Certificate policy of D-TRUST GmbH

Version 2.1

Date of issue	05 October 2015
Effective date	05 October 2015

D-TRUST EINE MARKE DER BUNDESDRUCKEREI

Copyright notice

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 February 2015	As part of the reorganisation 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	5 October 2015	Editorial changes and reference to certificates without CPS entry

Contents

1. Introduction

1.1 Overview

This document describes the certificate policy (CP) of the PKI 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 with whom the TSP maintains properly documented agreements and an established contractual relationship at the time services are provided.

The TSP managers or the management of the TSP are responsible for adherence to this document.

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 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 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 CPS that belongs to the certificate.

If no CPS is stored in the certificate in question, the implementation of the rules required in this CP is at the discretion of the TSP. Certificates which do not contain a CPS are not subject to certification according to ETSI TS 102 042 or the German Act on Digital Signature [SigG].

Under this policy, D-TRUST GmbH offers various products that meet the requirements of the certificate policy in terms of their special product properties.

Compliance with these requirements is described in a Certification Practice Statement (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.

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

The EV policy OID for EV certificates is assigned according to **Fehler! Verweisquelle konnte nicht gefunden werden.**:
1.3.6.1.4.1.4788.2.202.1

For certificates in certification class ETSI TS 102 042 LCP, the following policy OID is assigned:
1.3.6.1.4.1.4788.2.200.2

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

1.2 Name and identification of the document

Document name:	Certificate Policy of D-TRUST GmbH
Identifier (OID):	This document contains the policy OID: 1.3.6.1.4.1.4788.2.200.1
Version	2.1

1.3 PKI entities

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 and legal entities (EE certificate)
- Team certificates for groups of individuals, functions and IT processes (EE certificate)
- Machine certificates for IT processes and communication connections (SSL certificates/EE certificate)
- Certification authorities (lower-level CA certificates of the TSP)

Root authorities issue certificates exclusively with the extension basicConstraints: cA=TRUE (CA certificate). Lower-level CAs issue EE certificates and/or further CA certificates. The name of the certification authority is shown in the "issuer" field of the certificates issued and in the CRLs.

1.3.2 Registration authorities (RAs)

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

1.3.3 Subscriber

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 Use of certificates

1.4.1 Permitted uses of certificates

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

1.4.2 Forbidden uses of certificates

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

1.5 Updating the CP/CPS

1.5.1 Responsibility for the document

This CP is maintained and updated by D-TRUST GMBH. The TSP manager 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 **Fehler! Verweisquelle konnte nicht gefunden werden.**).

1.6 Terminology and abbreviations

1.6.1 German terms and names

Third parties concerned	If a certificate contains details of subscriber's powers of representation, these sections are referred to as "third parties concerned".
CA certificate	The certificate issued for a certification authority for the signature key of the CA
Cross-certificate	Certificate that is used in order to confirm that other CAs are trusted.
D-TRUST root CA	Root certification authority, see section 1.3.1.
D-TRUST root PKI	PKI operated by D-TRUST GMBH.
EE certificate	See end-entity certificate.

End entity/Subject	The identity of the subject/end entity is linked to the certificate and the pertinent key pair, see also section 1.3.3.
End-entity certificate	Certificate that may not be used to certify other certificates or CRLs.
EV certificate	Certificate with extended validation of the subscriber
Postident Basic	Identification method, offered by Deutsche Post AG.
Registration Authority	Registration authority (RA), an instance of the PKI that identifies the entities, refer to section 1.3.2.
Signature card	Processor smartcard that can be used to generate electronic signatures and for other PKI applications.
Third party authorised to revoke	An individual or a legal entity authorised to revoke certificates.
Status request service	PKI service for online requests regarding the status of a certificate (OCSP).
Repository service	PKI service for online requests for information, such as certificates and revocation lists, usually carried out via LDAP protocol.
Subscriber	An individual or a legal entity who/that applies for and holds the EE certificate, see section 1.3.3.
Relying party	An individual or a legal entity who/that uses certificates, see section 1.3.4.
Certificate policy	Certificate policy (CP), see section 1.1.
Certification Service Provider	Provider of certification services
Certification Authority	Certification Authority (CA), an instance of the PKI that issues certificates; see section 1.3.1.

1.6.2 English terms

Certification Authority (CA)	Certification Authority (CA), 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 issuance of advanced certificates

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].
Registration Authority (RA)	Registration authority, an instance of the PKI that identifies the entities, refer to section 1.3.2.
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 instance.
Token	Medium for certificates and key material.
Trust center	The security zone on the premises of D-Trust GmbH.
Trust Service Provider	Formerly certification service provider

1.6.3 Abbreviations

BRG	Baseline Requirements Guidelines
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
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
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
CSP	Certification Service Provider

1.6.4 References

[AGB]	General Terms and Conditions of Bundesdruckerei GmbH for the sale of certification services of D-Trust, latest version
[BRG]	Baseline requirements of the CA/Browser Forum, Version 1.3.0, 16.04.2015
[CPS]	Certification Practice Statement of the D-TRUST PKI, D-Trust GmbH, latest version. The applicable CPS is referenced in the respective certificate.
[Co-PKI]	Common PKI Specification, version 2.0 from 20 January 2009
[ETSI-ALG]	ETSI, Algorithms and Parameters for Secure Electronic Signatures, TS 102 176-1 V2.1.1, Jul. 2011
[ETSI-F]	ETSI, Technical Specification Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, ETSI TS 102 042 V2.4.1, Feb. 2013
[GL-BRO]	Guidelines for Extended Validation Certificates, CA/Browser Forum, Version 1.5.6, 25 June 2015

[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 1.0, 1.1.2013
[RFC 2247]	Using Domains in LDAP/X.500 Distinguished Names, January 1998
[RFC 2560]	X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP, June 1999
[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
[SigG] (German abbreviation)	Act on Digital Signature (Act on the Boundary Conditions for Electronic Signatures (Digital Signature Act – SigG) in the version dated 16 May 2001 (Federal Gazette I p. 876), last amended by Article 4 of the Act from 17 July 2009 (Federal Gazette. I p. 2091)
[SigV] (German abbreviation)	Ordinance on the electronic signature of 16 November 2001 (Federal Gazette I, p. 3074), last amended by ordinance of 5 November 2010 (Federal Gazette I, p. 1542)
SiKo-DTR]	Security concept D-TRUST GMBH, a certification service provider in compliance with the Act on Digital Signature
[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. Responsibility for repositories and publications

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/de/53-support-fuer-behoerden-buerger-unternehmen.

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/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/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 document, can be issued on request against proof of a legitimate interest.

3. Identification and authentication

Identification and authentication of D-TRUST GmbH certificates are carried out according to product and customer-specific requirements as well as the requirements for the respective certification (e.g. Act on Digital Signature or ETSI TS 102 042).

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

4. Operational requirements

The operational requirements for D-TRUST GmbH certificates are carried out according to product and customer-specific requirements as well as the requirements for the respective certification (e.g. Act on Digital Signature or ETSI TS 102 042).

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

5. Non-technical security measures

The TSP sets up non-technical security measures that meet with the requirements of **Fehler! Verweisquelle konnte nicht gefunden werden.** and **Fehler! Verweisquelle konnte nicht gefunden werden.**.

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

6. Technical security measures

The TSP sets up technical security measures that meet with the requirements of **Fehler! Verweisquelle konnte nicht gefunden werden.** and **Fehler! Verweisquelle konnte nicht gefunden werden.**. The latest information on the signature and encryption algorithms used can be found in the **Fehler! Verweisquelle konnte nicht gefunden werden.**, 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. Profiles of certificates, revocation lists and OCSP

7.1 Certificate profiles

The certificates issued by the CAs of the D-TRUST root PKI meet the requirements of ITU standard **Fehler! Verweisquelle konnte nicht gefunden werden.** and IETF standard **Fehler! Verweisquelle konnte nicht gefunden werden.**, as well as the Common PKI 2.0 **Fehler! Verweisquelle konnte nicht gefunden werden.** profile. Deviations are described, when necessary, in a referenced document.

EVCP
: EV certificates issued in the D-TRUST root PKI meet with the requirements of **Fehler! Verweisquelle konnte nicht gefunden werden.**.

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

7.2 Certificate revocation list profiles

The revocation lists meet the requirements of ITU standard **Fehler! Verweisquelle konnte nicht gefunden werden.** and IETF standard **Fehler! Verweisquelle konnte nicht gefunden werden.**, as well as the Common PKI 2.0 **Fehler! Verweisquelle konnte nicht gefunden werden.** profile.

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

7.3 Profiles of the status request service (OCSP)

The status request service complies with standard [RFC 2560] and meets the requirements of the Common PKI 2.0 **Fehler! Verweisquelle konnte nicht gefunden werden.** profile.

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

8. Checks and other evaluations

The CAs of D-TRUST are operated by the TSP in the same rooms as the CA of D-TRUST GMBH for issuing qualified certificates with provider accreditation according to the German Act on Digital Signature.

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

9. Other financial and legal provisions

9.1 Prices

9.1.1 Certificate prices

Remuneration for certification is laid down 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, refer to the 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 responsibilities

9.2.1 Insurance cover

TSP D-TRUST GMBH has insurance cover pursuant to Section 12 of the Act on Digital Signature [§ 12 SigG]:

"The certification service provider is obliged to take out suitable insurance cover, enabling it to meet with its statutory obligation to compensate for damage which can arise if such certification service provider fails to fulfil the requirements of the law or the ordinance pursuant to Section 24 or if its products for qualified signatures or other technical security measures fail. [...]"

The TSP meets the requirements of **Fehler! Verweisquelle konnte nicht gefunden werden.** 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 data

9.3.1 Definition of confidential business data

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

9.3.2 Business data not treated as confidential

All information in issued and published certificates as well as the data referred to in section 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 organisational 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 organisational measures, the employees working for TSP will be obliged to maintain confidentiality regarding the data in as far as permitted by law.

9.4 Protection of personal data

9.4.1 Data protection concept

The TSP works on the basis of an auditable security concept that determines the protection of confidential personal data (in short: personal data). The TSP fulfils the requirements pursuant to sections 4a, b, section 9 and sections 27 cf. of the Federal Data Protection Act.

9.4.2 Definition of personal data

Section 3 (2) of the Federal Data Protection Act is applicable.

9.4.3 Data not treated as confidential

Data which is explicitly contained in certificates, in certificate revocation lists and in status information 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

At the time of application, the subscriber is 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 applications.

All other personal data that is no longer needed is immediately deleted. Personal data which is needed for certificate proof is subject to the deadlines foreseen in section 5.5.2 of the **Fehler! Verweisquelle konnte nicht gefunden werden.**.

9.4.6 Information pursuant to legal or government requirements

The TSP, as a company under private law, is subject to the Federal Data Protection 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 Industrial property and copyrights

9.5.1 TSP

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

9.5.2 Subscriber

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

9.6 Representations and guarantees

9.6.1 Scope of services by the TSP

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

Class 3, Class 2, 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.

The TSP ensures that the procedures described in sections 4, 3.2 and 3.3 of the **Fehler! Verweisquelle konnte nicht gefunden werden.** are adhered to.

The TSP ensures that a name (*DistinguishedName* in the *subject* field) is always unambiguous within the D-TRUST root PKI and beyond the life cycle of the certificate and that it is always assigned to the same subscriber. This ensures the unambiguous identification[1] 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.

Class 3 EV certificates, 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 6.2 **Fehler! Verweisquelle konnte nicht gefunden werden.** 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 an EV reporting unit pursuant to section 11.3 **Fehler! Verweisquelle konnte nicht gefunden werden.**. The reporting unit offers relying parties the possibility to report suspicious EV 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 **Fehler! Verweisquelle konnte nicht gefunden werden.** are observed.

[1] See footnote **Fehler! Textmarke nicht definiert.** on page 17.

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.

Class 3, Class 2, EVCP, OVCP, LCP

The subscriber agrees to the subscriber agreement containing the subscriber's representations and guarantees. The subscriber undertakes to inform the subject of its rights and obligations. The subscriber agreement meets with the requirements of **Fehler! Verweisquelle konnte nicht gefunden werden.**.

Class 3 EV certificates, EVCP

The subscriber agreement meets with the requirements of section 9.3 **Fehler! Verweisquelle konnte nicht gefunden werden.**.

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

9.7.1 TSP's disclaimer

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

Class 3 EV certificates, EVCP

If EV certificates are issued, the following provisions pursuant to section 15.2 **Fehler! Verweisquelle konnte nicht gefunden werden.** 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.

9.8 Limitations of liability

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 15.2 **Fehler! Verweisquelle konnte nicht gefunden werden.**:

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 authorisation 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/or 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 organisation.

The subscriber is liable for damage which D-TRUST 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 Damages

9.9.1 Claims by the TSP against subscribers

If the subscriber deliberately provides fraudulent or incorrect data to the RA, the subscriber will bear statutory liability for damages. Furthermore, the claims arising from the respective agreements and the General Terms and Conditions [AGB] also apply.

9.9.2 Claims by the subscriber against the TSP

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

9.10 Validity of the CP and termination of validity

9.10.1 Validity of the CP

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

9.10.2 Termination of validity

See section 9.10.1.

9.10.3 Effect of termination

See section 9.10.1.

9.11 Individual communications to and agreements with PKI entities

Messages by the TPS 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 provisions

Complaints regarding adherence to or implementation of this CP should be submitted in writing to the TSP (D-TRUST GMBH, Kommandantenstr. 15, 10969 Berlin, Germany). If the matter has not been resolved within 4 weeks after the complaint was submitted, the following applies: Each of the parties is at liberty to refer the matter to a German court of law.
Moreover, the TSP operates an EV reporting unit pursuant to section 9.6.1. Suspected misuse of D-TRUST EV certificates can be reported to the following e-mail address: ev-support@d-trust.net.

9.14 Place of jurisdiction

The General Terms and Conditions [AGB] apply.

9.15 Compliance with applicable law

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

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 version thereof that becomes subsequently valid,
- the CP in effect at the time of the 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 version thereof that becomes subsequently valid,
- the version of the **Fehler! Verweisquelle konnte nicht gefunden werden.** and the CP valid at the time of application.

9.16.2 Differentiation

Not applicable

9.16.3 Partial invalidity

In the event that any provision of this CP or the application thereof is found to be invalid or non-enforceable for whatever reason and to whatever extent, the remaining provisions of this CP (as well as the application of the invalid or non-enforceable provision to other persons or under other conditions) shall be interpreted in such a manner that the intentions of the parties are considered to the maximum extent possible.

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

The export of certain software that is used in conjunction with public certification services by D-TRUST GMBH may require approval by the respective authorities. The parties will observe the applicable export laws and regulations.

The use of public certification services by D-TRUST GMBH is subject to various laws of the Federal Republic of Germany. In any case, D-TRUST GMBH reserves the right to initiate criminal proceedings with regard to any violations of D-TRUST GMBH's public certification services.