Certificate Policy of D-TRUST GmbH

ENGLISH

DEUTSCH

BUNDESDRUCKEREI

Certificate Policy of D-TRUST GmbH

Version 3.6

COPYRIGHT NOTICE AND USE LICENSE

Certificate Policy of D-TRUST GmbH
©2018 D-TRUST GmbH

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

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

Document history

Version	Date	Description
2.0	23/02/2015	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	05/10/2015	▪ Editorial changes and reference to certificates without a CPS entry
2.2	03/10/2016	▪ Change to EN 319 411-1
3.0	01/01/2017	▪ Introduction of qualified products according to EN 319 411-2 and eIDAS
3.1	01/04/2017	▪ Introduction of qualified time stamp service according to EN 319 421
3.2	01/10/2017	▪ Editorial changes and reference to the German Trust Services Act (VDG)
3.3	28/03/2018	▪ Editorial changes and adaption with Mozilla Root Store Policy 2.5 ▪ Adaptation of the use license to "Creative Commons Attribution" ▪ Additional OIDs for E.ON SE PKI and Uniper
3.4	08.05 2018	▪ Section 9.4 adapted to the amended Data Protection Act effective as of 25 May 2018
3.5	05.07.2018	▪ OID supplemented for the telematics infrastructure of the public health care system (medical profession ID card – HBA) ▪ Adapted to the requirements of the Baseline Requirements of the CA/Browser Forum, Version 1.5.7, 29.04.2018
3.6	11.10.2018	▪ Section 1.5.2 updated according Ballot SC6 (Part 2)

Contents

1. Introduction 5
1.1 Overview 5
1.2 Document Name and Identification 8
1.3 PKI Participants 8
1.4 Certificate Usage 9
1.5 Policy Administration 9
1.6 Definitions and Acronyms 10
2. Publication and Repository Responsibilities 15
2.1 Repositories 15
2.2 Publication of information concerning certificates 15
2.3 Publication frequency 15
2.4 Directory access control 15
3. Identification and Authentication (I&A) 16
4. Certificate Life-Cycle Operational Requirements 17
5. Facility, Management, and Operational Controls 18
6. Technical Security Controls 19
7. Certificate, CRL, and OCSP Profiles 20
7.1 Certificate Profile 20
7.2 CRL Profile 20
7.3 OCSP Profile 20
8. Compliance Audit and Other Assessment 21
9. Other Business and Legal Matters 22
9.1 Fees 22
9.2 Financial Responsibility 22
9.3 Confidentiality of Business Information 22
9.4 Privacy of Personal Information 23
9.5 Intellectual Property Rights 24
9.6 Representations and Warranties 24
9.7 Disclaimers of Warranties 25
9.8 Limitations of Liability 25
9.9 Indemnities 26
9.10 Term and Termination 26
9.11 Individual notices and communications with participants 26
9.12 Amendments 26
9.13 Dispute Resolution Procedures 26
9.14 Reporting of security poblems with certificates 27
9.15 Governing Law 27
9.16 Miscellaneous Provisions 27
9.17 Other Provisions 28

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

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

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.

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. Unless expressly stated, no warranties or guarantees in a legal sense are given on the basis of this CP.

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.

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

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 certificate.

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

The following policy OID is assigned for qualified certificates of the health-care telematics infrastructure (medical profession ID card – HBA) 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 policy 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 website certificates (SSL/TLS)
The following policy OID is assigned for certificates of certification class EN 319 411-2 QCP-w: 1.3.6.1.4.1.4788.2.150.4

Non-qualified website certificates (SSL/TLS)
The EV policy OID is assigned when EV certificates are used in accordance with EN 319 411-1 and [GL-BRO]: 1.3.6.1.4.1.4788.2.202.1

The general policy OID is assigned for OV certificates in accordance with EN 319 411-1: 1.3.6.1.4.1.4788.2.200.1

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

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

The following policy 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 policy OID is assigned for certificates without a certification class: 1.3.6.1.4.1.4788.2.500[1]

The following policy OID is assigned for certificates that are issued exclusively for test purposes: 1.3.6.1.4.1.4788.2.2.2[1]

All other certificates under this policy are given the following policy OID: 1.3.6.1.4.1.4788.2.200.1

Non-qualified certificates of the cloud PKI
The secret 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 policy OID is additionally assigned for certificates of certification class EN 319 411-1 LCP: 1.3.6.1.4.1.4788.2.250.1

Qualified certificates of the cloud PKI
The secret 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 policy 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 policy 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 policy 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

[1] 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.

1.2 Document Name and Identification

Document name:	Certificate Policy of D-TRUST GmbH
Identifier (OID):	This document has the policy OID: 1.3.6.1.4.1.4788.2.200.1
Version	3.6

1.3 PKI Participants

1.3.1 Certification authorities (CAs)

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

- Personal certificates for individuals (EE certificate)
- Seal certificates for legal entities (EE certificate), group certificates for groups of people, functions and IT processes (EE certificate)
- Machine certificates for IT processes and communication connections (SSL certificates/EE certificate) that serve a technical purpose but which can also suitably authenticate the end-entity system (subject)
- Machine certificates for IT processes and communication connections that serve a purely technical purpose. Certificate contents are not verified in this case.
- Certification authorities (subordinate CA certificates of the TSP) and
- 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 the 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

Relying parties are individuals 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 uses of certificates

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 uses of certificates

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.

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

1.4.3 Use of service certificates

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

The types of use include:

- CA certificates for CA and certificate issuance,
- Signing revocation information[2]
- Signing time stamps[3]

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.

contact details:

D-TRUST GmbH
CP and CPS editorial unit
Kommandantenstr. 15
10969 Berlin, Germany

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

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

[3] Time stamps are signed using separate service certificates.

1.5.2 Reporting security problems with certificates[4]

Subscribers should revoke certificates in the fastest manner possible, i.e. through unambiguous authentication via an online interface.

The TSP provides the following Internet page for reporting security problems with certificates (for instance, in the case of suspected misuse):

https://www.bundesdruckerei.de/en/Service-Support/Support/Security-issue-notification

To report a security problem with certificates, please complete the "Certificate Problem Report" form and send it to the e-mail address shown.

Within 24 hours following receipt of a Certificate Problem Report, D-TRUST GmbH will contact both the sender of the Certificate Problem Report and the subscriber (preliminary report). The Certificate Problem Report must be filled in completely and its contents must be understandable.

- As soon as an urgent security incident has been detected for an end-entity certificate (subscriber certificate/TLS-Certificate), the certificate will be revoked within 24 hours.
- If a justified, but not urgent reason for revocation of an end-entity certificate (subscriber certificate) was detected, the certificate will be revoked within five days.
- If a justified reason for revocation of a subordinate CA was found, revocation will be carried out within seven days.

The precise time of revocation will be defined as agreed to between D-TRUST GmbH, the subscriber and the requester of the revocation.

The reasons for certificate revocation are listed in the Baseline Requirements (BRG) of the CA/Browser Forum (refer to section 4.9).

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 Terms and names

CA certificate	The certificate issued for a certification authority for the signature key of the CA.
Certification Authority (CA)	Part of the root PKI, see section 1.3.1.
Certificate Policy (CP)	Certificate Policy.
Certification Practice Statement (CPS)	Declaration of implementation by the CA

[4] Only for SSL-/TLS-Certificate according EVCP, OVCP und QCP-w

Certificate Service Manager (CSM)	Web application for issuing advanced 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.
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].
D-TRUST root CA	Root certificate authority, see section 1.3.1.
D-TRUST root PKI	PKI operated by D-TRUST GmbH.
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 certificate	Certificate that may not be used to certify other certificates or CRLs.
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.
EV certificate	Certificate with extended validation of the subscriber
HR-DB	Human resource database (staff database of an organization)
Other third party	Individual or legal entity, for instance, requesting certificate revocation
Postident Basic	Identification method, offered by Deutsche Post AG.
Qualified certificate	A certificate issued by a qualified trust service provider that fulfils the requirements of Annex I of eIDAS
Qualified trust service	Electronic service according to Art. 3 (17) eIDAS
Registration authority	Registration authority (RA), part of the PKI that identifies the entities, refer to section 1.3.2.
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.
sign-me	A service provided by Bundesdruckerei GmbH for remotely triggered signature processes
Signature card	Processor smartcard that can be used to generate electronic signatures and for other PKI applications.

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 subordinate CA that issues EE certificates and/or further CA certificates.
Subscriber	An individual or a legal entity who/that applies for and holds the EE certificate, see section 1.3.3.
Third parties concerned	If a certificate contains details of subscriber's powers of representation, these are referred to as "third parties concerned".
Third party authorized to revoke	An individual or a legal entity authorized to revoke certificates.
Token	Medium for certificates and key material.
Trust service	Electronic service according to Art. 3 (16) eIDAS
Trust service provider	Formerly certification service provider; provider of trust services according to Art. 3 (19) eIDAS
VideoIdent	Identification method, offered by Identity TM AG

1.6.2 Abbreviations

BDSG	Federal Data Protection Act (Bundesdatenschutzgesetz)
BRG	Baseline Requirements Guidelines
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DSGVO	General Data Protection Regulation (Datenschutz-Grundverordnung)
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
NetSec-CAB	Network Security Requirements- CA/Browser Forum
NCP	Normalized Certificate Policy

NCP+	Normalized Certificate Policy requiring a secure user device
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVCP	Organizational Validation Certificate Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PSE	Personal Security Environment
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
RA	Registration Authority
RFC	Request for Comment
SSCD	Secure Signature Creation Device
SUD	Secure User Device
TSP	Trust Service Provider
URL	Uniform Resource Locator
UTF8	Unicode Transformation Format-8

1.6.3 References

[AGB]	General Terms and Conditions of Bundesdruckerei GmbH for the sale of trust services of D-TRUST, latest version
[BRG]	Baseline Requirements of the CA/Browser Forum, CA/Browser Forum, version 1.6.0, June 22, 2018
[CPS]	Certification Practice Statement of the D-TRUST PKI, D-TRUST GmbH, latest version. The applicable CPS is referenced in the respective certificate.
[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 V1.2.1 (2017-05)
[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 V1.1.1 (2016-02)
[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 V2.2.1 (2017-11)

[GL-BRO] Guidelines for Extended Validation Certificates, CA/Browser Forum, version 1.6.7, November 23, 2017

[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 1.1, October 01, 2017

[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

[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 August 2005

[X.509] ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, June 1997

2. Publication and Repository Responsibilities

2.1 Repositories

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

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

Moreover, CA certificates are published on the D-TRUST GmbH websites and can be requested using the following link:

https://www.bundesdruckerei.de/en/Roots-and-CRLs

(German Website: https://www.bundesdruckerei.de/de/2825-repository)

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.bundesdruckerei.de/en/OCSP-Request

(German Website: https://www.bundesdruckerei.de/de/2720-ocsp-abfrage)

The status of the certificates can be retrieved there for up to at least one year after they have expired. This CP and the subscriber agreement can be downloaded in PDF format from the application pages of the TSP: https://www.bundesdruckerei.de/en/Repository

(German Website: https://www.bundesdruckerei.de/de/2833-repository).

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

2.2 Publication of information concerning certificates

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

2.3 Publication frequency

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

2.4 Directory access control

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

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

3. Identification and Authentication (I&A)

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 CPS that belongs to the certificate.

4. Certificate Life-Cycle Operational Requirements

The operating 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 CPS that belongs to the certificate.

5. Facility, Management, and Operational Controls

The TSP sets up non-technical security measures that meet with the requirements of [EN 319 411-1], [EN 319 411-2] and [eIDAS].

These rules are described in the 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], [GL-BRO] 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 CPS that belongs to the certificate.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

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

QCP
The issued qualified certificates meet the requirements of [eIDAS], Annex I, III and IV.

EVCP
The issued EV certificates meet the requirements of [GL-BRO].

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

7.2 CRL Profile

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

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

7.3 OCSP Profile

The status request service complies with the [RFC 6960] standard.

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

8. Compliance Audit and Other Assessment

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

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate prices

The remuneration for the services described in this document are specified in the price list or in the respective agreement.

9.1.2 Prices for the access to certificates

Certificate requests in the repository service are free of charge.

9.1.3 Prices for revocations or status information

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

9.1.4 Prices for other services

When offered, see price list or the respective agreement.

9.1.5 Rules for cost refunds

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

9.2 Financial Responsibility

9.2.1 Insurance cover

D-TRUST GmbH has the necessary means and the financial stability 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) and, with a view to damage pursuant to Article 13, has taken out liability insurance pursuant to section 10 of VDG (€250,000 for each case of damage caused by the liability-triggering event). Non-qualified trust services are covered by business liability insurance.

The TSP meets the requirements of [GL-BRO] 8.4. The minimum insurance amount for professional liabilities totalling five million US dollars is warranted.

9.2.2 Other resources for maintaining operations and compensation for damage

No information

9.2.3 Insurance or warranty for end users

No information

9.3 Confidentiality of Business Information

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 2.2 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 purpose 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 Privacy of Personal Information

9.4.1 Data protection concept

The TSP works on the basis of a data protection concept that determines the protection of personal data. The TSP fulfils the requirements of the Federal Data Protection Act (BDSG) and of the General Data Protection Regulation (DSGVO) effective as of 25 May 2018.

9.4.2 Definition of personal data

Section 4 (1) of the General Data Protection Regulation is applicable.

9.4.3 Data not treated as confidential

Data which must be published in order to fulfil its purpose (certificate revocation lists, status information, published certificates) does not constitute data treated as confidential.

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 affected third parties 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, the Trust Services Act and the laws of the Federal Republic of Germany. Information is disclosed accordingly.

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 Intellectual Property Rights

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 Warranties

9.6.1 Scope of services by the TSP

Agreements, if any, and the General Terms and Conditions [AGB] apply together with this CP. Unless otherwise explicitly mentioned, the TSP does not issue any guarantees or representations in the legal sense.

The TSP ensures that the procedures described in the respective CPS are adhered to.

QCP, EVCP, OVCP, LCP

The TSP ensures the unambiguous identification of the subscriber and/or (according to the agreement) the subject and the allocation of the public key to the subject according to the applicable requirements. The TSP ensures that a name (DistinguishedName in the subject field) is always unambiguous within the D-TRUST PKI and beyond the lifecycle 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, a repository service and the revocation information service.

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 [GL-BRO] 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 operates with reporting mechanism pursuant to section 4.9.3 [BRG]. The reporting mechanisms offer subscriber, relying parties, application software suppliers and other third parties the possibility to report suspicious certificates of the TSP. The TSP then follows up on the relying party's suspicion (e.g. fraud, phishing, etc.).

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 Representations and guarantees of the subscriber

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

QCP, EVCP, OVCP, LCP

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

EVCP, OVCP, LCP

The subscriber undertakes to inform the subject of its rights and obligations. The subscriber agreement meets with the requirements of [GL-BRO].

EVCP

The subscriber agreement meets with the requirements of section 10.3 [GL-BRO].

9.6.4 Representations and guarantees of the relying party

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 of Warranties

9.7.1 TSP's disclaimer

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

EVCP

If EV certificates are issued, the following provisions pursuant to section 18 [GL-BRO] 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.

9.8 Limitations of Liability

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

In the event that the TSP deviated from the provisions of this Certificate Policy when issuing the EV certificate, the following liability provisions apply also in accordance with the requirements laid down in section 18 [GL-BRO]:

Bundesdruckerei GmbH's 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. If the registration authority violates these requirements, D-TRUST 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 checks the identity of subscribers who belong to its organization.

The subscriber is liable for damage which D-TRUST and/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 US $ 2,000.00 or the equivalent amount in euro on the day such damage occurred.

9.9 Indemnities

9.9.1 Claims by the TSP against subscribers

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.

9.10 Term and Termination

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 notices and communications with participants

Messages 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 information.

9.12.3 Conditions for OID changes

No information.

9.13 Dispute Resolution Procedures

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 4 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 shall be 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 of security poblems with certificates

See section 1.5.2

9.15 Governing Law

The General Terms and Conditions [AGB] apply.

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.

9.16 Miscellaneous Provisions

9.16.1 Completeness

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

- contract 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 and qualified time stamping services, the PKI user information valid at the time of application.

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

- contract and application documents,
- the General Terms and Conditions [AGB] valid at the time of application or any valid version included,
- the version of the [GL-BRO] and the CP valid at the time of application.

9.16.2 Differentiation

Not applicable

9.16.3 Partial invalidity

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

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

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

BUNDESDRUCKEREI

Zertifikatsrichtlinie der D-TRUST GmbH

Version 3.6

Erscheinungsdatum 11.10.2018
Datum des Inkrafttretens 11.10.2018

D-TRUST
EINE MARKE DER BUNDESDRUCKEREI

COPYRIGHT UND NUTZUNGSLIZENZ

Zertifikatsrichtlinie der D-TRUST GmbH
©2018 D-TRUST GmbH

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)

Inhaltsverzeichnis

1. Einleitung 5
1.1 Überblick 5
1.2 Name und Kennzeichnung des Dokuments 8
1.3 PKI-Teilnehmer 8
1.4 Verwendung von Zertifikaten 9
1.5 Administration der Policy 10
1.6 Begriffe und Abkürzungen 11
2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen 16
2.1 Verzeichnisse 16
2.2 Veröffentlichung von Informationen zu Zertifikaten 16
2.3 Häufigkeit von Veröffentlichungen 16
2.4 Zugriffskontrollen auf Verzeichnisse 16
3. Identifizierung und Authentifizierung 17
4. Betriebsanforderungen 18
5. Nicht-technische Sicherheitsmaßnahmen 19
6. Technische Sicherheitsmaßnahmen 20
7. Profile von Zertifikaten, Sperrlisten und OCSP 21
7.1 Zertifikatsprofile 21
7.2 Sperrlistenprofile 21
7.3 Profile des Statusabfragedienstes (OCSP) 21
8. Auditierung und andere Prüfungen 22
9. Sonstige finanzielle und rechtliche Regelungen 23
9.1 Preise 23
9.2 Finanzielle Zuständigkeiten 23
9.3 Vertraulichkeit von Geschäftsdaten 23
9.4 Datenschutz von Personendaten 24
9.5 Gewerbliche Schutz- und Urheberrechte 25
9.6 Zusicherungen und Garantien 25
9.7 Haftungsausschlüsse 26
9.8 Haftungsbeschränkungen 26
9.9 Schadensersatz 27
9.10 Gültigkeitsdauer der CP und Beendigung der Gültigkeit 27
9.11 Individuelle Mitteilungen und Absprachen mit PKI-Teilnehmern 27
9.12 Nachträge 27
9.13 Bestimmungen zur Schlichtung von Streitfällen 28
9.14 Meldung von Sicherheitsvorfällen mit Zertifikaten 28
9.15 Gerichtsstand 28
9.16 Sonstige Bestimmungen 28
9.17 Andere Bestimmungen 29

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

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 nicht ausdrücklich genannt, erfolgen auf Basis dieser CP keine Zusicherungen oder Garantien im Rechtssinne.

Die Kenntnis der in dieser CP beschriebenen Zertifizierungsverfahren und -regeln sowie der rechtlichen Rahmenbedingungen erlaubt es Zertifikatnutzern, 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 ist eng an den Internet-Standard RFC 3647 „Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework" angelehnt, um eine einfache Lesbarkeit und Vergleichbarkeit mit anderen CPs zu erreichen.

[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.

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 Zertifikat 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 keiner 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 keine Vertrauensdienste im Sinne der eIDAS sondern Dienste für technische Verfahren.

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 Policy-OID vergeben: 1.3.6.1.4.1.4788.2.150.1

Für qualifizierte Zertifikate der Telematikinfrastruktur des Gesundheitswesens (HBA)
Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QCP-n-qscd wird die folgende 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 Policy-OID vergeben: 1.3.6.1.4.1.4788.2.150.2

Qualifizierte Webseitenzertifikate (SSL/TLS)
Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QCP-w wird die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.150.4

Nichtqualifizierte Webseitenzertifikate (SSL/-TLS)
Für die EV-Policy-OID wird die Verwendung bei EV-Zertifikaten gemäß EN 319 411-1 und [GL-BRO] vergeben: 1.3.6.1.4.1.4788.2.202.1

Für OV-Zertifikate gemäß EN 319 411-1 wird die allgemeine Policy-OID vergeben: 1.3.6.1.4.1.4788.2.200.1

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

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

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

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

Für Zertifikate ohne Zertifizierungsklasse wird die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.500[2]

Für Zertifikate, die ausschließlich zu Testzwecken ausgestellt wurden, wird die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.2.2[2]

Alle anderen Zertifikate unter dieser Policy enthalten die Policy-OID: 1.3.6.1.4.1.4788.2.200.1

Nichtqualifizierte Zertifikate der Cloud PKI
Die geheimen 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 Policy-OID vergeben: 1.3.6.1.4.1.4788.2.250.1

Qualifizierte Zertifikate der Cloud PKI
Die geheimen 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 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 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 Policy-OID vergeben: 1.3.6.1.4.1.4788.2.100.3

[2] 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.

1.2 Name und Kennzeichnung des Dokuments

Dokumentname:	Zertifikatsrichtlinie der D-TRUST GmbH
Kennzeichnung (OID):	Dieses Dokument erhält die Policy-OID: 1.3.6.1.4.1.4788.2.200.1
Version	3.6

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), Gruppenzertifikate für Personengruppen, Funktionen und IT-Prozesse (EE-Zertifikat),
- Maschinenzertifikate für IT-Prozesse und Kommunikationsverbindungen (SSL-Zertifikate / EE-Zertifikat), die einen technischen Einsatzzweck haben aber auch das End-Entity-System (subject) entsprechend authentisieren können,
- Maschinenzertifikate für IT-Prozesse und Kommunikationsverbindungen, 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 Zertifikatnehmer (ZNE) und Endanwender (EE)

Diese Regelungen sind in der zum Zertifikat gehörenden CPS beschrieben.

1.3.4 Zertifikatnutzer (ZNU)

Zertifikatnutzer (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.

Weitere Regelungen sind in dem zum Zertifikat gehörenden CPS beschrieben.

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 Sperrauskünften[3]
- Signatur von Zeitstempeln[4]

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

[4] Zeitstempel werden durch gesonderte Dienstezertifikate signiert.

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.

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[5]

Der Zertifikatnehmer sollte für eine Sperrung den schnellsten Weg wählen. Der schnellste Sperrweg für den Zertifikatnehmer ist die Sperrung durch eine eindeutige Authentifizierung über die Online-Schnittstelle.

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

https://www.bundesdruckerei.de/de/Service-Support/Support/Zertifikatssicherheitsvorfall-melden

Das Formular „Certificate Problem Report" ist zur Meldung des Sicherheitsvorfalls mit Zertifikaten zu beschreiben und an den genannten E-Mail-Kontakt 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 Zertifikatnehmer Kontakt (preliminary report) auf. Der Certificate Problem Report muss vollständig und inhaltlich nachvollziehbar ausgefüllt werden.

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

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

Gründe, die eine Sperrung von Zertifikaten bedingen, werden in den Baseline Requirements (BRG) des CA/Browser Forums aufgeführt, siehe Abschnitt 4.9. CERTIFICATE REVOCATION AND SUSPENSION.

[5] Nur für SSL-/TLS-Zertifikate gemäß EVCP, OVCP und QCP-w

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 Zertfizierungspraktiken 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 Zertifikatnehmers für dritte Personen, so werden diese Stellen als „Betroffene Dritte" bezeichnet.
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)	Webanwendung zur Ausstellung fortgeschrittener Zertifikate
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 Zertifikatnehmer 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.
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.
sign-me	Ist ein Service der Bundesdruckerei GmbH für fernausgelöste Signaturprozesse
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. die Sperrung eines Zertifikats beantragt.
Sperrberechtigter Dritter *(Third party authorized to revoke)*	Natürliche oder juristische Person, die zur Sperrung 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
Zertifikatnehmer *(Subscriber)*	*Subscriber*, natürliche oder juristische Personen, die EE-Zertifikat beantragen und inne haben, siehe Abschnitt 1.3.3.
Zertifikatnutzer *(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

BDSG	Bundesdatenschutzgesetz
BRG	Baseline Requirements Guidelines
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DSGVO	Datenschutz-Grundverordnung
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
NetSec-CAB	Network Security Requirements- CA/Browser Forum
NCP	Normalized Certificate Policy
NCP+	Normalized Certificate Policy requiring a secure user device
OCSP	Online Certificate Status Protocol
OID	Object Identifier

OVCP	Organizational Validation Certificate Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PSE	Personal Security Environment
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
RA	Registration Authority
RFC	Request for Comment
SSCD	Secure Signature Creation Device
SUD	Secure User Device
TSP	Trust Service Provider
URL	Uniform Resource Locator
UTF8	Unicode Transformation Format-8
VDA	Vertrauensdiensteanbieter

1.6.3 Referenzen

[AGB]	Allgemeine Geschäftsbedingungen der Bundesdruckerei GmbH für den Verkauf von Vertrauensdiensten der D-TRUST, aktuelle Version
[BRG]	Baseline Requirements des CA/Browser Form, CA/Browser Forum, Version 1.6.0, 22.06.2018
[CPS]	Certification Practice Statement der D-TRUST PKI, D-TRUST GmbH, aktuelle Version. Die geltende CPS wird im jeweiligen Zertifikat referenziert.
[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 V1.2.1 (2017-05)
[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 V2.2.1 (2017-11)

[GL-BRO] Guidelines for Extended Validation Certificates, CA/Browser Forum, Version 1.6.7, 23. November 2017

[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 1.1, 01. Oktober 2017

[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

[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 August 2005

[X.509] ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, June 1997

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

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

Der vollständige zertifikatsspezifische Link ist dem Zertifikat selbst zu entnehmen.

Zusätzlich werden CA-Zertifikate auf den Webseiten der D TRUST GmbH veröffentlicht und können über den folgenden Link abgefragt werden:
https://www.bundesdruckerei.de/de/2825-repository

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.bundesdruckerei.de/de/2720-ocsp-abfrage.

Der Status der Zertifikate kann dort bis mindestens ein Jahr nach Ablauf der Gültigkeit der Zertifikate abgerufen werden. Diese CP und die Verpflichtungserklärung (Subscribers Agreement) können im PDF-Format von den Antragsseiten des TSP herunter geladen werden:

https://www.bundesdruckerei.de/de/2833-repository.

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

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

3. Identifizierung und Authentifizierung

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], [GL-BRO] 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], [GL-BRO] und [eIDAS] erfüllen. Aktuelle Angaben zu verwendeten Signatur- und Verschlüsselungsalgorithmen sind dem CPS Abschnitt 7.1.3 zu entnehmen.

Zertifikatnehmer und Zertifikatnutzer 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

Die ausgestellten qualifizierten Zertifikate erfüllen die Anforderungen aus [eIDAS] Anhang I, III und IV.

EVCP

Die ausgestellten EV-Zertifikate erfüllen die Anforderungen aus[GL-BRO].

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.

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 sind 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 Sperrungen oder Statusinformationen

Sperrungen und das Abrufen von Statusinformationen sind kostenlos.

9.1.4 Preise für andere Dienstleistungen

Soweit angeboten siehe Preisliste bzw. in der jeweiligen Vereinbarung.

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 [GL-BRO] 8.4. Die Mindestversicherungshöhe für Vermögenschäden („professional liabilities“) in Höhe von fünf Millionen US Dollars wird gewährleistet.

9.2.2 Andere Ressourcen für Betriebserhaltung und Schadensdeckung

Keine Angaben.

9.2.3 Versicherung oder Gewährleistung für Endnutzer

Keine Angaben.

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

Soweit keine andere Rechtsgrundlage herangezogen wird, willigt der Zertifikatnehmer 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.

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 0 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 Zertifikatnehmer

Der Zertifikatnehmer 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 nicht ausdrücklich erwähnt, räumt der TSP keine Garantien oder Zusicherungen im Rechtssinne ein.

Der TSP stellt sicher, dass die in dem jeweils zugehörigen CPS beschriebenen Verfahren eingehalten werden.

QCP, EVCP, OVCP, LCP

Der TSP sorgt für die eindeutige Identifizierung der Zertifikatnehmer 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 Zertifikatnehmer zugeordnet ist. Dadurch ist die eindeutige Identifizierung des Zertifikatnehmers 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 [GL-BRO] hinsichtlich "Legal Existence", "Identity", "Right to Use Domain Name", "Authorization for EV Certificate", "Accuracy of 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 Zertifikatnehmern, Zertifikatnutzern, 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.

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 Zertifikatnehmers

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

QCP, EVCP, OVCP, LCP
Der Zertifikatnehmer willigt in die Verpflichtungserklärung (Subscriber Agreement) ein, die Zusicherungen und Garantien des Zertifikatnehmers beinhaltet.

EVCP, OVCP, LCP
Der Zertifikatnehmer verpflichtet sich, den Endanwender über seine Rechte und Pflichten zu informieren. Das Subscriber Agreement entspricht den Anforderungen von [GL-BRO].

EVCP
Das Subscriber Agreement entspricht den Anforderungen von Abschnitt 10.3 [GL-BRO].

9.6.4 Zusicherungen und Garantien des Zertifikatnutzers

Zusicherungen und Garantien des Zertifikatnutzers werden nach dieser CP nicht geregelt. Es entsteht zwischen dem TSP und dem Zertifikatnutzer 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 [GL-BRO]:

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 entstehen.

9.8 Haftungsbeschränkungen

Es gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

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 [GL-BRO]:

Für die korrekte Antragsprüfung und den daraus resultierenden Inhalt der EV-Zertifikate haftet der TSP der Bundesdruckerei GmbH 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 D-TRUST und die Bundesdruckerei GmbH hinsichtlich der daraus resultierenden Ansprüche des Zertifikatsnehmers oder sonstiger Dritter freizustellen. Selbiges gilt für die Fälle, dass der Zertifikatnehmer als Registrierungsstelle selbst Identifizierung von Zertifikatsnehmern vornimmt, die zu seiner eigenen Organisation gehören.

Der Zertifikatnehmer haftet für Schäden, die D–TRUST 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.

9.9 Schadensersatz

9.9.1 Ansprüche des TSP gegenüber Zertifikatnehmern

Es gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

9.9.2 Ansprüche der Zertifikatnehmer gegenüber dem TSP

Es gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

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 Zertifikatnehmer 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 Angaben.

9.12.3 Bedingungen für OID-Änderungen

Keine Angaben.

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

Es gelten die [AGB].

9.15.1 Einhaltung geltenden Rechts

Diese CP unterliegt dem Recht der Bundesrepublik Deutschland sowie dem Recht der Europäischen Union.

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 SSL 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 [GL-BRO], die zum Zeitpunkt der Antragsstellung gültige CP.

9.16.2 Abgrenzungen

entfällt

9.16.3 Salvatorische Klausel

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

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

Es gelten die etwaigen jeweiligen Vereinbarungen und [AGB].