Certificate Policy of D-TRUST GmbH

Version 3.4

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

Contents

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

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

[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.

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

1.2 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	3.4

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 (lower-level 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]

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

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

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.

1.5.2 Contact partner/contact person/secretariat

The following contact addresses are available:

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

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
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
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).
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 1.5.4, October 4, 2017
[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 1: General requirements; ETSI EN 319 411-2 V2.1.1 (2016-02)
[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 (2016-02)
[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.

To report security incidents with security certificates issued by the TSP (for instance, suspected misuse), the TSP operates the following website:

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

The security incident can be described using the notification form provided and sent to the e-mail contact specified there.

9.14 Governing Law

The General Terms and Conditions [AGB] apply.

9.14.1 Compliance with Applicable Law

This CP is subject to the laws of the Federal Republic of Germany and the laws of the European Union.

9.15 Miscellaneous Provisions

9.15.1 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.

9.15.2 Differentiation

Not applicable

9.15.3 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.

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

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

9.15.5 Force majeure

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

9.16 Other Provisions

9.16.1 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.

9.16.2 Compliance with export laws and regulations

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