4 Liability for identification

The issuing of certificates only confirms that the required proof of identity or proof of legitimization was properly and verifiably submitted to D-Trust GmbH at the time of application in accordance with the applicable statutory regulations in Germany or the contractually agreed provisions. In as far as the customer performs the required identity verification on the basis of the specific agreement with D-Trust GmbH, the customer will adhere to D-Trust GmbH’s requirements for identity verification. In the event that the

customer violates such requirements, the customer will indemnify and hold harmless D-Trust GmbH with regard to any resultant claims raised by third parties.

9.8.5 Liability provisions in the case of EV certificates

In the event that the provisions of this Certificate Policy were not adhered to when issuing the EV certificate, the following liability provisions apply also in accordance with the requirements laid down in section 18 [EVGL]:

The TSP is only liable for the correct verification of the application and the resultant contents of the EV certificates to the extent of its verification possibilities. The issuance of EV certificates merely confirms that at the time of application D-Trust was given the necessary proof of identity or authorization pursuant to the requirements of this Certificate Policy. In as far as an external registration authority performs the necessary identity verification with a view to the subscriber, this registration authority must observe and undertake to observe the requirements of D-Trust in line with the provisions of this Certificate Policy during the verification of identity. In the event that the registration authority violates these requirements, D-Trust GmbH and Bundesdruckerei GmbH must be held harmless against all claims by the subscriber or third parties. The foregoing also applies to cases where the subscriber itself as a registration authority verifies the identity of subscribers who belong to its organization.

The subscriber is liable for damage which D-Trust GmbH or Bundesdruckerei GmbH may suffer due to incorrect data in the EV certificate or incorrect use of EV certificates for which the subscriber is liable.

Otherwise, in the cases stated above, the TSP's liability for each EV certificate is limited to a maximum of USD 2,000.00 or the equivalent amount in euro on the day such damage occurred.

9.8.6 Customer’s liability

The customer is liable for any damage which D-Trust GmbH may suffer as a result of incorrect information in the certificate caused by the customer, and as a result of the incorrect use of electronic signatures for which the customer is responsible. The customer is also liable for any damage which results from the authorized or unauthorized use of the services rendered by D-Trust GmbH if and to the extent that the customer is responsible for such damage.

9.8.7 Limitation period

If the customer is a company, any claims for damages which the customer may raise on the grounds of a defect in the products supplied will become statute-barred one year after delivery of the product. If the customer is a consumer, any claims for damages due to a defect in the delivered goods will become statute-barred two years after delivery of the goods. This foregoing does not apply to cases where D-Trust GmbH can be blamed for gross default or to cases of physical injury, damage to health or death of the customer caused by reasons for which D-Trust GmbH is responsible.

9.9 Damages

9.9.1 Claims by the TSP against subscribers

In the event that the customer demands correction of the information specified in its order, the customer will be obliged to bear the costs of such correction on the basis of the agreed prices in as far as the customer was responsible for the incorrect information in the order form, for instance, due to faulty transmission for which the customer is responsible.

Furthermore, the respective agreements, if any, and the General Terms and Conditions [AGB] apply.

9.9.2 Claims by the subscriber against the TSP

Agreements, if any, and the General Terms and Conditions [AGB] apply.

The customer will only be entitled to offset against claims which are uncontested or have been recognized by a court of law. The customer will only be entitled to exercise a right of retention due to counterclaims resulting from this contractual relationship.

Furthermore, the respective agreements, if any, and the General Terms and Conditions [AGB] apply.

9.9.3 Claims by application software suppliers against the TSP

EVCP, OVCP, DVCP, NCP, LCP

Notwithstanding the limitations on its liability to subscribers and Relying Parties, the TSP understands and acknowledges that the application software suppliers who have entered into a root certificate distribution agreement with the TSP do not assume any obligation or potential liability in relation to the TSP under these requirements or that might otherwise exist due to the issuance and maintenance of certificates or reliance thereon by Relying Parties or others. Therefore, the TSP must defend, indemnify and hold harmless any application software supplier against any third-party claims, damages or losses suffered by such application software supplier in conjunction with a certificate issued by the TSP, regardless of the cause of the claim or the jurisdiction involved. However, the foregoing does not apply to any claims, damages or losses suffered by such application software supplier in conjunction with a certificate issued by the TSP if such claim, damage or loss was directly caused by such application software supplier's software displaying as not trustworthy a certificate that is still valid or displaying as trustworthy: (1) a certificate that has expired, or (2) a certificate that has been revoked (but only in cases where the revocation status is currently available online from the TSP and the application software either failed to check the status or ignored a notice of revoked status).

9.10 Validity of the CP and termination of validity

9.10.1 Validity of the CP

This CP is applicable from the time of its publication and will remain in effect until the last certificate issued under this CP expires. The version of the CP published at the time the application is made is the applicable version.

9.10.2 Termination of validity

See section 9.10.1.

9.10.3 Effect of termination

See section 9.10.1.

9.11 Individual communications to and agreements with PKI entities

Messages issued by the TSP to subscribers will be forwarded to the most recent address recorded in D-Trust GmbH's documents or to the e-mail address in the (electronically signed) application.

9.12 Amendments

9.12.1 Procedure for amendments

Amendments to this CP are included in this document and published under the same OID. Editorial changes will be marked.

9.12.2 Notification mechanisms and deadlines

No stipulation.

9.12.3 Conditions for OID changes

No stipulation.

9.13 Dispute resolution provisions

Complaints regarding adherence to or implementation of this CP should be submitted in writing to the TSP (D-Trust GmbH, Kommandantenstr. 15, 10969 Berlin, Germany). If the matter has not been resolved within four weeks after the complaint was submitted, the following applies: Any legal relations between Bundesdruckerei, D-Trust GmbH and third parties who derive legal relations under this CP are subject to the laws of the Federal Republic of Germany, barring the United Nations Convention on Contracts for the International Sale of Goods.

9.14 Reporting security incidents with certificates

See section 1.5.2.

9.15 Place of jurisdiction

The place of jurisdiction for any legal disputes is Berlin in as far as the customer is a merchant, a legal entity under public law or a special fund under public law, or if the customer does not have a place of general jurisdiction in the Federal Republic of Germany. D-Trust GmbH is entitled to enforce its rights at the general place of jurisdiction for the customer. An exclusive place of jurisdiction, if any, will not be affected by the foregoing provision.

9.15.1 Compliance with applicable law

This CP is subject to the laws of the Federal Republic of Germany and the laws of the European Union. Any legal relations between D-Trust GmbH and the customer are subject to the laws of the Federal Republic of Germany. The UN Convention on Contracts for the International Sale of Goods is excluded.

9.15.2 Place of performance

The place of performance for D-Trust GmbH and the customer is Berlin.

9.16 Miscellaneous provisions

9.16.1 Completeness

The following documents are the subject matter of the applicable agreements involving PKI entities:

- Agreement and application documents
- The General Terms and Conditions [AGB] valid at the time of application or any valid version included
- The CP in effect at the time of application
- In the case of qualified certificates, the PKI user information valid at the time of application

The following documents are applicable for TLS CAs, their sub-CAs and root CAs:

- Agreement and application documents

- The General Terms and Conditions [AGB] valid at the time of application or any valid version included
- The version of the [EVGL] and the CP valid at the time of application

9.16.2 Differentiation

No stipulation.

9.16.3 Partial invalidity

In the event that one or more of the provisions of this CP are invalid, the validity of the remaining provisions will not be affected by such invalidity.

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP
The provisions of BRG 9.16.3 apply.

9.16.4 Enforcement (legal counsel's fees and waiver of remedies in law)

Agreements, if any, and the General Terms and Conditions [AGB] apply.

9.16.5 Force majeure

Agreements, if any, and the General Terms and Conditions [AGB] apply.

9.17 Other provisions

9.17.1 Conflicting provisions

The provisions contained in section 9.16.1 are final. They are applicable in relation to each other in the order in which they are enumerated in section 9.16.1 with subordinate effect.

9.17.2 Compliance with export laws and regulations

D-Trust GmbH particularly hereby rejects any terms and conditions of the customer, which would involve D-Trust GmbH in a boycott that exceeds the applicable statutory EU and UN penalty provisions or would cause D-Trust GmbH to make any declarations in this regard.

Right to refuse performance, termination, rescission, disclaimer
In the event that the deliveries or services to be rendered by D-Trust GmbH require prior export or import authorization of any government and/or state authority, or in the event that the delivery or service is otherwise restricted or prohibited due to national or international laws, D-Trust GmbH is entitled to suspend performance of its obligation to render such deliveries or services or to make payments until such authorization has been granted or such restriction or prohibition has been cancelled. In the event that the delivery or service depends on the granting of export or import authorization and such authorization is not granted, D-Trust GmbH will be entitled to terminate or withdraw from the contract at any time. D-Trust GmbH will not be held liable if delivery is delayed for any one or more of the reasons listed in this section or if delivery cannot be effected at all due to export regulations unless D-Trust GmbH acted intentionally or with gross negligence. The same applies in cases of justified withdrawal or termination.

Undertaking
By accepting the offer, or at the latest by accepting the delivery or service, the customer guarantees that it will not conduct any business with the goods which breaches applicable statutory export regulations and, in particular, that it will perform any further deliveries, transfers or exports of the delivered goods solely in compliance with the applicable statutory export control regulations. The customer undertakes to also impose the above regulations on its customers.

Exclusion of participants
The customer undertakes to ensure that no persons, organizations or institutions are involved in the handling of the contract or will be supported by the contract who/which are listed in the sanction lists of the EU and of the United Nations (in particular, Council Regulation (EC) No 881/2002, Council Regulation (EC) No 2580/2001, Council Regulation (EU) No 753/2011). The foregoing also applies to persons, organizations or institutions named in the sanctions lists of other governments (in particular, the US Denied Persons List, US Entity List, US Specially Designated Nationals List, US Debarred List) in as far as these do not unilaterally go beyond the UN or EU sanctions.

The customer further guarantees that neither it nor any of its shareholders are listed on such a list, and that it is not under the control of or a partner of any person or corporate body found on such lists. In the event that the customer or any of its shareholders, or a person or corporate body that the customer is a partner of, is added to a sanctions list during the term of this contract, the customer will be obliged to immediately notify D-Trust GmbH in this regard. D-Trust GmbH will in such case also be entitled at any time to cancel or withdraw from the contract without the customer being entitled to any claims as a result thereof.

Violation against export control laws
D-Trust GmbH and the customer agree that effective export control by the customer is an important prerequisite for performance of the agreement. D-Trust and the customer will therefore always consider a breach of export control regulations in conjunction with D-Trust products to be a severe violation of the interests of D-Trust GmbH. The foregoing is also applicable in the case of any violations committed by third parties. In such case, D-Trust GmbH will be entitled to terminate the contract for cause or to withdraw from the contract. The customer is obliged to indemnify and hold harmless D-Trust GmbH with regard to any resultant third-party claims for damages. The customer is obliged to compensate D-Trust GmbH for other costs and damage, whether tangible or intangible, including, in particular, penalties and fines, which are incurred due to failure to observe the obligations listed in section 9.17.2.

Furthermore, the respective agreements, if any, and the General Terms and Conditions [AGB] apply.

Zertifikatsrichtlinie (CP) der D-Trust GmbH
Version 4.5

Teil der Bundesdruckerei-Gruppe

COPYRIGHT UND NUTZUNGSLIZENZ

Zertifikatsrichtlinie der D-Trust GmbH
©2023 D-Trust GmbH

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

Alle weiteren Rechte vorbehalten.

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

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

Dokumentenhistorie

Version	Datum	Beschreibung
2.0	23.02.2015	▪ Im Rahmen der Umstrukturierung der Zertifikatsrichtlinie der D-Trust GmbH, wurde die Version des Dokumentes auf 2.0 hochgezählt. Die Dokumentenhistorie der Zertifikatsrichtlinie bis zu diesem Zeitpunkt kann in der Version 1.12 vom 17.11.2014 nachgelesen werden. ▪ Es wurden Inhalte, die die konkrete Umsetzung betreffen in die jeweilige CPS verschoben. Es ist aus dem jeweiligen Zertifikat zu erkennen unter welcher CPS dieses Zertifikat entstanden ist.
2.1	05.10.2015	▪ Editorische Änderungen und Hinweis auf Zertifikate ohne CPS-Eintrag
2.2	03.10.2016	▪ Umstellung auf EN 319 411-1
3.0	01.01.2017	▪ Einführung von qualifizierten Produkten gemäß EN 319 411-2 und eIDAS
3.1	01.04.2017	▪ Einführung eines qualifizierten Zeitstempeldienstes gemäß EN 319 421
3.2	01.10.2017	▪ Editorische Änderungen und Hinweise auf das Vertrauensdienstegesetz (VDG)
3.3	28.03.2018	▪ Editorische Änderungen und Angleichung an Mozilla Root Store Policy 2.5 ▪ Anpassung Nutzungslizenz an „Creative Commons Attribution" ▪ Ergänzung der OID für die PKI der E.ON SE und der Uniper
3.4	08.05.2018	▪ Anpassung vom Abschnitt 9.4 an die Datenschutzgesetzänderung zum 25.05.2018
3.5	05.07.2018	▪ Ergänzung der OID für die Telematikinfrastruktur des Gesundheitswesens (HBA) ▪ Angleichung an die Anforderungen der Baseline Requirements des CA/Browser Forum, Version 1.5.7, 29.04.2018
3.6	11.10.2018	▪ Aktualisierung des Abschnitts 1.5.2 gem. Ballot SC6 (Part 2)
3.7	30.11.2018	▪ Dieses CP entspricht den Anforderungen der Mozilla Policy 2.6.1 ▪ Jährliches Review der gesamten CP ▪ Redaktionelle Anpassungen
3.8	15.05.2019	▪ Ergänzung von PSD2 spezifischen Abkürzungen ▪ Jährliches Review der gesamten CP ▪ Redaktionelle Anpassungen
3.9	22.05.2019	▪ Ergänzung der qualifizierten Siegelzertifikate mit der Ausprägung PSD2 ohne QSCD in Abschnitt 1.1.3
3.10	23.10.2019	▪ Änderung der Vertriebsprozesse für Vertrauensdienste ▪ Abschnitt 2.5 ergänzt ▪ Ergänzung der OID für die Device PKI CPS in Abschnitt 1.1.3 ▪ Editorische Änderungen
3.11	19.03.2020	▪ Einführung von Domain validierten TLS-Zertifikaten (DVCP) gemäß EN 319 411-1 und BRG ▪ Jährliches Review der gesamten CP ▪ Abschnitt 2.5: Bezug zur Richtlinie WCAG ▪ Diese CP entspricht den Anforderungen BRG 1.6.7 und der Mozilla Policy 2.7
3.12	28.04.2020	▪ Einbindung neuer SubCAs zur Ausstellung von EV- und OV-Zertifikaten, siehe Abschnitt 1.1.3 ▪ Einführung von Zertifikaten für die Verwaltungs-PKI (V-PKI)

Teil der Bundesdruckerei-Gruppe

3.13	17.06.2020	▪ Konkretisierungen in Abschnitt 1.5.2 und Ergänzungen in Abschnitt 1.6.2.
3.14	21.08.2020	▪ Einführung einer OID für Zertifikate aus der Verwaltung-PKI (V-PKI) in Abschnitt 1.1.3
4.0	10.11.2020	▪ Einführung eines übergeordnetes Practice Statements (TSPS, V1.0) für die folgenden CPS-Dokumente: CSM CPS, Root CPS und Cloud CPS, siehe Abschnitt 1.1.2 ▪ Ergänzungen in Abschnitt 9
4.1	23.04.2021	▪ Einführung der neuen D-TRUST OV OID in Abschnitt 1.1.3 ▪ Aufnahme der CA/Browser Forum OIDs für die Policy Level von TLS Zertifikaten ▪ Aktualisierung der Referenzen in Abschnitt 1.6.3 ▪ Jährliches Review des gesamten CP
4.2	18.06.2021	▪ Update im Rahmen des BR Self Assessments ▪ Ergänzungen in den Abschnitten 1.6.1, 9.6, 9.9 und 9.16
4.3	14.04.2022	▪ Informative Einführung des Policy Levels NCP ▪ Umbenennung des Policy Levels QCP-w in QEVCP-w und Einführung des Policy Levels QNCP-w ▪ Jährliches Review des gesamten CP
4.4	14.11.2022	▪ Aktualisierung der Referenzen in Abschnitt 1.6.3 ▪ Ergänzungen im Abschnitt 1.4.2 ▪ Editorische Änderungen
4.5	14.02.2023	▪ Einführung einer neuen OID in Abschnitt 1.1.3 ▪ Editorische Änderungen ▪ Anpassung der BRG und EVGL Versionen in Abschnitt 1.6.3

Teil der Bundesdruckerei-Gruppe

Inhaltsverzeichnis

1. Einleitung ... 6
1.1 Überblick ... 6
1.2 Name und Kennzeichnung des Dokuments ... 10
1.3 PKI-Teilnehmer ... 10
1.4 Verwendung von Zertifikaten ... 11
1.5 Administration der Policy ... 12
1.6 Begriffe und Abkürzungen ... 13
2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen ... 20
2.1 Verzeichnisse ... 20
2.2 Veröffentlichung von Informationen zu Zertifikaten ... 21
2.3 Häufigkeit von Veröffentlichungen ... 21
2.4 Zugriffskontrollen auf Verzeichnisse ... 21
2.5 Zugang und Nutzung von Diensten ... 21
3. Identifizierung und Authentifizierung ... 21
4. Betriebsanforderungen ... 21
5. Nicht-technische Sicherheitsmaßnahmen ... 22
6. Technische Sicherheitsmaßnahmen ... 22
7. Profile von Zertifikaten, Sperrlisten und OCSP ... 22
7.1 Zertifikatsprofile ... 22
7.2 Sperrlistenprofile ... 22
7.3 Profile des Statusabfragedienstes (OCSP) ... 22
8. Auditierung und andere Prüfungen ... 23
9. Sonstige finanzielle und rechtliche Regelungen ... 23
9.1 Preise ... 23
9.2 Finanzielle Zuständigkeiten ... 23
9.3 Vertraulichkeit von Geschäftsdaten ... 24
9.4 Datenschutz von Personendaten ... 24
9.5 Gewerbliche Schutz- und Urheberrechte ... 25
9.6 Zusicherungen und Garantien ... 25
9.7 Haftungsausschlüsse ... 27
9.8 Haftungsbeschränkungen ... 27
9.9 Schadensersatz ... 28
9.10 Gültigkeitsdauer der CP und Beendigung der Gültigkeit ... 29
9.11 Individuelle Mitteilungen und Absprachen mit PKI-Teilnehmern ... 29
9.12 Nachträge ... 29
9.13 Bestimmungen zur Schlichtung von Streitfällen ... 30
9.14 Meldung von Sicherheitsvorfällen mit Zertifikaten ... 30
9.15 Gerichtsstand ... 30
9.16 Sonstige Bestimmungen ... 30
9.17 Andere Bestimmungen ... 31

Teil der Bundesdruckerei-Gruppe

1. Einleitung

1.1 Überblick

Dieses Dokument beschreibt die Zertifikatsrichtlinie (engl. *Certificate Policy*, im Folgenden CP genannt) der von D-Trust GmbH betriebenen Vertrauensdienste.

1.1.1 Vertrauensdiensteanbieter

Der Vertrauensdiensteanbieter (Trust Service Provider, im Folgenden TSP genannt) ist – auch im juristischen Sinne – die

D-Trust GmbH
Kommandantenstr. 15
10969 Berlin.

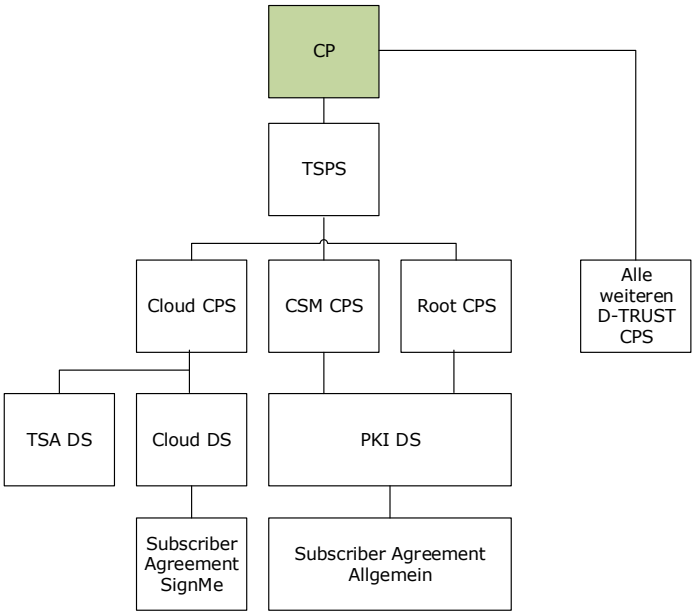
Der TSP kann Teilaufgaben an Partner oder externe Anbieter auslagern.

Für die Einhaltung der Verfahren im Sinne dieses Dokuments bzw. etwaiger gesetzlicher oder zertifizierungstechnischer Anforderungen an den TSP, bleibt der TSP, vertreten durch die Geschäftsführung oder deren Beauftragte, verantwortlich.

Die D-Trust GmbH stellt auch Zertifikate für eigene Zwecke aus. Hierbei werden ebenfalls die entsprechenden gesetzlichen bzw. zertifizierungstechnischen Anforderungen eingehalten.

1.1.2 Über dieses Dokument

Die folgende Grafik skizziert die Dokumentenhierarchie der D-Trust GmbH. Die grüne Markierung hebt das Dokument hervor, indem Sie sich befinden. Aktuell sind die drei genannten CPS dem TSPS untergeordnet. Die anderen CPS unterliegen direkt der CP. Schrittweise werden auch diese unter die TSPS gehängt.



Diese CP stellt Vorgaben und Anforderungen an die PKI und regelt somit den Zertifizierungsprozess während der gesamten Lebensdauer der End-Entity-Zertifikate (EE-Zertifikate) sowie das Zusammenwirken, Rechte und Pflichten der PKI-Teilnehmer[1].

Die gesamte CP ist rechtsverbindlich, soweit dies im Rahmen der deutschen bzw. europäischen Gesetzgebung zulässig ist. Sie enthält Aussagen über Pflichten, Gewährleistung und Haftung für die PKI-Teilnehmer. Soweit Garantien oder Zusicherungen betroffen sind, enthält die CP ausschließlich die für diesen Bereich ausdrücklich eingeräumten Garantien oder Zusicherungen.

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

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

1.1.3 Eigenschaften der PKI und Notation

Diese Regelungen sind in dem zum Zertifikat gehörenden Certification Practice Statement (im Folgenden CPS genannt) beschrieben.

Die D-Trust GmbH bietet unter dieser Policy diverse Produkte an, die die Anforderungen aus dieser Zertifikatsrichtlinie in ihren speziellen Produkteigenschaften erfüllen. Die Dienste werden nach Möglichkeit barrierefrei angeboten.

Die Erfüllung dieser Anforderungen wird in einem CPS beschrieben, welches zu einem Produkt oder einer Produktgruppe zugeordnet werden kann.

Die D-Trust GmbH verwendet mehrere CPS-Dokumente. Welches CPS zu dem jeweiligen Zertifikat gehört, ist in jedem Endanwenderzertifikat im Zertifikatsfeld „cpsURI" ersichtlich.

Vertrauensdienste die mit dem Zusatz „qualifiziert" genannt werden, sind qualifizierte Vertrauensdienste im Sinne der eIDAS. Vertrauensdienste die nicht mit dem Zusatz „qualifiziert" genannt werden, sind nichtqualifizierte Vertrauensdienste im Sinne der eIDAS.

Sollte in dem vorliegenden Zertifikat kein CPS hinterlegt sein, so liegt die Umsetzung der in dieser CP geforderten Regelungen im Ermessen des TSP. Zertifikate, in denen keine CPS eingetragen wurde, unterliegen <u>keiner</u> Zertifizierung im Sinne EN 319 411-1, EN 319 411-2, bzw. der eIDAS.

Dienste, die mit Zertifikaten ohne CP (PolicyOID) oder/und CPS-Eintrag (cpsURI) betrieben werden, sind im eigentlichen Sinne <u>keine</u> Vertrauensdienste im Sinne der eIDAS sondern Dienste für technische Verfahren.

[1] Im Interesse einer leichteren Lesbarkeit wird in diesem Dokument auf die weibliche Form der PKI-Teilnehmer und sonstigen genannten Personengruppen verzichtet. Es wird gebeten, die weibliche Form jeweils als eingeschlossen anzusehen.

Teil der Bundesdruckerei-Gruppe

Die Zugehörigkeit der Zertifikate zu dieser Policy ist durch die eingetragen OID zu erkennen:

Qualifizierte Personenzertifikate auf qualifizierter Signaturerstellungseinheit
Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QCP-n-qscd wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.150.1

Für qualifizierte Zertifikate der Telematikinfrastruktur des Gesundheitswesens (eHBA) Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QCP-n-qscd wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.211.1

Qualifizierte Siegelzertifikate auf qualifizierter Signaturerstellungseinheit
Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QCP-l-qscd wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.150.2

Qualifizierte Siegelzertifikate ohne qualifizierter Signaturerstellungseinheit
Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QCP-l wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.150.5

Qualifizierte Webseitenzertifikate (TLS)
Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QEVCP-w[2] wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.150.4

Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QNCP-w wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.150.3

Für PTC-Webseitenzertifikate (TLS)
Für EV-Zertifikate gemäß EN 319 411-1 und [EVGL] wird die folgende D-Trust EV-Policy-OID vergeben: 1.3.6.1.4.1.4788.2.202.1

CA/Browser Forum EV OID: 2.23.140.1.1

Für EV-Zertifikate aus der SubCA „VR IDENT EV SSL CA 2020" gemäß EN 319 411-1 und [EVGL]wird die D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.230.1[3]

CA/Browser Forum EV OID: 2.23.140.1.1

Für OV-Zertifikate gemäß EN 319 411-1 wird die D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.200.1. Für alle neuen OV-Zertifikate aus der SubCA „D-TRUST BR CA 1-20-1 2020" gemäß EN 319 411-1 wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.202.2

CA/Browser Forum OV OID: 2.23.140.1.2.2

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

[3] Die SubCA „VR IDENT EV SSL CA 2020" wurde gesperrt.

Teil der Bundesdruckerei-Gruppe

Für OV-Zertifikate aus der SubCA „VR IDENT SSL CA 2020" gemäß EN 319 411-1 wird die D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.230.2[4]

CA/Browser Forum OV OID: 2.23.140.1.2.2

Für DV-Zertifikate gemäß [EN 319 411-1] und [BRG] wird die D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.202.3

CA/Browser Forum DV OID: 2.23.140.1.2.1

Für PTC-Zertifikate
Für Zertifikate der Zertifizierungsklasse EN 319 411-1 LCP wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.200.2

Für Zertifikate der Zertifizierungsklasse EN 319 411-1 NCP wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.200.3

Für Zertifikate der E.ON SE PKI der Zertifizierungsklasse EN 319 411-1 LCP wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.210.1

Für Zertifikate der E.ON SE PKI der Zertifizierungsklasse EN 319 411-1 NCP wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.210.2

Für Zertifikate der Uniper PKI der Zertifizierungsklasse EN 319 411-1 LCP wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.212.1

Für Zertifikate der Uniper PKI der Zertifizierungsklasse EN 319 411-1 NCP wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.212.2

Fortgeschrittene Zertifikate der Cloud PKI
Die privaten Schlüssel für Zertifikate aus der Cloud PKI verbleiben in der gesicherten Umgebung des Trust Service Provider. Für solche Zertifikate werden zusätzlich die folgenden OIDs vergeben.

Für Zertifikate der Zertifizierungsklasse EN 319 411-1 LCP wird zusätzlich die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.200.2

Qualifizierte Zertifikate der Cloud PKI
Die privaten Schlüssel für Zertifikate aus der Cloud PKI verbleiben in der gesicherten Umgebung des Trust Service Provider. Für solche Zertifikate werden zusätzlich die folgenden OIDs vergeben.

Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QCP-n-qscd wird zusätzlich die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.100.1

Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QCP-l-qscd wird zusätzlich die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.100.2

Für den qualifizierten Zeitstempeldienst gemäß EN 319 421 BTSP wird zusätzlich die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.100.3

[4] Die SubCA „VR IDENT SSL CA 2020" wurde gesperrt.

Teil der Bundesdruckerei-Gruppe

Fortgeschrittene Zertifikate (Advanced Certificates)

Für Zertifikate aus der V-PKI (Verwaltungs-PKI) der Zertifizierungsklasse TR-03145-1 wird durch das BSI die Policy-OID 0.4.0.127.0.7.3.6.1.1.4.4 und durch die D-Trust wird die Policy OID 1.3.6.1.4.1.4788.2.201.2 vergeben.

Für Maschinen-Zertifikate der Zertifizierungsklasse TR-03145 wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.400.1.

Für Zertifikate ohne Zertifizierungsklasse wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.500[5,6]

Für Zertifikate ohne Zertifizierungsklasse mit ererbten Eigenschaften aus zertifizierten Produkten[7]

Für Personenzertifikate mit ererbten Eigenschaften aus zertifizierten Produkten wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.600.1

Für Zertifikate, die ausschließlich zu Testzwecken ausgestellt wurden, wird die folgende D-Trust Policy-OID vergeben: 1.3.6.1.4.1.4788.2.2.2[5]

Zertifikate, die Produkteigenschaften eines Produktes oder einer Produktgruppe der zuvor aufgeführten Policies besitzen, können unter folgendem Link abgerufen werden:

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

1.2 Name und Kennzeichnung des Dokuments

Dokumentname:	Zertifikatsrichtlinie der D-Trust GmbH
Kennzeichnung (OID):	Dieses Dokument erhält die D-Trust Policy-OID: 1.3.6.1.4.1.4788.2.200.1
Version	4.5

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (CA)

Die Zertifizierungsstellen (Certification Authority – CA) stellen Zertifikate sowie Sperrlisten aus. Möglich sind folgende Arten von Zertifikaten:

- Personenzertifikate für natürliche Personen (EE-Zertifikat),
- Siegelzertifikate für juristische Personen (EE-Zertifikat),

[5] Hierbei handelt es sich um Zertifikate, die alleine für technische Anwendungen oder Testzwecke vorgesehen sind. Es handelt sich somit NICHT um einen Vertrauensdienst im Sinne der eIDAS.

[6] Diese OID kann weitere dienstespezifische Unterebenen enthalten.

[7] Zertifikate mit diesen OIDs werden immer in Verbindung mit anderen zertifizierten Produkten ausgegeben. Für beide Zertifikate werden bestimmte Eigenschaften (z.B. distinguished name) unverändert verwendet sowie die gleichen Verfahren (z.B. Beantragung, Ident-Prozess) eingesetzt.

Teil der Bundesdruckerei-Gruppe

- Gruppenzertifikate für Personengruppen, Funktionen und IT-Prozesse (EE-Zertifikat),
- Zertifikate für Webserver (TLS-Zertifikate / EE-Zertifikat), die einen technischen Einsatzzweck haben aber auch das End-Entity-System (subject) entsprechend authentisieren können,
- Zertifikate für Geräte oder Maschinen, die einen rein technischen Einsatzzweck haben. Zertifikatsinhalte werden hierbei nicht verifiziert,
- Zertifizierungsinstanzen (untergeordnete CA-Zertifikate des TSP) und
- Dienstezertifikate für juristische Personen (EE-Zertifikat sowie Dienstezertifikate für Zeitstempel) unter denen unter anderem auch der qualifizierte Zeitstempel ausgestellt wird.

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

Die Zertifizierungsstelle betreibt als TSP Dienste im Sinne Kapitel III Verordnung (EU) Nr. 910/2014 i.V.m. (52) der Erwägungsgründe (Service für fernausgelöste Signaturen)

1.3.2 Registrierungsstellen (RA)

Diese Regelungen sind in der zum Zertifikat gehörenden CPS beschrieben.

1.3.3 Zertifikatsnehmer (ZNE) und Endanwender (EE)

Diese Regelungen sind in der zum Zertifikat gehörenden CPS beschrieben.

1.3.4 Zertifikatsnutzer (ZNU)

Zertifikatsnutzer (englisch *relying parties*) sind natürliche oder juristische Personen, die die Zertifikate der D-Trust GmbH nutzen und Zugang zu den Diensten des TSP haben.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

Zertifikate, die dieser Certificate Policy unterliegen, können im Allgemeinen für alle Zwecke verwendet werden. Der Zertifikatsnehmer ist dafür verantwortlich, Zertifikate so zu verwenden, dass die Verwendung den anwendbaren gesetzlichen Bestimmungen entspricht. Dies gilt insbesondere für die Einhaltung der jeweils anwendbaren Ausfuhr- oder Einfuhrbestimmungen.

Weitere Regelungen sind in dem zum Zertifikat gehörenden CPS beschrieben.

1.4.2 Verbotene Verwendungen von Zertifikaten

Die Verwendung von Zertifikaten für Dienste und Systeme, die bei Störungen oder Ausfällen zu großen materiellen oder immateriellen Schäden führen sowie Schäden an Leib und Leben verursachen können, ist nicht gestattet.

Hierzu zählen u.a. Atomkraftwerke, Chemieproduktionsanlagen oder Luftfahrtsysteme sowie insbesondere Dienste und Systeme, die in Zusammenhang mit kritischen Infrastrukturen stehen.

Hiervon abweichende Regelungen können im Einzelnen mit dem Vertrauensdiensteanbieter schriftlich vereinbart werden.

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

1.4.3 Verwendung von Dienstezertifikaten

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

Zu den Verwendungsarten zählen:

- CA-Zertifikate zur CA- und Zertifikatserstellung,
- Signatur von Statusauskünften[8],
- Signatur von Zeitstempeln[9].

1.5 Administration der Policy

1.5.1 Zuständigkeit für das Dokument

Diese CP wird durch die D-Trust GmbH gepflegt und aktualisiert. Der Beauftragte der Geschäftsführung übernimmt die Abnahme des Dokuments.

Diese CP wird jährlich durch den TSP überprüft und aktualisiert. Eine Änderung wird durch eine neue Versionsnummer dieses Dokumentes kenntlich gemacht.

Kontaktdaten:

D-Trust GmbH
Redaktion CP und CPS
Kommandantenstr. 15

10969 Berlin, Germany

Tel: +49 (0)30 259391 0
E-Mail: info@d-trust.net

1.5.2 Meldung von Sicherheitsvorfällen mit Zertifikaten

Der Zertifikatsnehmer sollte für einen Widerruf den schnellsten Weg wählen. Der schnellste Sperrweg für den Zertifikatsnehmer ist der Widerruf durch eine eindeutige Authentifizierung über die Online-Schnittstelle.

Zur Meldung von Sicherheitsvorfällen mit Zertifikaten (z.B. im Fall eines Missbrauchsverdachts), hält der TSP folgende Kontakte bereit:

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

Für die Meldung von Problemen mit TLS-Zertifikaten und CA-Zertifikaten, die für die Ausstellung von TLS-Zertifikaten geeignet sind, steht folgende Internetseite bereit:

https://www.d-trust.net/de/support/meldung-eines-zertifikatsproblems

Das Formular „Certificate Problem Report" ist zur Meldung des Sicherheitsvorfalls mit Zertifikaten zu beschreiben und zu versenden.

Die D-Trust GmbH nimmt innerhalb von 24 Stunden nach Erhalt des Certificate Problem Reports sowohl mit dem Verfasser Certificate Problem Reports als auch dem Zertifikatsnehmer Kontakt (preliminary report) auf. Der Certificate Problem Report muss vollständig und inhaltlich nachvollziehbar ausgefüllt werden.

---

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

[9] Zeitstempel werden durch gesonderte Dienstezertifikate signiert.

- Sobald ein dringender Sicherheitsvorfall bei einem End-Entity Zertifikat (Subscriber Certificate/ TLS-Zertifikat) festgestellt wird, erfolgt der Widerruf des Zertifikats innerhalb von 24 Stunden.
- Sobald ein berechtigter, nicht dringender Sperrgrund bei einem End-Entity Zertifikat (Subscriber Certificate) festgestellt wird, erfolgt der Widerruf innerhalb von fünf Tagen.
- Sobald ein berechtigter Sperrgrund für eine Subordinate CA festgestellt wird, erfolgt der Widerruf innerhalb von sieben Tagen.

Der konkrete Sperrzeitpunkt wird in Abstimmung zwischen der D-Trust GmbH, Zertifikatsnehmer und dem Sperrantragsteller festgelegt.

Gründe, die einen Widerruf von Zertifikaten bedingen, werden in den Baseline Requirements (BRG) des CA/Browser Forums aufgeführt, siehe Abschnitt 4.9. Certificate Revocation and Suspension.

QCP-n, QCP-l

Wenn bei qualifizierten Vertrauensdiensten der D-Trust eine Sicherheitsverletzung oder ein Integritätsverlust festgestellt wird, der erhebliche Auswirkungen auf den bereitgestellten Vertrauensdienst und die darin gespeicherten personenbezogenen Daten hat, benachrichtigt der TSP innerhalb von 24 Stunden nach Kenntnisnahme die zuständige Aufsichtsbehörde und/oder andere zuständige Behörden gemäß Artikel 19 Absatz 2 der Verordnung (EU) Nr. 910/2014.

Sollte sich die Sicherheitsverletzung oder der Integritätsverlust voraussichtlich nachteilig auf eine natürliche oder juristische Person auswirken, für die der Vertrauensdienst erbracht wurde, so unterrichtet der TSP auch diese natürliche oder juristische Person über die Sicherheitsverletzung oder den Integritätsverlust.

Für Meldungen eines festgestellten Missbrauchsverdachts steht folgende E-Mail Adresse bereit: support@d-trust.net

NCP, LCP, V-PKI

In allen anderen Fällen, wie z.B. S/MIME steht die folgende E-Mail Adresse bereit: support@d-trust.net

1.5.3 Verträglichkeit von CPs fremder CAs mit dieser CP

In dieser CP werden Mindestanforderungen beschrieben, die von allen PKI-Teilnehmern erfüllt werden müssen.

Sowohl in CA- als auch in EE-Zertifikaten können weitere CPs über Policy-OIDs referenziert werden, die dieser CP nicht widersprechen. Die Referenz einer Policy-OID in den Zertifikatserweiterungen bestätigt seitens der CA die Kompatibilität der Zertifizierungspraktiken mit der referenzierten CP (z.B. NCP 0.4.0.2042.1.1 gemäß EN 319 411-1).

1.6 Begriffe und Abkürzungen

1.6.1 Begriffe und Namen

Betroffene Dritte *(Third parties concerned)*	Enthält ein Zertifikat Angaben über die Vertretungsmacht des Zertifikatsnehmers für dritte Personen, so werden diese Stellen als „Betroffene Dritte" bezeichnet.

CA Root Inclusion Prozess	Aufnahme von CAs in Softwareanwendungs-komponenten von prüfenden Drittherstellern.
CA-Zertifikat *(CA certificate)*	das für eine Zertifizierungsinstanz ausgestellte Zertifikat zum Signaturschlüssel der CA
Certification Authority (CA)	Instanz der Root PKI, siehe Abschnitt 1.3.1.
Certificate Policy (CP)	Zertifikatsrichtlinie.
Certification Practice Statement (CPS)	Umsetzungserklärung der CA
Certificate Service Manager (CSM)	Dienst der D-Trust für die Erstellung und Verwaltung von Zertifikaten.
Cross-Zertifikat	Zertifikat, das verwendet wird, um andere CAs für vertrauenswürdig zu bestätigen.
D-TRUST Root CA	Wurzelzertifizierungsstelle, siehe Abschnitt 1.3.1.
D-TRUST Root PKI	Von der D-Trust GmbH betriebene PKI.
Distinguished Name	Ein aus mehreren Namensbestandteilen bestehender technischer Name, der in Zertifikaten die ausstellende CA und/oder den Zertifikatsnehmer innerhalb der Root PKI eindeutig beschreibt. Der Distinguished Name ist im Standard [X.501] definiert.
EE-Zertifikat	Siehe End-Entity-Zertifikat.
Elektronisches Siegel	Ein elektronisches Siegel dient als Nachweis, dass ein elektronisches Dokument von einer juristischen Person ausgestellt wurde und belegt den Ursprung und die Unversehrtheit des Dokuments.
Endanwender *(End-Entity /Subject)*	*Subject*, die Identität des Endanwenders ist mit dem Zertifikat und dem zugehörigen Schlüsselpaar verknüpft, siehe auch Abschnitt 1.3.3.
End-Entity-Zertifikat	Zertifikat, das nicht zum Zertifizieren anderer Zertifikate oder CRLs verwendet werden darf.
EV-Zertifikate	Zertifikat mit erweiterter Validierung des Zertifikatsnehmers (extended validation)
HR-DB	Human-Resource Datenbank (Personaldatenbank einer Organisation)
Postident Basic	Verfahren zur Identifizierung, angeboten von der Deutschen Post AG.
publicly trusted (PT) Vertrauensdienste	sind Vertrauensdienste gemäß den Vorgaben der Certificate Consumer Mitglieder des CA Browser/Forums in Kombination mit den Vorgaben des CA Browser/Forums.

publicly trusted certificate (PTC)	ist ein von einem publicly trusted (PT) Vertrauensdienst ausgestelltes Zertifikat.
Qualifizierter Vertrauensdienst	Elektronischer Dienst entsprechend Art. 3 Abs. 17 eIDAS
Qualifiziertes Zertifikat	ist ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat, das die Anforderungen des Anhangs I der eIDAS erfüllt
Registrierungsstelle *(Registration Authority - RA)*	Registration Authority – (RA), Einrichtung der PKI, die die Teilnehmeridentifizierung vornimmt, siehe Abschnitt 1.3.2.
Root Store	Der Speicher von vertrauenswürdigen Root CA Zertifikaten in Softwareanwendungskomponenten von prüfenden Drittherstellern.
sign-me	Ist ein Service der D-Trust GmbH für fernausgelöste Signaturprozesse
seal-me	Ist ein Service der D-Trust GmbH für fernausgelöste Siegelprozesse
Signaturkarte	Prozessorchipkarte, die für die Erzeugung elektronischer Signaturen und für andere PKI-Anwendungen benutzt werden kann.
Soft-PSE	Software Personal Security Environment, auch Software-Token genannt, enthalten das EE-Schlüsselpaar, das EE-Zertifikat sowie das Zertifikat der ausstellenden CA-Instanz.
Sonstige dritte Partei	Natürliche oder juristische Person, die z.B. den Widerruf eines Zertifikats beantragt.
Sperrung	Die Sperrung eines Zertifikats kann nicht rückgängig gemacht werden und ist daher einem Widerruf gleichzusetzen.
Sperrberechtigter Dritter *(Third party authorized to revoke)*	Natürliche oder juristische Person, die zum Widerruf eines Zertifikats berechtigt ist.
Statusabfragedienst	PKI-Dienstleistung zur Online-Abfrage über den Status eines Zertifikats (OCSP)
Subordinate CA (Sub-CA) bzw. Intermediate CA	Ist eine untergeordnete CA, die EE-Zertifikate und/oder weitere CA-Zertifikate ausstellt.
Token	Trägermedium für Zertifikate und Schlüsselmaterial.
Trustcenter	Der Sicherheitsbereich in den Räumen der D-Trust GmbH.
Trust Service Provider	Vertrauensdiensteanbieter (ehem. Zertifizierungs-diensteanbieter)

Verzeichnisdienst *(Repository service)*	PKI-Dienstleistung zum Online-Abrufen von Informationen, wie Zertifikaten und Sperrlisten, erfolgt i.d.R. über das LDAP-Protokoll.
Vertrauensdienst	Elektronischer Dienst entsprechend Art. 3 Abs. 16 eIDAS
Vertrauensdiensteanbieter *(Trust Service Provider - TSP)*	Anbieter von Vertrauensdiensten entsprechend Art. 3 Abs. 19 eIDAS
VideoIdent	Verfahren zur Identifizierung, angeboten von Identity TM AG
Widerruf	Zwischen den Begriffen Widerruf und Sperrung wird nicht unterschieden. Der Widerruf bzw. die Sperrung eines Zertifikats kann nicht mehr rückgängig gemacht werden.
Zertifikatsnehmer *(Subscriber)*	*Subscriber*, natürliche oder juristische Personen, die EE-Zertifikate beantragen und inne haben, siehe Abschnitt 1.3.3.
Zertifikatsnutzer *(Relying Party)*	Relying Party, natürliche oder juristische Personen, die Zertifikate nutzen, siehe Abschnitt 1.3.4.
Zertifikatsrichtlinie	Certificate Policy – (CP), siehe Abschnitt 1.1.
Zertifizierungsdiensteanbieter	Anbieter von Zertifizierungsdiensten. Wird gleichbedeutend mit dem Begriff Vertrauensdiensteanbieter verwendet.
Zertifizierungsstelle	Certification Authority – (CA), Instanz der Root PKI, siehe Abschnitt 1.3.1.

1.6.2 Abkürzungen

BAFIN	Bundesanstalt für Finanzdienstleistungsaufsicht
BDSG	Bundesdatenschutzgesetz
BRG	Baseline Requirements Guidelines
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
Cloud CPS	Certification Practice Statement der D-TRUST Cloud PKI
CN	Common Name
CP	Certificate Policy (Zertifikatsrichtlinie der D-Trust GmbH)
CPS	Certification Practice Statement
CSM CPS	Certification Practice Statement der D-TRUST CSM PKI
CRL	Certificate Revocation List

DN	Distinguished Name
DSGVO	Datenschutz-Grundverordnung
DVCP	Domain Validation Certificate Policy
EBA	European Banking Authority
EVCP	Extended Validation Certificate Policy
FIPS	Federal Information Processing Standard
FQDN	Fully qualified domain name
HSM	Hardware Security Module
ISO	International Organization for Standardization
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
NCA	National Competent Authority
NetSec-CAB	Network Security Requirements- CA/Browser Forum
NCP	Normalized Certificate Policy
NCP+	Normalized Certificate Policy requiring a secure user device
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVCP	Organizational Validation Certificate Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PSD2	Payment Services Directive 2
PSE	Personal Security Environment
PSP	Payment Service Provider
PSP_AI	Account Information Service Provider
PSP_AS	Account Servicing Payment Service Provider
PSP_IC	Payment Service Provider Issuing Card-based payment instruments
PSP_PI	Payment Initiation Service Provider
PUK	Personal Unblocking Key
QCP	Qualified Certificate Policy
QCP-l	Qualified Certificate Policy for Legal Persons
QCP-n	Qualified Certificate Policy for Natural Persons

QCP-w	Qualified Certificate Policy for Qualified Website-Authentication
QSCD	Qualified Signature Creation Device
QSealC	Qualified electronic Seal Certificate
QWAC	Qualified Website Authentication Certificate
RA	Registration Authority
RFC	Request for Comment
Root CPS	Certification Practice Statement der D-TRUST Root PKI
RTS	Regulatory Technical Standard for PSD2 strong customer authentication and common and secure open standards of communication
SSCD	Secure Signature Creation Device
SUD	Secure User Device
TLS	Transport Layer Security, auch bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (SSL)
TSP	Trust Service Provider
TSPS	Trust Service Practice Statement
URL	Uniform Resource Locator
UTF8	Unicode Transformation Format-8
V-PKI	Verwaltungs-PKI
VDA	Vertrauensdiensteanbieter

1.6.3 Referenzen

[AGB]	Allgemeine Geschäftsbedingungen der D-Trust GmbH, aktuelle Version
[BRG]	Baseline Requirements des CA/Browser Forum, CA/Browser Forum, Version 1.8.6, 2022-12-14
[CP V-PKI BSI]	„Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung" Version 3.2 vom 09.01.2003 und die dazugehörigen Ergänzungen und Änderungen Version 1.1 vom 29.01.2013 vom Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/VerwaltungsPKIVPKI/Dokumente/dokumente_node.html
[CPS]	Certification Practice Statement der D-TRUST PKI, D-Trust GmbH, aktuelle Version. Die geltende CPS wird im jeweiligen Zertifikat referenziert.

[eHealth Network]	eHealth Network Guidelines
	Technical Specifications for Digital Green Certificates; Volume 1; V1.0.5 (2021-04-21);
	Technical Specifications for Digital Green Certificates; Volume 5; Public Key Certificate Governance; V1.02 (2021-05-12)
[eIDAS]	Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
[ETSI-ALG]	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites; ETSI TS 119 312 V1.3.1 (2019-02)
[EN 319 401]	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers; ETSI EN 319 401 V2.2.1 (2018-04)
[EN 319 411-1]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements; ETSI EN 319 411-1 V1.2.2 (2018-04)
[EN 319 411-2]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2:Requirements for trust service providers issuing EU qualified certificates; ETSI EN 319 411-2 V2.2.2 (2018-04)
[EN 319 412]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures; ETSI EN 319 412-1 V1.1.1 (2016-02),
	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons; ETSI EN 319 412-2 V2.1.1 (2016-02),
	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons; ETSI EN 319 412-3 V1.1.1 (2016-02),
	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates; ETSI EN 319 412-4 V1.1.1 (2016-02),
	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements; ETSI EN 319 412-5 V2.2.3 (2020-01)
[EN 319 421]	Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers issuing Time-Stamps; ETSI EN 319 421 V1.1.1 (2016-03)
[EN 319 422]	Electronic Signatures and Infrastructures (ESI);Time-stamping protocol and time-stamp token profiles; ETSI EN 319 422 V1.1.1 (2016-03)
[EVGL]	Guidelines for the Issuance and Management of Extended Validation Certificates, CA/Browser Forum, Version 1.8.0, 2022-11-30

HADDEX Sanktionsliste	https://www.awr-portal.de/SubBoy/pdf.jsp?site=ReadMe&lang=en
[ISO 3166]	ISO 3166-1:1997: Codes for the representation of names of countries and their subdivisions - Part 1: Country codes
[NetSec-CAB]	CA / Browser Forum Network and Certificate System Security Requirements, Version 1.7, 05. April 2021
[RFC 2247]	Using Domains in LDAP/X.500 Distinguished Names, January 1998
[RFC 3647]	Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, November 2003
[RFC 5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Mai 2008
[RFC 6818]	Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, January 2013
[RFC 6960]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013
[RFC 6962]	Certificate Transparency, June 2013
[TR-03145-1]	Secure CA operation, Part 1: Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high', Version 1.1
[TR-02102-1]	"Kryptographische Verfahren: Empfehlungen und Schlüssellängen", Version 2020-01
[VDG]	Vertrauensdienstegesetz (Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist)
[X.501]	ITU-T RECOMMENDATION X.501, Information technology – Open Systems Interconnection – The Directory: Models, Version Oktober 2019
[X.509]	ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, Oktober 2019

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Der TSP veröffentlicht CRLs und Zertifikate im LDAP-Verzeichnis[10] unter: ldap://directory.d-trust.net

Der vollständige zertifikatsspezifische Link ist dem Zertifikat selbst zu entnehmen.

CA-Zertifikate, diese CP, TSPS, CPS und die Verpflichtungserklärung (Subscribers Agreement) werden auf den Webseiten der D-Trust GmbH veröffentlicht und können über den folgenden Link

[10] Der Abruf von Zertifikaten und Sperrlisten erfolgt über LDAPv3 gemäß RFC4511 ohne Security Layer.

im Repository abgefragt bzw. im PDF-Format heruntergeladen werden:
https://www.d-trust.net/de/support/repository

Zusätzlich sind im Repository Test-Webseiten für TLS Zertifikate sowie weitere Demozertifikate für weitere Produkte hinterlegt, über die der Zertifikatsstatus abgerufen werden kann.

Der TSP stellt einen Online-Dienst (OCSP) zur Abfrage des Sperrstatus von Zertifikaten der D-Trust zur Verfügung. Der Link ist dem Zertifikat zu entnehmen. Zusätzlich können Endanwender den Status ihrer Zertifikate über die folgende Webseite abfragen:

https://www.d-trust.net/de/support/ocsp-abfrage

Kundenspezifisch können abweichende Verfahren für die Übermittlung der Verpflichtungserklärung vereinbart werden.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Diese Regelungen sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

2.3 Häufigkeit von Veröffentlichungen

Diese Regelungen sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

2.4 Zugriffskontrollen auf Verzeichnisse

Zertifikate, Sperrlisten, TSPS, CPS und CPs können öffentlich und unentgeltlich 24x7 abgerufen werden. Es gibt keine Zugriffsbeschränkungen für lesenden Zugriff. Änderungen der Verzeichnis- und Webinhalte werden ausschließlich vom TSP vorgenommen.

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

2.5 Zugang und Nutzung von Diensten

Die Dienste der D-Trust GmbH werden öffentlich angeboten und sind für jedermann zugänglich. Sie können grundsätzlich von allen genutzt werden, die der AGB, der Verpflichtungserklärung, der Certificate Policy und dem jeweiligen Dienst zugehörigen Certification Practice Statemet der D-Trust GmbH zugestimmt haben (zusammengefasst: Terms & Conditions). Die D-Trust GmbH ist bestrebt ihre Dienste barrierearm anzubieten.

Als Richtlinie zur Erstellung weitgehend barrierefreier Internetinhalte dienen in erster Linie die Web Content Accessibility Guidelines (WCAG) des W3C.

3. Identifizierung und Authentifizierung

Die Identifizierung und Authentifizierung für Zertifikate der D-Trust GmbH erfolgt gemäß produkt- und kundenspezifischen Anforderungen sowie den Anforderungen der entsprechenden Zertifizierungen (z.B. eIDAS, EN 319 411-1 oder EN 319 411-2)

Diese Regelungen sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

4. Betriebsanforderungen

Die Betriebsanforderung für Zertifikate der D-Trust GmbH erfolgt gemäß produkt- und kundenspezifischen Anforderungen sowie den Anforderungen der entsprechenden Zertifizierungen (z.B. eIDAS, EN 319 411-1 oder EN 319 411-2)

Diese Regelungen sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

5. Nicht-technische Sicherheitsmaßnahmen

Der TSP etabliert nicht-technische Sicherheitsmaßnahmen, die die Anforderungen aus [EN 319 411-1], [EN 319 411-2], [EVGL] und [eIDAS] erfüllen.

Diese Regelungen sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

6. Technische Sicherheitsmaßnahmen

Der TSP etabliert technische Sicherheitsmaßnahmen, die die Anforderungen aus [EN 319 411-1], [EN 319 411-2], [EVGL] und [eIDAS] erfüllen. Aktuelle Angaben zu verwendeten Signatur- und Verschlüsselungsalgorithmen sind dem CPS Abschnitt 7.1.3 zu entnehmen.

Zertifikatsnehmer und Zertifikatsnutzer müssen vertrauenswürdige Computer und Software verwenden.

Diese Regelungen sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

7. Profile von Zertifikaten, Sperrlisten und OCSP

7.1 Zertifikatsprofile

Die von CAs der D-Trust-PKI ausgestellten Zertifikate erfüllen die Anforderungen der Standards ITU [X.509], IETF [RFC 5280] und IETF [RFC 6818], sowie der ETSI [ETSI EN 319 412]. Abweichungen werden ggf. in einem referenzierten Dokument beschrieben.

QCP, QEVCP-w und QNCP-w
Die ausgestellten qualifizierten Zertifikate erfüllen die Anforderungen aus [eIDAS] Anhang I, III und IV.

EVCP
Die ausgestellten EV-Zertifikate erfüllen die Anforderungen aus[EVGL].

Die Profile sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

7.2 Sperrlistenprofile

Die ausgestellten Sperrlisten erfüllen die Anforderungen der Standards ITU [X.509], IETF [RFC 5280] und IETF [RFC 6818].

Die Profile sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

7.3 Profile des Statusabfragedienstes (OCSP)

Der Statusabfragedienst ist konform zum Standard [RFC 6960].

Die Profile sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

Teil der Bundesdruckerei-Gruppe

8. Auditierung und andere Prüfungen

Diese Regelungen sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

9. Sonstige finanzielle und rechtliche Regelungen

9.1 Preise

9.1.1 Preise für Zertifikate

Die Vergütung für die in diesem Dokument beschriebenen Leistungen ist in der Preisliste bzw. in der jeweiligen Vereinbarung festgelegt.

9.1.2 Preise für den Zugriff auf Zertifikate

Die Abfrage von Zertifikaten im Verzeichnisdienst ist kostenlos.

9.1.3 Preise für den Widerruf oder Statusinformationen

Der Widerruf und das Abrufen von Statusinformationen sind kostenlos.

Ersatz für ein widerrufenes Zertifikat wird nicht geleistet.

9.1.4 Preise für andere Dienstleistungen

Soweit angeboten siehe Preisliste bzw. in der jeweiligen Vereinbarung.

Ist der Erwerb oder die zeitweise Überlassung von Hard- oder Software, insbesondere von Kartenlesegeräten, vereinbart, ist die vereinbarte Überlassung mit der Zahlung der vereinbarten Preise abgegolten einschließlich der erforderlichen einfachen Nutzungslizenz.

9.1.5 Regeln für Kostenrückerstattungen

Es gelten die jeweiligen Vereinbarungen mit dem Kunden bzw. [AGB].

9.2 Finanzielle Zuständigkeiten

9.2.1 Versicherungsdeckung

Die D-Trust GmbH verfügt über die nötigen Mittel sowie die finanzielle Stabilität, den Betrieb von Vertrauensdiensten ordnungsgemäß durchzuführen.

Der TSP erfüllt die Anforderung gemäß Artikel 24 Absatz 2 Buchstabe c [eIDAS] in Verbindung mit § 10 VDG und verfügt in Bezug auf das Haftungsrisiko für Schäden gemäß Artikel 13 über eine Haftpflichtversicherung gemäß § 10 VDG (jeweils 250 000 Euro für einen Schaden, der durch ein haftungsauslösendes Ereignis verursacht worden ist). Nicht-qualifizierte Vertrauensdienste sind durch eine Betriebshaftpflichtversicherung abgedeckt.

Der TSP erfüllt die Anforderungen von [EVGL] 8.4.

9.2.2 Andere Ressourcen für Betriebserhaltung und Schadensdeckung

Keine Vorgaben.

9.2.3 Versicherung oder Gewährleistung für Endnutzer

Keine Vorgaben.

9.3 Vertraulichkeit von Geschäftsdaten

9.3.1 Definition von vertraulichen Geschäftsdaten

Die Vertraulichkeit von Informationen kann vereinbart werden, sofern sie nicht bereits durch geltendes Recht definiert ist.

9.3.2 Geschäftsdaten, die nicht vertraulich behandelt werden

Als öffentlich gelten alle Informationen in ausgestellten und veröffentlichten Zertifikaten sowie die unter Abschnitt 2.2 genannten Daten.

9.3.3 Zuständigkeiten für den Schutz vertraulicher Geschäftsdaten

Der TSP kann im Einzelfall verpflichtet werden, die ihm als vertrauliche Geschäftsdaten benannten Daten durch entsprechende technische und organisatorische Maßnahmen gegen Preisgabe und Ausspähung zu schützen, und zu unterlassen, diese Daten zweckentfremdet zu nutzen oder sie Drittpersonen offen zu legen, soweit eine solche Verpflichtung nicht gegen das Gesetz verstößt. Im Rahmen der organisatorischen Maßnahmen werden die vom TSP eingesetzten Mitarbeiter in dem gesetzlich zulässigen Rahmen zur Geheimhaltung der vertraulichen Daten verpflichtet.

9.4 Datenschutz von Personendaten

9.4.1 Datenschutzkonzept

Der TSP arbeitet auf Basis eines Datenschutzkonzeptes, das den Schutz der personenbezogenen Daten regelt. Der TSP erfüllt die Anforderungen nach den Bundesdatenschutzgesetzen (BDSG) sowie ab dem 25.5.2018 der Datenschutz-Grundverordnung (DSGVO).

9.4.2 Definition von Personendaten

Es gilt Art. 4 Abs. 1 DSGVO.

9.4.3 Daten, die nicht vertraulich behandelt werden

Daten, die für ihre Zweckerfüllung veröffentlicht werden müssen (Sperrlisten, Statusinformationen, veröffentlichte Zertifikate), gehören nicht zu den vertraulich behandelten Daten.

9.4.4 Zuständigkeiten für den Datenschutz

Der TSP gewährleistet die Einhaltung des Datenschutzes. Alle Mitarbeiter des TSP sind auf die Einhaltung des Datenschutzes verpflichtet worden. Die interne Kontrolle erfolgt durch den betrieblichen Datenschutzbeauftragten, die externe Kontrolle erfolgt durch die Berliner Beauftragte für Datenschutz und Informationsfreiheit.

9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten

Dem Zertifikatsnehmer wird spätestens bei Antragstellung kenntlich gemacht, welche persönlichen Daten im Zertifikat enthalten sein werden. Zertifikate werden nur veröffentlicht, wenn der Zertifikatsnehmer dem bei der Antragstellung zustimmt.

Soweit keine andere Rechtsgrundlage herangezogen wird, willigt der Zertifikatsnehmer spätestens mit der Antragstellung in die Verwendung seiner personenbezogenen Daten ein bzw. hat die Einwilligung von ggf. betroffenen Dritten zu diesem Zeitpunkt eingeholt.

Alle für die Bereitstellung des Services nicht mehr benötigten personenbezogenen Daten werden umgehend gelöscht. Für personenbezogene Daten, die zum Zertifikatsnachweis benötigt werden, gelten die Fristen nach Abschnitt 5.5.2 des CPS.

9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften

Der TSP, als privatrechtliches Unternehmen, unterliegt der DSGVO, dem BDSG, dem Vertrauensdienstgesetz sowie den Gesetzen der Bundesrepublik Deutschland. Auskünfte werden entsprechend erteilt.

Eine Herausgabe von Informationen erfolgt bei einem gesetzlichen Anspruch gemäß §8 Abs. 2 VDG.

Endanwender wenden sich bei Auskunftsanfragen gemäß BDSG an die jeweils verantwortliche Stelle im Sinne des BDSG.

9.4.7 Andere Bedingungen für Auskünfte

Auskünfte anderer Art als unter Abschnitt 9.4.6 beschrieben werden nicht erteilt.

9.5 Gewerbliche Schutz- und Urheberrechte

9.5.1 TSP

Bestand und Inhalt von Urheber- und sonstigen Immaterialgüterrechten richten sich nach den allgemeinen gesetzlichen Vorschriften.

9.5.2 Zertifikatsnehmer

Der Zertifikatsnehmer verpflichtet sich zur Einhaltung geistiger Eigentumsrechte in den Antrags- und Zertifikatsdaten.

9.6 Zusicherungen und Garantien

9.6.1 Leistungsumfang des TSP

Es gelten die jeweiligen Vereinbarungen und [AGB] und diese CP. Soweit Garantien oder Zusicherungen betroffen sind, enthält die CP und das jeweils relevante CPS ausschließlich die für diesen Bereich ausdrücklich eingeräumten Garantien oder Zusicherungen.

Der TSP stellt sicher, dass die in dem jeweils zugehörigen CPS bzw. TSPS beschriebenen Verfahren implementiert sind und eingehalten werden.

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

Der TSP sorgt für die eindeutige Identifizierung der Zertifikatsnehmer und/oder (nach Vereinbarung) des Endanwenders und die Zuordenbarkeit des öffentlichen Schlüssels zum Endanwender gemäß den anwendbaren Vorgaben. Der TSP stellt sicher, dass ein in Zertifikaten verwendeter Name (DistinguishedName im Feld subject) innerhalb der D-Trust PKI und über den Lebenszyklus des Zertifikats hinaus stets eindeutig ist und stets dem gleichen Zertifikatsnehmer zugeordnet ist. Dadurch ist die eindeutige Identifizierung des Zertifikatsnehmers anhand des im Zertifikat verwendeten Namens (subject) gewährleistet.

Der TSP betreibt die CAs und stellt den Verzeichnisdienst und die Sperrinformationen bereit.

EVCP

Der TSP übernimmt keine Garantien im gesetzlichen Sinne nach dem BGB, unterwirft sich aber den Bestimmungen gemäß Abschnitt 7.1 [EVGL] hinsichtlich "Legal Existence", "Identity", "Right to Use Domain Name", "Authorization for EV Certificate", "Accuracy of

Teil der Bundesdruckerei-Gruppe

Information", "Subscriber Agreement", "Status", "Revocation" und gewährleistet deren Einhaltung.

Zusätzlich hält der TSP den Betrieb von Reportingmechanismen gemäß Abschnitt 4.9.3 [BRG] vor. Die Reportingmechanismen bieten Zertifikatsnehmern, Zertifikatsnutzern, Lieferanten von Anwendungssoftware und anderen betroffenen Dritten die Möglichkeit ihnen suspekte Zertifikate des TSP anzuzeigen. Der TSP geht dann dem Verdacht (z. B. Betrug, Phishing etc.) nach.

Austausch von Signaturerstellungseinheiten
Die D-Trust GmbH behält sich das Recht zum Austausch von Signaturerstellungseinheiten vor Ende des jeweiligen Nutzungszeitraums vor, sofern dies zur Wahrung des geltenden Rechts, berechtigter Interessen von D-Trust GmbH geboten ist oder sonst aus wichtigem Grund erforderlich wird, insbesondere wenn ein Austausch aus Sicherheitsgründen notwendig wird. Die D-Trust GmbH wird hierbei die Interessen der Kunden angemessen berücksichtigen.

Support- und Beratung
Soweit Support- und Beratungsleistungen erbracht werden, wird die D-Trust GmbH die hierzu eingesetzten Mitarbeiter auswählen und Support und Beratung innerhalb der gewöhnlichen Geschäftszeiten in der Zeit von Montag bis Freitag, 07.00 bis 18.00 Uhr, mit Ausnahme der bundeseinheitlichen Feiertage, im Wege des First Level Supports durch Kontakt via Internet oder Telefon anbieten, sofern nichts anderes vereinbart wurde. Soweit erforderlich ist der D-Trust GmbH zur Erbringung von Support- oder Beratungsleistungen Einsichtnahme in die entsprechenden Unterlagen oder Daten zu gewähren bzw. notwendige Auskünfte zu erteilen.

Der TSP kann Teilaufgaben an Partner oder an externe Anbieter auslagern. Der TSP stellt sicher, dass in diesem Fall die Bestimmungen von CP und CPS eingehalten werden.

9.6.2 Leistungsumfang der RA

Der TSP betreibt Registrierungsstellen (RA). Die RA erbringt Identifizierung und Registrierung. Es gelten die [AGB] sowie die Bestimmungen dieser CP.

9.6.3 Zusicherungen und Garantien des Zertifikatsnehmers

Es gelten die jeweiligen Vereinbarungen und [AGB] und diese CP.

QCP, QEVCP-w, QNCP-w, EVCP, OVCP, DVCP, NCP, LCP, V-PKI
Der Zertifikatsnehmer willigt in die Verpflichtungserklärung (Subscriber Agreement) ein, die Zusicherungen und Garantien des Zertifikatsnehmers beinhaltet.

EVCP, OVCP, DVCP, NCP, LCP, V-PKI
Der Zertifikatsnehmer verpflichtet sich, den Endanwender über seine Rechte und Pflichten zu informieren. Das Subscriber Agreement entspricht den Anforderungen von [EVGL] und [BRG].

EVCP
Das Subscriber Agreement entspricht den Anforderungen von Abschnitt 10.3 [EVGL].

9.6.4 Zusicherungen und Garantien des Zertifikatsnutzers

Zusicherungen und Garantien des Zertifikatsnutzers werden nach dieser CP nicht geregelt. Es entsteht zwischen dem TSP und dem Zertifikatsnutzer kein Vertragsverhältnis. Im Übrigen gelten die [AGB] sowie gesetzliche Bestimmungen.

9.7 Haftungsausschlüsse

9.7.1 Haftungsausschlüsse des TSP

Es gelten die jeweiligen Vereinbarungen und [AGB].

EVCP

Soweit EV-Zertifikate ausgegeben werden, gelten ergänzend die nachfolgenden Bestimmungen gemäß Abschnitt 18 [EVGL]:

Soweit der TSP ohne Abweichungen nach den Bestimmungen dieser Zertifikatsrichtlinie das EV-Zertifikat ausgegeben hat, ist seine Haftung für Schäden ausgeschlossen, die mit dem Zertifikat verursacht wurden.

Der TSP haftet insbesondere und ausdrücklich nicht für Schäden, die durch die Nutzung oder Nicht-Nutzung von Zertifikaten ohne Zertifizierung oder dem verschuldeten, fehlerhaften Einsatz elektronischer Signaturen entstehen.

Beeinträchtigungen der Funktion des Zertifikatsträgers, die sich aus der Nutzung ungeeigneter Hard- oder Software ergeben, fallen in den Risikobereich des Kunden.

9.8 Haftungsbeschränkungen

9.8.1 Beschränkung der Haftung

Die Haftung der D-Trust GmbH für die im Rahmen der Zertifizierungs- und Vertrauensdienste angebotenen Produkte ist entsprechend den Angaben in der Produktbeschreibung beschränkt.

Desweiteren gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

9.8.2 Haftung bei leichter Fahrlässigkeit

Unbeschadet Abschnitt 9.8.1 beschränkt sich die Haftung der D-Trust GmbH bei leicht fahrlässigen Pflichtverletzungen auf den nach der Art der Ware und den Zertifizierungs- und Vertrauensdiensten vorhersehbaren, vertragstypischen, unmittelbaren Durchschnittsschaden. Dies gilt auch bei leicht fahrlässigen Pflichtverletzungen der gesetzlichen Vertreter und Erfüllungsgehilfen. Gegenüber Unternehmern haftet die D-Trust GmbH bei leicht fahrlässiger Verletzung unwesentlicher Vertragspflichten nicht.

9.8.3 Keine Haftungsbeschränkung in besonderen Fällen

Die vorstehenden Haftungsbeschränkungen betreffen nicht Ansprüche des Kunden aus Produkthaftung. Weiter gelten die Haftungsbeschränkungen nicht bei der D-Trust GmbH zurechenbaren Körper- und Gesundheitsschäden oder bei Verlust des Lebens des Kunden. Abschnitt 9.8.1 bleibt unberührt.

9.8.4 Haftung bei Identifizierung

Die Erteilung von Zertifikaten bestätigt nur, dass zum Zeitpunkt der Antragstellung der erforderliche Identitäts- bzw. Legitimationsnachweis nach den in Deutschland anwendbaren gesetzlichen oder vertraglich vereinbarten Bestimmungen gegenüber der D-Trust GmbH ordnungsgemäß prüfbar erbracht wurde. Soweit der Kunde aufgrund des konkreten Vertragsverhältnisses mit der D-Trust GmbH selbst erforderliche Identifizierungen vornimmt, hat der Kunde die Vorgaben der D-Trust GmbH bei der Identifizierung einzuhalten. Verstößt er gegen diese Vorgaben, so hat er die D-Trust GmbH hinsichtlich der daraus resultierenden Ansprüche Dritter freizustellen.

9.8.5 Haftungsbestimmungen bei EV-Zertifikaten

Soweit bei der Ausstellung des EV-Zertifikats von den Bestimmungen dieser Zertifikatsrichtlinie abgewichen wurde, gelten die nachfolgenden Haftungsbestimmungen ebenfalls in Übereinstimmung mit den Vorgaben nach Abschnitt 18 [EVGL]:

Für die korrekte Antragsprüfung und den daraus resultierenden Inhalt der EV-Zertifikate haftet der TSP nur im Rahmen seiner Prüfungsmöglichkeiten. Die Erteilung von EV-Zertifikaten bestätigt nur, dass D-Trust zum Zeitpunkt der Antragstellung der erforderliche Identitäts- bzw. Legitimationsnachweis nach den Vorgaben dieser Zertifikatsrichtlinie erbracht wurde. Soweit eine ausgelagerte Registrierungsstelle erforderliche Identitätsprüfungen bezogen auf den Zertifikatsnehmer vornimmt, hat diese Registrierungsstelle die Vorgaben der D-Trust im Einklang mit den Bestimmungen dieser Zertifikatsrichtlinie bei der Identitätsprüfung einzuhalten, wozu sie sich verpflichtet. Verstößt die Registrierungsstelle gegen diese Vorgaben, so hat sie die D-Trust GmbH und die Bundesdruckerei GmbH hinsichtlich der daraus resultierenden Ansprüche des Zertifikatsnehmers oder sonstiger Dritter freizustellen. Selbiges gilt für die Fälle, dass der Zertifikatsnehmer als Registrierungsstelle selbst Identifizierung von Zertifikatsnehmern vornimmt, die zu seiner eigenen Organisation gehören.

Der Zertifikatsnehmer haftet für Schäden, die D-Trust GmbH und/ oder der Bundesdruckerei GmbH durch von ihm verursachte fehlerhafte Angaben im EV-Zertifikat, sowie durch von ihm verschuldeten, fehlerhaften Einsatz der EV-Zertifikate entstehen.

Im Übrigen ist in den vorgenannten Fällen die Haftung des TSP auf einen Betrag von maximal 2.000,00 US Dollars bzw. auf den entsprechenden EURO Betrag am Tag des Schadenseintritts pro EV-Zertifikat begrenzt.

9.8.6 Haftung des Kunden

Der Kunde haftet für Schäden, die der D-Trust GmbH durch von ihm verursachte fehlerhafte Angaben im Zertifikat, sowie durch verschuldeten, fehlerhaften Einsatz elektronischer Signaturen entstehen. Der Kunde haftet auch für Schäden, die durch die befugte oder unbefugte Benutzung der von der D-Trust GmbH erbrachten Dienste entstehen, wenn und soweit er diese Schäden zu vertreten hat.

9.8.7 Verjährung

Ist der Kunde Unternehmer verjähren Schadenersatzansprüche wegen eines Mangels an gelieferten Waren nach einem Jahr ab Ablieferung der Ware. Ist der Kunde Verbraucher verjähren Schadenersatzansprüche wegen eines Mangels an gelieferten Waren nach zwei Jahren ab Ablieferung der Ware. Dies gilt nicht, wenn der D-Trust GmbH grobes Verschulden vorwerfbar ist, sowie im Falle von der D-Trust GmbH zurechenbaren Körper- und Gesundheitsschäden oder bei Verlust des Lebens des Kunden.

9.9 Schadensersatz

9.9.1 Ansprüche des TSP gegenüber Zertifikatsnehmern

Soweit der Kunde Berichtigungen zu den in seiner Bestellung getätigten Angaben verlangt, ist er zur Tragung der daraus resultierenden Kosten gemäß der vereinbarten Preise verpflichtet, sofern er die Aufnahme der unrichtigen Angaben im Bestellformular zu vertreten hat, beispielweise im Fall verschuldeter, fehlerhafter Übermittlung.

Deweiteren gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

9.9.2 Ansprüche der Zertifikatsnehmer gegenüber dem TSP

Es gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

Der Kunde ist zur Aufrechnung nur mit unbestrittenen oder rechtskräftig festgestellten Ansprüchen berechtigt. Ihm steht die Geltendmachung eines Zurückbehaltungsrechts nur wegen Gegenansprüchen aus diesem Vertragsverhältnis zu.

Deweiteren gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

9.9.3 Ansprüche der Anwendungssoftwareanbieter (Application Software Suppliers) gegenüber dem TSP

EVCP, OVCP, DVCP, NCP, LCP

Ungeachtet der Haftungsbeschränkungen gegenüber Zertifikatnehmern und Zertifikatsnutzern (Relying Parties) ist sich der TSP darüber im Klaren und erkennt an, dass die Anbieter von Anwendungssoftware, die mit dem TSP einen Distributionsvertrag von Root-Zertifikaten abgeschlossen haben, keine Verpflichtung oder potenzielle Haftung des TSP gemäß diesen Anforderungen, oder anderweitig bestehender Haftung aufgrund der Ausstellung oder Pflege von Zertifikaten oder des Vertrauens darauf durch Zertifikatsnutzer (Relying Parties) oder anderen, übernehmen. Daher muss der TSP jeden Anbieter von Anwendungssoftware gegen Ansprüche Dritter verteidigen, sie entschädigen und schadlos halten gegenüber allen Ansprüchen, Schäden und Verlusten, die dieser Anbieter von Anwendungssoftware im Zusammenhang mit einem von dem TSP ausgestellten Zertifikat erleidet, unabhängig von der Ursache des Anspruchs oder des betroffenen Rechtskreises. Dies gilt jedoch nicht für Ansprüche, Schäden oder Verluste, die ein solcher Anbieter von Anwendungssoftware im Zusammenhang mit einem von dem TSP ausgestellten Zertifikat erleidet, wenn diese Ansprüche, Schäden oder Verluste direkt durch die Software dieses Anbieters von Anwendungssoftware verursacht wurden, die ein noch gültiges Zertifikat als nicht vertrauenswürdig anzeigt oder als vertrauenswürdig anzeigt: (1) ein Zertifikat, das abgelaufen ist, oder (2) ein Zertifikat, das widerrufen wurde (jedoch nur in Fällen, in denen der Status des Widerrufs aktuell online bei dem TSP verfügbar ist und die Anwendungssoftware diesen Status entweder nicht überprüft oder einen Hinweis auf den widerrufenen Status ignoriert hat).

9.10 Gültigkeitsdauer der CP und Beendigung der Gültigkeit

9.10.1 Gültigkeitsdauer der CP

Diese CP gilt ab dem Zeitpunkt der Veröffentlichung und bleibt wirksam bis zum Ablauf des letzten, unter dieser CP ausgestellten Zertifikates. Es gilt jeweils die Version der CP, die zum Zeitpunkt der Antragsstellung veröffentlicht ist.

9.10.2 Beendigung der Gültigkeit

Siehe Abschnitt 9.10.1.

9.10.3 Auswirkung der Beendigung

Siehe Abschnitt 9.10.1.

9.11 Individuelle Mitteilungen und Absprachen mit PKI-Teilnehmern

Mitteilungen des TSP an Zertifikatsnehmer werden an die letzte in den Unterlagen von D-Trust GmbH verzeichnete Anschrift oder der entsprechenden E-Mail-Adresse aus dem Antrag (elektronisch signiert) versendet.

9.12 Nachträge

9.12.1 Verfahren für Nachträge

Nachträge zu dieser CP werden in dieses Dokument eingearbeitet und unter demselben OID veröffentlicht. Editorische Änderungen werden markiert.

9.12.2 Benachrichtigungsmechanismen und –fristen

Keine Vorgaben.

9.12.3 Bedingungen für OID-Änderungen

Keine Vorgaben.

9.13 Bestimmungen zur Schlichtung von Streitfällen

Beschwerden bezüglich der Einhaltung oder Umsetzung dieser CP sind beim TSP (D-Trust GmbH, Kommandantenstr. 15, 10969 Berlin, Germany) schriftlich einzureichen. Soweit nicht innerhalb einer Frist von 4 Wochen nach Einreichung der Beschwerde abgeholfen wurde, gilt: Für sämtliche Rechtsbeziehungen zwischen der Bundesdruckerei, der D-Trust GmbH und Dritten, die Rechtsbeziehungen aus dieser CP herleiten, findet deutsches Recht unter Ausschluss des UN-Kaufrechts Anwendung.

9.14 Meldung von Sicherheitsvorfällen mit Zertifikaten

Siehe Abschnitt 1.5.2

9.15 Gerichtsstand

Der Gerichtstand für alle Rechtsstreitigkeiten ist Berlin, soweit der Kunde Kaufmann, eine juristische Person des öffentlichen Rechts bzw. ein öffentlich-rechtliches Sondervermögen ist oder in der Bundesrepublik Deutschland keinen allgemeinen Gerichtstand hat. Die D-Trust GmbH kann ihre Rechte auch am allgemeinen Gerichtstand des Kunden geltend machen. Ein etwaiger ausschließlicher Gerichtstand bleibt von der vorliegenden Vereinbarung unberührt.

9.15.1 Einhaltung geltenden Rechts

Diese CP unterliegt dem Recht der Bundesrepublik Deutschland sowie dem Recht der Europäischen Union. Für sämtliche Rechtsbeziehungen zwischen der D-Trust GmbH und dem Kunden findet deutsches Recht Anwendung. UN-Kaufrecht ist ausgeschlossen.

9.15.2 Erfüllungsort

Erfüllungsort für die D-Trust GmbH und den Kunden ist Berlin.

9.16 Sonstige Bestimmungen

9.16.1 Vollständigkeitserklärung

Folgende Dokumente sind Gegenstand der geltenden Vereinbarungen an denen PKI-Teilnehmer beteiligt sind:

- Vertrags- und Antragsunterlagen,
- die zum Zeitpunkt der Antragsstellung gültigen [AGB] bzw. die ggf. wirksam einbezogene Fassung derselben,
- die zum Zeitpunkt der Antragsstellung gültige CP
- bei qualifizierten Zertifikaten und qualifizierten Zeitstempeldiensten die zum Zeitpunkt der Antragsstellung gültige PKI Nutzerinformation.

Für TLS CAs, deren Sub- sowie Root-CAs gelten die folgenden Dokumente:

- Vertrags- und Antragsunterlagen,

- die zum Zeitpunkt der Antragsstellung gültigen [AGB], bzw. die ggf. wirksam einbezogene Fassung derselben,
- die zum Zeitpunkt der Antragsstellung gültige Version der [EVGL], die zum Zeitpunkt der Antragsstellung gültige CP.

9.16.2 Abgrenzungen

Keine Vorgaben.

9.16.3 Salvatorische Klausel

Durch etwaige Unwirksamkeit einer oder mehrerer Bestimmungen dieser CP wird die Wirksamkeit der übrigen Bestimmungen nicht berührt.

QEVCP-w, QNCP-w, EVCP, OVCP, DVCP
Die Bestimmungen der BRG 9.16.3 finden Anwendung.

9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

Es gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

9.16.5 Höhere Gewalt

Es gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

9.17 Andere Bestimmungen

9.17.1 Konflikt von Bestimmungen

Die unter 9.16.1 genannten Regelungen sind abschließend. Sie gelten untereinander in der in 9.16.1 aufgeführten Reihenfolge jeweils nachrangig.

9.17.2 Einhaltung von Ausfuhrgesetzen und -vorschriften

Die D-Trust GmbH lehnt alle Bedingungen des Kunden ab, durch die sich die D-Trust GmbH an einem Boykott, der über die geltenden gesetzlichen EU- und UN-Sanktionsbestimmungen hinausgeht, beteiligen oder hierauf gerichtete Erklärungen abgeben würde.

Leistungsverweigerungsrecht, Kündigung, Rücktritt, Haftungsausschluss
Setzt die von der D-Trust GmbH zu erbringende Lieferung oder Leistung eine vorherige Ausfuhr- oder Einfuhrgenehmigung einer Regierung und/oder staatlichen Behörde voraus oder ist die Lieferung oder Leistung aufgrund nationaler oder internationaler gesetzlicher Regelungen anderweitig beschränkt oder verboten, ist die D-Trust GmbH berechtigt, die Erfüllung ihrer Liefer-, Leistungs- oder Zahlungsverpflichtung so lange zu suspendieren, bis die Genehmigung erteilt oder die Beschränkung bzw. das Verbot aufgehoben ist. Ist die Lieferung oder Leistung von der Erteilung einer Ausfuhr- oder Einfuhrgenehmigung abhängig und wird diese nicht erteilt, ist die D-Trust GmbH jederzeit berechtigt, den Vertrag zu kündigen bzw. hiervon zurückzutreten. Die D-Trust GmbH haftet nicht für Lieferverzögerungen, die sich aus den in diesem Abschnitt genannten Gründen ergeben, oder dafür, dass eine Lieferung aufgrund von Exportvorschriften überhaupt nicht durchgeführt werden kann, es sei denn sie handelte vorsätzlich oder grob fahrlässig. Das gleiche gilt in Fällen des berechtigten Rücktritts oder der Kündigung.

Zusicherung
Mit der Annahme des Angebots, spätestens jedoch durch Annahme der Lieferung oder Leistung versichert der Kunde, dass er keine Geschäfte mit diesen Gütern betreiben wird, die gegen anwendbare gesetzliche Ausfuhrbestimmungen verstoßen, und insbesondere Weiterlieferungen, Verbringungen und Ausfuhren der gelieferten Güter nur unter Einhaltung

anwendbarer gesetzlicher Exportkontrollbestimmungen durchführen wird. Der Kunde verpflichtet sich, die obigen Verpflichtungen an seine Abnehmer weiter zu geben.

Ausschluss Mitwirkender
Der Kunde verpflichtet sich sicherzustellen, dass in der Vertragsabwicklung keine Personen, Organisationen oder Einrichtungen involviert sind oder hierdurch gefördert werden, die in den Sanktionslisten der Europäischen Gemeinschaft und der Vereinten Nationen (insb. den VO (EG) Nr. 881/2002; VO (EG) Nr. 2580/2001; VO (EU) Nr. 753/2011) aufgeführt sind. Dies gilt auch im Hinblick auf Personen, Organisationen oder Einrichtungen, die in den Sanktionslisten anderer Regierungen aufgeführt sind (insb. US Denied Persons List, US Entity List, US Specially Designated Nationals List, US Debarred List), sofern diese nicht unilateral über die VN- oder EU- Sanktionen hinausgehen.

Der Kunde versichert weiter, dass weder er selbst noch einer seiner Gesellschafter auf einer solchen Sanktionsliste gelistet sind, er nicht einer darauf befindlichen Person oder Körperschaft untersteht oder deren Teilhaber ist. Sollte der Kunde selbst oder einer seiner Gesellschafter oder eine Person oder Körperschaft, deren Teilhaber der Kunde ist, während der Dauer des Vertrages in eine Sanktionsliste aufgenommen werden, ist der Kunde verpflichtet, die D-Trust GmbH hiervon unverzüglich in Kenntnis zu setzen. Die D-Trust GmbH ist in einem solchen Fall jederzeit berechtigt, den Vertrag zu kündigen bzw. hiervon zurückzutreten, ohne dass der Kunde hieraus Ansprüche geltend machen kann.

Verstoß gegen exportkontrollrechtliche Vorschriften
Die D-Trust GmbH und der Kunde sind sich darüber einig, dass eine wirksame Exportkontrolle durch den Kunden eine wesentliche Voraussetzung für die Durchführung des Vertrags ist. Die D-Trust GmbH und der Kunde verstehen daher einen Verstoß gegen exportkontrollrechtliche Vorschriften im Zusammenhang mit D-TRUST Produkten stets als eine schwerwiegende Verletzung der Interessen der D-Trust GmbH. Dies gilt auch dann, wenn der Verstoß von Dritten herbeigeführt worden ist. In diesem Fall ist die D-Trust GmbH berechtigt, den Vertrag außerordentlich zu kündigen oder hiervon zurück zu treten. Der Kunde ist verpflichtet, die D-Trust GmbH von allen hierdurch entstehenden Schadensersatzansprüchen Dritter freizustellen. Er ist verpflichtet, der D-Trust GmbH Ersatz für sonstige Aufwendungen und Schäden, seien es materielle oder immaterielle, insbesondere auch Bußgeld- oder Strafzahlungen, zu leisten, die durch Nichteinhaltung der in dem Kapitel 9.17.2 aufgeführten Verpflichtungen entstehen.

Deweiteren gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

Teil der Bundesdruckerei-Gruppe