

D-TRUST-Root PKI Certificate Policy

Version 1.2_EN

Disclosure:

Only the version in German language is the legally binding document.

Publication date
Effective date

01.06.2009
01.06.2009



Copyright statement

D-TRUST-Root PKI Certification Practice Statement ©2009 D-TRUST GMBH, all rights reserved.

No part of this publication may be reproduced, saved or transferred by any means (electronically, mechanically, through a photocopy, a recording or any other method) to any storage system without the prior written consent of the D-Trust GmbH, if it is not in full accordance with the reserved rights and the explicitly stated terms of reproduction.

Irrespective of afore mentioned constraints, it is permitted to reproduce and distribute this CP non-exclusively and free of charge, provided that (i) the original copyright statement as well as these preliminary paragraphs are included prominently at the beginning of the reproduction and (ii) this document is reproduced verbatim and in its entirety, prefaced with the naming of the D-TRUST GMBH as its author.

Requests for approval of reproductions differing from the explicit terms of use or any utilization otherwise diverging from the permissions granted are to be addressed 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
1.0	18.06.2008	- Initial version
1.1	01.11.2008	- Adoption of certificate request requirements related to the majority age of the requester - Adoption of authentication procedures for SSL certificates with DNS names - General adoptions for SSL certificates - Change of OCSP paths - Adoption of authentication procedures for Class1 certificates
1.1_EN	17.11.2008	English version
1.2_EN	01.06.2009	- Revocation reasons of code-signing certificates extended - Editorial changes - Changes due to the WebTrust audit



Table of contents

- 1. Introduction5
- 1.1 Overview5
- 1.2 Document and Identification7
- 1.3 PKI-participants7
- 1.4 Certificate Usage8
- 1.5 CP/CPS maintenance9
- 1.6 Definition of terms, Abbreviations and Acronyms 10
- 2. Responsibility for Directories and Publications 14
- 2.1 Directories 14
- 2.2 Publication of Certificate Information 14
- 2.3 Publication Frequency 14
- 2.4 Directory Access Control 15
- 3. Identification and Authentication 16
- 3.1 Naming Conventions 16
- 3.2 Initial Identity Inspection 17
- 3.3 Identification and Authentication of Re-Keying Applications 19
- 3.4 Identification and Authentication of Revocation Applications 20
- 4. Operating requirements 21
- 4.1 Certificate Application and Registration 21
- 4.2 Processing the Certificate Application 22
- 4.3 Certificate Issuing 23
- 4.4 Certificate Transfer 23
- 4.5 Certificate and Key-Pair Usage 24
- 4.6 Certificate Renewal 25
- 4.7 Certificate Renewal with Key-Renewal 26
- 4.8 Certificate Changes 28
- 4.9 Revocation and Suspension of Certificates 29
- 4.10 Status Monitoring Service for Certificate 31
- 4.11 Withdrawal from the Certification Service 31
- 4.12 Key-Escrow and Key-Recovery 32
- 5. Non-Technical Security Provisions 33
- 6. Technical Security Provisions 34
- 7. Profiles of Certificates, CRLs and OCSP 35
- 7.1 Certificate Profiles 35
- 7.2 CRL Profiles 35
- 7.3 Status Monitoring Service (OCSP) Profile 35
- 8. Verifications and other Appraisals 36
- 9. Other Financial and Legal Regulations 37
- 9.1 Prices 37
- 9.2 Financial Responsibilities 37
- 9.3 Confidentiality of Business Data 38
- 9.4 Privacy of Personal Data 38
- 9.5 Industrial Trademark- and Copyrights 40
- 9.6 Assurances and Guarantees 40
- 9.7 Non-Liability 41
- 9.8 Limitation of Liability 41
- 9.9 Compensation 42
- 9.10 CP validity period and expiration 42
- 9.11 Individual Announcements for and Agreements with PKI-participants 42
- 9.12 Addendums 42
- 9.13 Dispute-Mediation Regulations 43
- 9.14 Competent Court of Jurisdiction 43

9.15	Abidance of Applicable Law	43
9.16	Miscellaneous Regulations.....	43
9.17	Other Regulations.....	44

1. Introduction

1.1 Overview

This document describes the Certificate Policy (CP) of the D-TRUST Root-PKI, which is operated and maintained by the D-Trust GmbH.

1.1.1 Certification service provider

The Certification Service Provider (CSP) is the

D-TRUST GMBH
Kommandantenstr. 15
10969 Berlin.

The CSP may entrust contractual partners or external contractors with parts of the production process, as long as all agreements are meticulously documented and a contractual relationship has been established prior to the provision of supplied services.

1.1.2 About this document

This CP provides binding regulations and requirements for the Root-PKI and thereby defines the certification process throughout the validity period of the End-User certificates (EU-certificates) as well as the co-operation, rights and duties of other PKI-participants.

The CP is legally binding in its entirety, inasmuch as is permissible by the legislature of the Federal Republic of Germany. It contains statements describing duties, guarantees and liabilities for PKI-participants. Unless expressly stated otherwise, no warranties or formal guarantees in a legal sense may be derived from this CP.

The knowledge of the certification methods and –rules as well as the knowledge of the legal operating framework allows relying parties to form an informed decision about the components and PKI-participants as well as to decide if the trustworthiness imparted by the security-measures inherent in the PKI is sufficient for their applications.

The structure of this document is based on the internet-standard RFC 3647 „*Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*“, to facilitate understanding and comparisons with other Certificate Policies.

1.1.3 PKI traits

The D-TRUST-Root-PKI's hierarchical structure is multi-tiered. An example constellation of the D-TRUST-Root-PKI is shown in Figure 1.

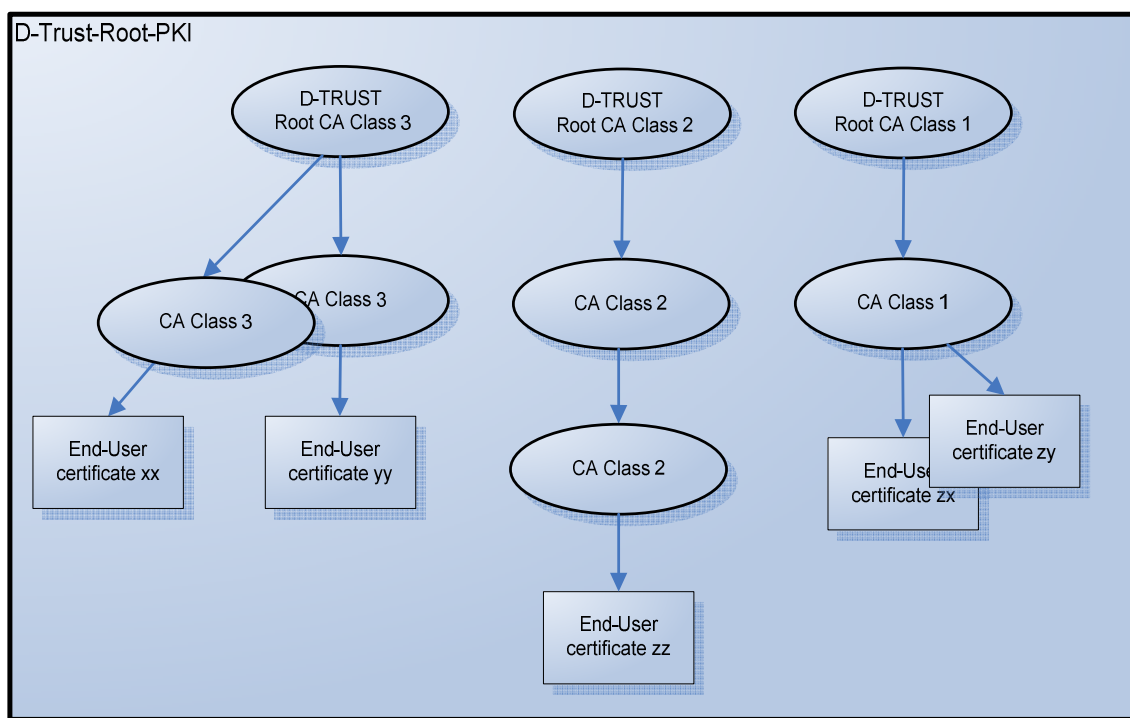


Figure 1 D-TRUST-Root-PKI example constellation

The CA- and EU-certificates can be categorized into three classes (Class 3, Class 2, Class 1). The higher the class (class 3 being the highest, class 1 the lowest), the higher the quality of the certificates. Class 3 certificates are nearly as high in quality as qualified certificates produced in full accordance with the German Signature Law [SigG]. Insofar as this document does not explicitly distinguish between the separate classes or exclude a class from a description, all requirements and stipulations of a paragraph apply to all three classes.

Class 3

Class-3-certificates are especially high-grade advanced certificates, that comply with most of the requirements for qualified certificates adhering to the stipulations of the German Signature Law [SigG] and fulfill all the requirements of [ETSI-F] „NCP“ and „NCP+“. SSL-certificates are only issued to legal entities. Class 3 EV-certificates do not comprise a separate class. Any explanations aimed at the compartment “Class 3” therefore also pertains to Class 3 EV-certificates. Differences are explicitly mentioned.

Class 3 EV-certificates

A special case of class-3 category certificates is represented by the class 3 SSL-EV-certificates, which follow the Guidelines for Extended Validation Certificates, CA/Browser Forum, version 1.1 April 2008 [GL-BRO] and [ETSI-F] “EVCP”. EU SSL-EV certificates are distinguishable by the inclusion of an EV-Policy-OID (compare chapter 1.2)

Class 2

Class-2-certificates are high-grade, advanced certificates adhering to the requirements of [ETSI-F] „LCP“.

Class 1

Class-1-certificates are simple certificates that do not follow the requirements of [ETSI-F].

1.2 Document and Identification

Document name:	D-TRUST-Root-PKI Certificate Policy
Object Identification (OID):	This document's Policy-OID: 1.3.6.1.4.1.4788.2.200.1 The EV-Policy-OID for EV-certificates is set according to [GL-BRO] as: 1.3.6.1.4.1.4788.2.202.1
Version	1.2_EN

1.3 PKI-participants

1.3.1 Certification Authority (CA)

CAs issue Certificate Revocation Lists (CRLs) and certificates. Possible certificates are:

- personalized certificates for natural and legal entities (EU-certificates),
- group-certificates for groups of individuals, functions and IT-processes (EU-certificates),
- certification authority certificates (CSP sub-CA-certificates).

Root-CAs (D-TRUST Root Class 3/2/1 CA) only issue certificates with the extension *basicConstraints: cA=TRUE* (CA-certificate). Sub-CAs issue EU-certificates and/or further CA-certificates. The Certification Service Provider is named in the field *issuer*, which is part of the issued certificates and CRLs.

1.3.2 Registration Authority (RA)

An RA identifies and authenticates applicants and processes. It also verifies the applications for different certification services. The CSP provides the RA with suitable hard- and software as well as work-flow processes that must be incorporated by the RA.

1.3.3 Subscriber

Applicants are individuals that apply for a certificate either for themselves or for another person.

Subscribers are individuals or legal entities, that own a certificate. The subscriber can differ from the entry in the certificate's *subject*-field.

End-Users (EU, *subject*) use the private End-User-Key (EU-key). The End-User may differ from the subscriber. Possible End-Users are:

- Individuals,
- Organizations (legal entities – under private law, public corporations or government owned),
- Groups of individuals,
- corporate functions which are administered by an organization’s employees and
- IT-Processes (SSL-Server, for example).

Class 3

Class-3-certificates may only be issued, if applicant, subscriber and end-user are identical. SSL certificates are only issued for legal entities.

Class 3 EV

EV-Certificates are not issued to sole proprietors.

Class 2

Class-2-certificates may be issued, even if applicant, subscriber and end-user differ.

Class 3-2 (Class 3 and Class 2)

The subscriber is responsible for the certificate and its keys. The applicant must acknowledge and guarantee the implementation of the subscriber’s obligation in the application process. He may do this for himself (i.e. the applicant will be the certificate’s subscriber) or in lieu of the subscriber (i.e. an individual that is not the applicant will be the certificate’s subscriber).

Class 1

Class 1 does not differentiate between an applicant, a subscriber and an End-User. An applicant will automatically be Certificate Holder and End-User and has full responsibility for the certificate and its keys.

1.3.4 Relying parties (RP)

Relying parties are individuals or legal entities that use the certificates of the D-TRUST-Root-PKI and have access to the services of the CSP.

1.4 Certificate Usage

1.4.1 Valid Usage of Certificates

CA-certificates are used exclusively in issuing CA- or End-User certificates and CRLs in accordance with their extensions (*BasicConstraints*, *PathLengthConstraint*).

EU-certificates may be used for those applications in accordance with the intended certificate usage as stated in the certificates themselves.

Relying parties assume responsibility for estimating if this CP applies in the case of the application of interest. The relying party must also assess the suitability of utilizing certificates for a given szenario.

1.4.2 Invalid Usage of Certificates

It is prohibited to use certificates for applications other than those explicitly mentioned in the certificates themselves.

1.5 CP/CPS maintenance

1.5.1 Document Administrator

This CP is maintained by the D-TRUST GMBH. The head of the CSP is responsible for approving this CP and any following versions hereof.

1.5.2 Contact Address

D-TRUST GMBH
Redaktion CP und CPS
Kommandantenstr. 15
10969 Berlin, Germany

Tel: +49 (0)30 259391 0

E-Mail: info@d-trust.net

1.5.3 Compatibility of CPs from other CAs with this CP

This CP describes the minimum mandatory requirements for PKI-participants.

Further CPs can be referenced in CA- as well as EU-certificates through their Policy-OIDs, as long as they do not contradict this CP. By referencing a Policy-OID in a certificate's extensions, the CA confirms the compatibility of the referenced CP with the certification-practices detailed in this CP (for example NCP (0.4.0.2042.1.1, according to [ETSI-F]).

CAs that refer to a CP that is comparable in the technical and judicial aspects of the provided services, may be certified by the CSP through a Cross-Certificate. A Cross-Certificate assures the equivalency of the Certificate Policies and can only be issued between CAs that are either non-ETSI-certified, or between CAs that have been ETSI-certified. Cross-Certificates have an extension of *pathlength = 1* and are published into the Directory Service of the CPS (compare section 2.1).

The CSP is responsible for the accuracy of the information in Cross-Certificates issued for outside CAs, as well as for the equivalency of the outside policy with this Certificate Policy at the time of certification. A subsequent and substantial change in the outside Policy that voids the equivalency to the D-TRUST GMBH Policy results in a revocation of the Cross-Certificate.

Should a CA plan to issue a Cross-Certificate for a D-TRUST GmbH CA, the D-TRUST GmbH must be informed prior to certification. The D-TRUST GmbH reserves the right to object to a cross-certification.

Class 3 SSL-EV-certificates as well as their Sub- and Root-CAs adhere to the specifications of the CA/Browser Forum Guidelines for Extended Validation Certificates [GL-BRO]. In the case of inconsistencies between this document and above mentioned guidelines, the [GL-BRO] takes precedence for Class 3 SSL EV CAs as well as their Sub- and Root-CAs.

1.6 Definition of terms, Abbreviations and Acronyms

1.6.1 Terms and names

Applicant	<i>Subscriber</i> , individual that applies for a certificate. Either for themselves or for others.
CA-certificate	A certificate for a Certification Authority's public key
Certificate Policy (CP)	Compare section 1.1
Certification Authority (CA)	Root PKI Authority, compare chapter 1.3.1.
Certification Service Provider (CSP)	Provider of Certification Services
Cross-certificate	Certificate used to affirm a trusted relationship between two CAs
D-TRUST Root CA	Root Certification Authority, existing in the categories class 3, class 2 and class 1; compare chapter 1.3.1.
D-TRUST-Root-PKI	D-TRUST GMBH implemented Public Key Infrastructure
Directory Service	PKI-service for online access of information pertaining to certificates and CRLs; commonly realized through the Light Weight Directory Access Protocol (LDAP)
Distinguished Name (DN)	A sequence of data-fields describing the CA <i>issuer</i> and/or the <i>subject</i> uniquely. The format of a Distinguished Name is defined in the [X.501] standard.
End-User (EU)	End-Users make use of the private End-User-key and may differ from the <i>Subject</i> .
End-User-certificate	Certificate, that may not be used to certify and issue other certificates or CRLs
EU-certificate	See "End-User-certificate"
Postident Basic	Process of authentication offered by the Deutsche Post AG. Also compare Registration Authority (RA).
Registration Authority (RA)	PKI-incorporated facility for participant-authentication; compare chapter 1.3.2.

SmartCard	Integrated circuit card including a micro-processor that can be used for the generation of digital signatures and for other PKI-applications
Soft-PSE	Software Personal Security Environment, aka Software-Token; contains the EU-key-pair, the EU-certificate and the certificate of the issuing CA
Relying parties	Individual or legal entity that uses certificates; compare chapter 1.3.4.
Revocation Authority	Individual or legal entity that is entitled to revoke a certificate
Status monitoring service	PKI-service for online inquiries concerning the status of a certificate (valid, revoked, unknown) through the Online Certificate Status Protocol-Responder (OSCP-R)
Subscriber	Individuals or legal entities that own End-User certificates; compare chapter 1.3.3.
Token	Transport-medium for certificates and keys
TrustCenter	The high-security area on the premises of the D-TRUST GMBH.

1.6.2 Abbreviations

CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification service provider
DN	Distinguished Name
FIPS	Federal Information Processing Standard
FQDN	Fully qualified domain name
HSM	Hardware Security Module
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PUK	Personal Unblocking Key
RA	Registration Authority

RFC	Request for Comment
SSCD	Secure Signature Creation Device
SUD	Secure User Device
URL	Uniform Resource Locator
UTF8	Unicode Transformation Format-8

1.6.3 References

[ALG-KAT]	The most recent version of the Regulation Agency's (Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn) announcement concerning digital signatures in accordance with the German Signature Law, specifying suitable cryptographic algorithms. The announcement is published annually in the federal bulletin (Bundesanzeiger).
[CP]	Certificate Policy of the D-TRUST-Root-PKI, D-TRUST GMBH, in its most recent version
[CPS]	Certification Practice Statement of the D-TRUST-Root-PKI, D-TRUST GMBH, in its most recent version
[Co-PKI]	Common PKI Specification, Version 2.0, 20 th of January 2009
[ETSI-ALG]	ETSI, Algorithms and Parameters for Secure Electronic Signatures, ETSI TS 102 176-1 V2.0.0, Nov. 2007
[ETSI-F]	ETSI, Technical Specification Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, ETSI TS 102 042 V2.1.1, May 2009
[GL-BRO]	Guidelines for Extended Validation Certificates, CA/Browser Forum, Version 1.1 April 2008
[ISO-3166]	List stating the country names as official short names in English
[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 5280]	Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile, May 2008
[SigÄndG]	First amendment to the German Signature Law, 4th of January 2005 (BGBl. I S. 2)
[SigG]	German Signature Law (Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG), 16 th of May 2001 (BGBl. I S. 876), revised last by this law's article 4 on the 26 th of February 2007 (BGBl. I S. 179)
[SigV]	Signature edict, 16 th of November 2001 (BGBl. I., S. 3074), revised last by this edict's article 9, paragraph 18, on the 23 rd of November 2007 (BGBl. I., S. 2631)

- [SiKo-DTR] Security concept of the SigG-compliant Certification Service Provider
D-TRUST GMBH
- [WebTrustEV] WEBTRUST^{SM/TM} for Certification Authorities – Extended Validation
Audit Criteria, Canadian Institute of Chartered Accountants, Version
1.1, 2008
- [WebTrustCA] WebTrust CA - WebTrust Program for Certification Authorities (Version
1.0; August 25, Verison 2000
- [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 Directories and Publications

2.1 Directories

The CSP publishes CRLs and certificates into the LDAP-directory. The LDAP-directory is accessible under the address: <ldap://directory.d-trust.net>.

The specific address for each certificate is part of the certificates information.

In addition, CA-certificates are published on the web-sites of the D-TRUST GMBH and can be accessed through the URL:

<https://www.d-trust.net/internet/content/d-trust-roots.html>

The CSP provides an online certificate status-monitoring-service (OCSP) through which the revocation status of every certificate in the D-TRUST-Root-PKI may be checked. The address for the OCSP-service is part of the certificate information. Any certificate's status may be checked up to a year after their expiration, after which time the entry will be removed from the service.

This CP, the [CPS] and the Subscriber's Obligation can be downloaded as PDF-documents from the CSP's web-site: <https://www.d-trust.net/repository>

2.2 Publication of Certificate Information

The CSP publishes the following information about the D-TRUST-Root-PKI:

- EU-certificates, if so requested by the applicant,
- CA-certificates (Trust-Anchor),
- Certificate Revocation Lists and Certificate Status information,
- this CP,
- the [CPS],
- Cross-certificates.

2.3 Publication Frequency

EU-certificates are published if the applicant wishes them to be published and remain listed for a year and additionally for the remainder of the year in which the listing-period of one year expires.

CA-certificates are published in the course of their creation and remain listed for either:

- at least five years (Class 3) or for
- at least one year (Class 1 and 2),

after the expiration date of the CA-certificate.

CRLs are published periodically and until the issuing CA-certificate expires. A new CRL is issued instantly with each new revocation of a certificate under the CA-tree. Even if no

revocation has occurred in the meantime, the CSP publishes a new CRL every five days. The CRLs are listed for at least a year after the CA has expired.

This CP and the [CPS] are published and remain listed and downloadable as long as they remain in effect (compare chapter 2.1). A hosting service availability of 99.5% is guaranteed.

2.4 Directory Access Control

Certificates, CRLs, CPs and the CPS are listed publically and can be downloaded free of charge. A read-only access is permitted for the general public. Changes and additions to public directory entries as well as web-site information are undertaken solely by the CSP.

The relevant parts of other, non-public documents can be made available on request, if a vested interest is in evidence.

3. Identification and Authentication

3.1 Naming Conventions

3.1.1 Types of Names

CA- and EU-certificates principally contain information on the *issuer* as well as on the Subscriber or End-User (*subject*). The names are listed in the fields *issuer* and *subject* and are formatted along the X.501 standard for *DistinguishedNames*.

Alternative names may be registered and would subsequently be displayed in the *subjectAltName*-extension of a certificate.

3.1.2 Necessity for unambiguous names

A Subscriber's *DistinguishedName* is unique in the D-TRUST-Root-PKI.

Class 3-2

An unambiguous, biunique correlation between certificate and subscriber is guaranteed.

If the extension *subjectAltName* is filled in a certificate, there is no need for an unambiguous name. SSL-certificates, including Class 3 EV-certificates, are excluded from this assertion.

The unique names may neither refer to the certificate in which they are used nor make use of an IP-address.

3.1.3 Subscriber Anonymity or Subscriber Pseudonyms

Pseudonyms may be used by individuals only and are generally assigned by the CSP. The free choice of a pseudonym may be arranged (compare chapter 3.1.6). The CSP reserves the right to deny the assignment of a pseudonym. The CSP is not obligated to justify such a refusal.

Class 3-2

In the case of issuing certificates with a pseudonym, the CSP will still record and retain the applicant's identity in its internal databases.

3.1.4 Rules for the Interpretation of Different Naming Combinations

The provisions for inclusion and interpretation of names are defined in the Certificate Practice Statement [CPS].

Not all of the listed possible DN-components need to be used and some DN-components that are not listed may be added.

Class 3 EV-Zertifikate

EU-certificates must contain the *subject*-DN-components „O“, „CN“ or „subjectAltName including the domain name“, „BusinessCategory“, „Jurisdiction of

Incorporation or Registration“, „serialNumber“, „L“, „State“ and „C“. The components „Street“ and „Postal Code“ may be included optionally.

Class 3-2

Additional DN-components must adhere to [RFC 5280] and [Co-PKI].

3.1.5 Uniqueness of Names

Class 3-2

The CSP guarantees, that the DistinguishedName for a Subscriber or End-User employed in the *subject* field of a D-TRUST-Root-PKI EU-certificate will be unique not only throughout the validity-period of the certificate, but throughout the entire existence of the D-TRUST-Root-PKI and will also stay strictly correlated with the same subscriber. DistinguishedName uniqueness is achieved through the incorporation of a serial number (usually the application number or the register of commerce number according to [GL-BRO] chapter 6(a) (5)), which guarantees the unambiguous identification¹ of the subscriber.

The CSP assures the uniqueness of its CAs' DistinguishedNames.

3.1.6 Acceptance, Authentication and Brand-Names

The subscriber is liable for complying with existing intellectual property rights in his application- and certificate data (compare chapter 9.5).

Class 3 EV-certificates

The CSP will take all necessary steps to ensure that the individual named in the *subject* field has the sole usage rights to the FQDN named in the certificate at the time of certificate creation.

3.2 Initial Identity Inspection

3.2.1 Verifying Ownership of the Private Key

Proof of ownership is divided into two cases:

1. A subscriber's key-pairs are produced inside the facilities of the CSP. With the delivery of the token and, if applicable, the PIN according to chapter 4.4.1 the transferal of the key-pairs is secured.
2. Key-pairs are produced in the applicant's sphere of influence. The ownership of the keys must be technically proven or comprehensibly stated by the applicant.

3.2.2 Identification and Authentication of Organizations

Organizations that are named in certificates or in whose name certificates are issued must authenticate themselves comprehensibly.

¹ Identification in this instance means the identification of the subscriber's true name in combination with the data obtained through the initial application, notwithstanding any possible changes in possible consecutive applications. Identification in this instance neither includes the elicitation of possible changes in the initial application data nor locating a subscriber at a later point in time.

Class 3

High-level identification and assessment. Personal participant identification as well as a thorough assessment of the applicant-data are conducted along the procedures defined for the creation of qualified certificates. Legal entities are verified in adherence with the [ETSI-F]- guidelines. The verification encompasses all of the DN-components.

Class 3 EV-certificates

Identification and authentication as well as data verification follow the standards stated in [GL-BRO] and section H 30 [GL-BRO].

Class 2

Mid-level identification and assessment. Personal participant identification as well as the assessment of applicant-data are at minimum based on the statements of a trustworthy third-party (for example a department head or the personell department, depending on contractual arrangement). The verification encompasses all of the DN-components.

Class 1

Low-level identification and assessment. Only the e-mail-address and, if applicable, the domain-name and/or the organization are verified.

If an application is submitted in the name of a legal entity, the representative must (analogous to the class-specific practices described in chapter 3.2.3) prove his identity and entitlement.

Proofs that are not provided in the Latin alphabet are not accepted.

3.2.3 Identification and Authentication of Individuals

Individuals applying for a certificate either in their own name or for a third party, planning on being named in the certificate must prove their identity beyond a doubt as well as their entitlement for applying through an organization.

Class 3

High-level identification and assessment. Personal participant identification as well as a thorough assessment of the applicant-data are conducted along the procedures defined for the creation of qualified certificates. The verification encompasses all of the DN-components. The identification and authentication as well as the verification of SSL-certificate data abide by the rules set in [ETSI-F].

Class 2

Mid-level identification and assessment. Personal participant identification as well as the assessment of applicant-data are at minimum based on the statements of a trustworthy third-party. The verification encompasses all of the DN-components.

Class 1

Low-level identification and assessment. Only the e-mail-address and, if applicable, the domain-name and/or the organization are verified.

Proofs that are not provided in the Latin alphabet are not accepted.

3.2.4 Unexamined Statements concerning the Subscriber

The information given by the applicant is class-dependently validated or taken on trust as described in the chapters 3.2.2, 3.2.3 and 4.2.1. If an *Alternative Name* is given, a validation is only carried out in the case of an e-mail-address. Other *Alternative Names*, such as addresses of LDAP-directories etc. as well as possible additional certificate-extensions (*AdditionalInformation, monetaryLimit, etc.*) are not verified (compare chapter 4.9.1).

3.2.5 Examination of Application Entitlement

Individuals and legal entities may apply for a certificate. The process is defined in the [CPS].

3.2.6 Criteria for Interoperability

Compare chapter 1.5.3.

3.3 Identification and Authentication of Re-Keying Applications

Re-keying is the process of recreating certificates and, if applicable, tokens and keys for a known applicant. Re-keying is offered for Class 3-2 certificates only. It is not offered for Class 1 and Class 3 EV-certificates. In the case of Class 3 EV-certificates, the entire process of identification and registration must be observed in the same form as for an initial application. Documents that have been submitted in a prior application-process may be reused, if they are still deemed valid according to section D 8 (b) [GL-BRO].

3.3.1 Routine Re-Keying Applications

After EU-certificates expire (Class 3-2) or by request of the applicant, new certificates and, if applicable, tokens and keys will be issued. No new identification is necessary upon a request for re-keying. The request must be signed:

- with a qualified, digital signature or
- with a digital signature from the same class as the requested certificate or
- by hand.

The specifications laid-out in chapter 4.7 must be kept.

3.3.2 Re-keying after Revocation

The re-keying of revoked EU-certificates is based on the process described in chapter 3.3.1, as long as the identifying data is still trusted and a previously asserted organizational affiliation has not been rescinded.

Note: Signatures created with the use of expired or revoked EU-certificates are not recognized.

3.4 Identification and Authentication of Revocation Applications

The CSP validates the revoking party's entitlement for the intended action prior to revoking a certificate. The validation procedures are defined in the [CPS].

Diverging procedures concerning the validation of revocation applications may be agreed upon with the applicant.

Revocation procedures are described in chapter 4.9.

4. Operating requirements

4.1 Certificate Application and Registration

4.1.1 Application Eligibility

Individuals and legal entities (their designated representatives) may apply for a certificate.

A subscriber may be represented by a substitute applicant, except when applying for a class-3-certificate for individuals or a class-1-certificate.

Group-certificates are exclusively issued to legal entities and individual enterprises.

Private EU-keys, that are not signature keys² or keys of class-3-EV-certificates can be securely escrowed by the CSP for future reuse in a new token. The conditions of a key-escrow are laid-out in chapter 6.2.3 of the [CPS]. The applicant must request the key escrow and assure that the key is supposed to be re-used for the same subscriber and/or group of individuals. For a re-use of an End-User-key according to 6.2.3 [CPS], an applicant must prove the fact, that he is authorized to re-commission the key.

Class 3 EV-certificates

Subscribers need to be in accordance with the requirements stated in section C 5 [GL-BRO].

CA-certificates are only issued to legal entities.

The CSP reserves the right to decline applications (compare chapter 4.2.2).

4.1.2 Registration-Process and Administrative Responsibility

During the registration-process the applicants are made aware of the CP, the CPS, in case of an application for class 3-2-certificates a subscriber agreement and further documents that inform the applicant of the restrictions and requirements in the usage of the chosen certificate-type.

The CSP ensures the correct observance of the registration-process.

The CSP may entrust contractual partners or external contractors with parts of the registration-process, as long as these externals are in agreement with the CP.

² The term "signature key" describes a private-key that has been created for a certificate which encloses the corresponding public key and indicates the key-usage "digital signature" or "contentCommitment"/ "nonRepudiation" ("contentCommitment" is the new term for "nonRepudiation").

4.2 Processing the Certificate Application

4.2.1 Identification and Authentication

The described procedures for identification and registration must be fully implemented in accordance with the provisions for the different class-categories; the necessary documents of proof must be impeccable.

Authentication of individuals or organizations, as well as the verification of relevant data may take place before or after application, but must be completed before certificates or, if applicable, keys and PINs are transferred to the subscriber.

Class 3-2

Individuals must be indentified beyond a doubt. Next to the full name, additional attributes such as place of birth and birth date, a passport/ID-card number or other features must be incorporated to ensure the future definite identification of an individual.

If legal entities act as the subscriber or are named in the certificate, the full name, legal status as well as possibly relevant register entries must be verified.

The identification-process is described in chapter 3.2.3. The applicable methods are defined in the [CPS].

4.2.2 Approval or Declination of Certificate Applications

The application will be declined should doubts remain in either the identity- or the data verification that cannot be alleviated fully and in a timely manner by the applicant.

Further reasons for a declination:

- suspicions concerning the violation of name rights,
- noncompliance with deadlines concerning the confirmation of information,
- outstanding payments of the applicant towards the CSP,
- circumstances indicating that a certificate may discredit the CSP.

The CSP reserves the right to deny a certificate application without explanation.

The application is rated as approved only after the application information has been verified and the certificate as well as, if applicable, the keys (compare chapter 4.4) have been transferred to the applicant.

4.2.3 Time Limit for Application Processing

Not applicable.

4.3 Certificate Issuing

4.3.1 CSP Approach in Issuing Certificates

After a satisfactory validation of the application, the certificates are produced in the high-security TrustCenter. The application documents are archived in their entirety.

4.3.2 Subscriber Notification Concerning Certificate Issue

There is no separate notification upon certificate production.

4.4 Certificate Transfer

4.4.1 Certificate Transaction Procedures

Class 3-2

SmartCards will (analogous to the procedures for qualified SmartCards) either be sent to the applicant's address on record by courier or equivalent means, or handed out personally by the RA, an authorized employee or other responsible party of the organization. Soft-PSEs, saved to a data carrier, can be sent by mail to the address on record in the application documents, be made available for download over a secured line or be included with an e-mail (the PKCS#12 file is secured by a PIN of at least 8 figures). If a certificate is created for an existing key-pair, the certificate will either be made available for download (through publication in the directory service for example) or sent by e-mail.

Class 1

SmartCards will either be sent to the applicant's address on record by courier or equivalent means, or handed out personally by the RA. Soft-PSEs, saved to a data carrier, can be sent by mail to the address on record in the application documents, be made available for download over a secured line or be included with an e-mail (the PKCS#12 file is secured by a PIN of at least 8 figures). If a certificate is created for an existing key-pair, the certificate will either be made available for download (through the publication in the LDAP-directory service for example) or sent by e-mail.

If the subscriber should discover any errors in his certificates or with the functions of the keys and tokens the CSP has to be informed. The certificates will subsequently be revoked. After the certificates have been revoked, the CSP can demand the return of the subscriber's SmartCards.

Incorrect data in the certificates will only then count as a contractual shortcoming, if such data is affected, as the CSP verified in accordance with this CP. Apart from that, the CSP's general terms and conditions in respect to the rules of retroactive compliance apply in the case of errors.

There is no acceptance procedure since the contractual basis is a service agreement.

4.4.2 Certificate Publication by the CSP

If the applicant agreed to the publication of the certificate during the application process, it will be made publicly available via the light-weight directory access protocol after

production³. If the applicant did not agree to publication, the certificate will not be made publicly available.

In either case, after production, the status of the certificate will be available to any interested party either through the access of CRLs or by sending a status request to the OCSP-responder (compare chapter 2.1)⁴.

4.4.3 Notification of other PKI-participants about the Creation of the Certificate

Third party revocation authorities as described in chapter 4.9.2 are notified in writing and issued a revocation-password, if no other provisions have been made.

4.5 Certificate and Key-Pair Usage

4.5.1 Subscriber Certificate and Private-Key Usage

The subscriber may only use his private key for those applications that are explicitly described as the possible use-cases in the certificate.

Class 3-2

The guidelines laid-out in chapter 1.4 are valid vor subscribers.

4.5.2 Relying Parties' Certificate and Private-Key Usage

The certificates of the D-TRUST-Root-PKI can be employed by all relying parties. **They retain their trustworthiness only, if**

- the certificates are used according to the use-cases noted in the certificate (key-usage, extended key-usage, possible constraints),
- the certificate chain is successfully verified all the way up to – and including – a trustworthy root-certificate⁵,
- the certificate-status is successfully verified through the online status monitoring service (OCSP), and
- all further agreements and otherwise published precautions are met and that possible certificate constraints as well as any necessary provisions for the deployed applications are noted, considered and found to be in accordance with the use-case(s) by the relying parties.

Note: In court the reversal of the burden of proof only applies to qualified signatures, it does not apply to non-qualified signatures, which means, that the signature's validity must be ascertained by an expert in court. The high degree of security in class 3-2 certificates is an excellent initial condition for an expert opinion.

³ If the token should contain qualified EU-certificates or qualified EU-certificates from an accredited provider in addition to the advanced certificates of the Root-PKI, then the publication will follow the procedure for the certificates of the highest class.

⁴ If the token should contain qualified EU-certificates or qualified EU-certificates from an accredited provider in addition to the advanced certificates of the Root-PKI, the status of the certificates will be available via CRL or OCSP only after the CSP is informed through a written receipt, that the certificates have been received by the applicant.

⁵ The verification of the certificate-chain should follow the PKIX-Modell (aka shell-modell) according to [RFC 5280], section 6. A formal description of the verification algorithm can be found in [Co-PKI] section 5.

4.6 Certificate Renewal

Certificate renewal means the renewed creation of a certificate. The new certificate is based on the information and keys of the original certificate, albeit with an altered validity period. When applying for a certificate renewal, any fields of the original certificate may be changed if according evidence is submitted. The CP that is valid at the time of the certificate renewal applies to the renewed certificate. A certificate renewal will only be issued for EU-keys on SmartCards.

There is no certificate renewal for CA-keys.

4.6.1 Criteria for Certificate Renewal

When applying for a certificate renewal, the initial identification of the applicant, which is mandatory when applying for a new certificate, may be waived.

Class 3-2

It is a prerequisite that the applicant be identical with the applicant from the initial application. The authorization must be discernible from a hand-signature or digital-signature comparison.

The renewable certificate must still be valid at the point of time that an electronic application is submitted. A written application may be submitted after the certificate has expired.

Class 2

Additional contracts may allow for a reloading process in which a trustee is authorized to submit the application for a certificate renewal. The subscriber is then obligated to permit the download of the new certificate to his card and to also acknowledge any new terms of use by entering his PIN during the reloading process.

Class 3-1 (Class 3, Class 2 and Class 1)

If certificate content changes, it must be verified by the class-specific procedures detailed in chapters 3.2.2 and 3.2.3. Applicants must confirm that only the explicitly marked certificate content has changed.

If the organizational affiliation was simply affirmed as being in place at the time of the initial application or a prior consecutive application and was issued without a time of repeal, a validity period or invariably, it must be renewed. The procedure is analogous to the procedure detailed in chapter 3.2.3. If the organizational affiliation has been repealed or if it has expired, it must be re-verified or left out of the certificate.

The applicant will be informed, if there are any major changes in the terms of use. The applicant needs to acknowledge the changed terms of use.

The re-certifiable keys and the cryptographic algorithm must meet the minimum requirements of the CP that is valid at the date of application (compare chapter 3.2.1, 6.1.1 [CPS] and 6.1.5 [CPS]) and may not be compromised.

4.6.2 Eligibility for Certificate Renewal

Every applicant that is authorized for a renewed application according to chapter 4.1.1 may apply for a certificate renewal in keeping with the requirements in chapter 4.6.1.

4.6.3 Processing an Application for Certificate Renewal

Applicants that are authorized for the application of a certificate renewal must either personally deliver their hand-signed application to the Registration Authority or need to digitally sign an electronic application with the valid original certificate or a valid class-equivalent certificate.

4.6.4 Informing the Applicant about the Issue of a new Certificate

The regulations of chapter 4.3.2 apply.

4.6.5 Renewed-Certificate Transaction Procedures

The subscriber is already in possession of the key-pair in the case of certificate renewal. The produced certificate is either written onto a SmartCard via a secure data-connection, which is similar to the procedure employed in the case of a qualified certificate, or it will be made available through the LDAP-directory service. Apart from these provisions, the requirements laid-out in chapter 4.4.1 apply.

PINs are not altered during a certificate renewal.

4.6.6 Publication of the Certificate-Renewal by the CSP

The requirements in chapter 4.4.2 apply according to the information given in the initial application. The applicant may change his decision about the publication of his certificate.

4.6.7 Notification of other PKI-participants about the Renewal of the Certificate

The requirements in chapter 4.4.3 apply.

4.7 Certificate Renewal with Key-Renewal

Key-renewal is the term for the renewed issue of a certificate based on the content of the original certificate with the generation of a new key-pair and a change of the validity-period. When applying for a key-renewal, any data employed in the certificate, except for the CN-field of the distinguished name in EU-certificates without a pseudonym (compare chapter 3.1.1), may be altered if sufficient evidence is provided. The CP that is valid at the time of the certificate renewal applies to the renewed certificate. Key-renewals are only offered for class 3-2. CA-keys of all classes may be renewed as long as they have not been revoked.

Class 3 EV-Zertifikate

Certificate renewal in conjunction with key renewal is not offered for EV-Certificates. The guidelines in [GL-BRO], sections D8 and F25 apply to Class 3 EV-certificates.

4.7.1 Criteria for Key-Renewal Certificates

The application for a key-renewal equals the application for a certificate renewal. When applying for a key renewal, the initial identification of the applicant, which is mandatory when applying for a new certificate, may be waived.

It is a prerequisite that the applicant be identical with the applicant from the initial application. The authorization must be discernible from a hand-signature or digital-signature comparison.

The renewable certificate must still be valid at the point of time that an electronic application is submitted. A written application may be submitted after the certificate has expired.

Applicants may need to prove that they are in possession of the private key along the guidelines in chapter 3.2.1.

If certificate content changes, it must be verified by the class-specific procedures detailed in chapters 3.2.2 and 3.2.3. Applicants must confirm that only the explicitly marked certificate content has changed.

If the organizational affiliation was simply affirmed as being in place at the time of the initial application or a prior consecutive application and was issued without a time of repeal, a validity period or invariably, it must be renewed. The procedure is analogous to the procedure detailed in chapter 3.2.3. If the organizational affiliation has been repealed or if it has expired, it must be re-verified or left out of the certificate.

The applicant will be informed, if there are any major changes in the terms of use. The applicant needs to acknowledge the changed terms of use.

If certificates are to be produced for an existing key-pair, the possession of the private key must be proven following the procedures in chapter 3.2.1. The uncompromised key material as well as the cryptographic algorithms must meet the minimum specified standards of the CP valid at the time of application see chapters 3.2.1, 6.1.1 [CPS] and 6.1.5 [CPS].

4.7.2 Eligibility for Key Renewal

Every applicant that is authorized for a renewed application according to chapter 4.1.1 may apply for a key renewal in keeping with the requirements in chapter 4.7.1.

4.7.3 Processing an Application for Key-Renewal

Applications may be in writing and hand-signed or electronic and digitally signed with the original certificate.

4.7.4 Informing the Subscriber about the Issue of a Follow-up Certificate

The regulations of chapter 4.3.2 apply.

4.7.5 Key-Renewed-Certificates Transaction Procedures

The regulations of chapter 4.4.1 apply.

4.7.6 Publication of Certificates after Key-Renewal by the CSP

The regulations of chapter 4.4.2 apply. The applicant may change his decision about the publication of his certificate.

4.7.7 Notifying other PKI-participants about Follow-Up Certificates

The regulations of chapter 4.4.3 apply.

4.8 Certificate Changes

Certificate changes are not offered.

4.8.1 Criteria for Certificate Change

Not applicable.

4.8.2 Eligibility for Certificate Changes

Not applicable.

4.8.3 Processing an Application for Certificate Change

Not applicable.

4.8.4 Informing the Subscriber about the Issue of a new Certificate

Not applicable.

4.8.5 Certificate Change Transaction Procedures

Not applicable.

4.8.6 Publication of the Certificate Change by the CSP

Not applicable.

4.8.7 Notifying other PKI-participants about the Issue of new Certificates

Not applicable.

4.9 Revocation and Suspension of Certificates

4.9.1 Criteria for Revocation

Hosting a certificate revocation service is part of the CSP's contractual and lawful obligation towards the subscriber and affected third parties. The CSP's procedures fulfill the requirements of [ETSI-F] and [GL-BRO].

Subscribers or affected third parties are encouraged to apply for a revocation if there is a suspicion that the private key may have been compromised, or the certificate data is no longer correct (for example in the case of the discontinuation of the organizational affiliation of the subscriber).

Revocations are fitted with a date and are not issued retroactively.

Revocation authorities must authenticate themselves according to chapter 3.4.

4.9.2 Eligibility for Revocation

The CSP is a revocation authority. The CSP must revoke according to [GL-BRO] chapter 27.b or as the case may be chapter 28 (c).

The subscriber is always authorized to revoke his certificates. Arrangements can be drawn up in which the subscriber waives this right.

If a certificate contains information about the substitute-power of the subscriber for a third party, the third party or the party responsible for information about said relationship may insist on the revocation of the certificate if the noted information is no longer valid. Additional revocation authorities may be named which would then have the power to revoke a certificate at any time.

The CSP also regards any party in possession of the revocation password as a revocation authority.

4.9.3 Processing a Revocation Application

A revocation application may be mailed in. If a revocation password was arranged, revocation authorities may e-mail the application or apply for a revocation by telephone during the hours of 09:00-17:00h on a standard work-day.

Revocation telephone number: +49 (0)30 / 25 93 91 - 602

E-Mail-Address: sperren@d-trust.net

Postal address: D-TRUST GMBH
Kommandantenstr. 15
10969 Berlin

Class 3 EV-Certificates

If a revocation password was arranged, a revocation authority may revoke a certificate telephonically 24/7.

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

Diverging revocation procedures may be agreed upon.

A revocation application must contain the following information:

- applicant name,
- subscriber name,
- subject-/applicant-serial-number (in the case of EV certificates the registration number),
- certificate serial-number (if possible as a decimal number), so the certificate may be indentified correctly.

Revocations are performed in the CSP's sphere of responsibility. The CSP may however assign partial tasks to contractually bound third parties. The revocation may be undertaken by a third party that acts according to the standards of the CSP. The CSP provides appropriate soft- and hardware as well as work-flow processes. The authentication of the revocation authority follows the guidelines as laid-out in chapter 3.4.

4.9.4 Deadlines for a Revocation Application

The subscriber is obliged to revoke – or have the authorized third party revoke – the certificate as soon as grounds for a revocation become known. The procedure that seems to offer the quickest handling of a revocation request is to be chosen.

4.9.5 CSP Revocation-Application Processing Time

On standard work days, revocation-applications are processed by the CSP from 09:00h to 17:00h. Revocation-applications that are phoned in are processed immediately, while written revocation-applications that are received via mail or e-mail are processed the following work day by the latest.

Class 3 EV-certificates

The revocation is processed immediately after the successful telephonic authorization of the revocation-applicant.

4.9.6 Methods of Validating Revocation-Information

Topical revocation information is stored in certificate revocation lists that may be accessed through the light-weight directory-access protocol or downloaded via the link given in section 2.1. Additionally the OCSP-service is provided. These services' reachability is noted in the form of URLs in the certificates themselves. Revocation-information can also be obtained from the websites of the CSP (compare chapter 2.1). Delta-CRLs are not used. Integrity and authenticity of the revocation-information is ensured through a signature.

4.9.7 Revocation List Publication Frequency

Compare chapter 2.3.

4.9.8 Maximum Latency Period for Certificate Revocation Lists

Revocation lists are published with their production.

4.9.9 Online Accessibility of Revocation Information

An OCSP-service is provided for the online status check of certificates. This service's reachability is noted in the form of a URL in the certificates themselves.

4.9.10 Necessity of Checking Revocation Information online

There is no obligation to check revocation information online; the stipulations in section 4.5.2 stay in effect.

4.9.11 Other Forms of Publishing Revocation-Information

None.

4.9.12 Special Requirements for Compromised Private-Keys

None.

4.9.13 Conditions for a Suspension

Certificate suspensions are not offered.

4.10 Status Monitoring Service for Certificate

4.10.1 Mechanics of the Status Monitoring Services

The status monitoring service is implemented through the Online Certificate Status Protocol. The service's reachability is noted in the form of a URL in the certificates themselves.

4.10.2 Availability of the Status Monitoring Service

The status monitoring service is permanently (24/7) available.

4.10.3 Optional Services

None.

4.11 Withdrawal from the Certification Service

The certificate's validity ends according to the date noted in the certificate. Key-renewal may be applied for according to the details in section 3.3.1. A revocation request by the subscriber or an authorized third party results in the CSP revoking the certificate. With these services, the CSP's contractual conditions are fulfilled in their entirety.

4.12 Key-Escrow and Key-Recovery

Key-escrow of private EU-keys may be applied for except in the following cases:

Class 3-2

EU-certificate signature-keys are not stored.

Class 3 EV-certificates

Class 3 EV keys are not stored.

4.12.1 Conditions and Procedures for Private-Key-Escrow and -Recovery

The applicant must request a key escrow and assure that the key is supposed to be re-used for the same subscriber and/or group of individuals.

For the re-usal of an End-User-key according to 6.2.3 [CPS], an applicant must prove the fact, that he is authorized to re-commission the key.

4.12.2 Conditions and Procedures for Session-Key-Escrow and -Recovery

Session keys are not offered.

5. Non-Technical Security Provisions

The CSP establishes non-technical security provisions according to the requirements stated in [ETSI-F] and [GL-BRO].

The procedures are defined in the [CPS].

6. Technical Security Provisions

The CSP establishes technical security provisions according to the requirements stated in [ETSI-F] and [GL-BRO].

Subscribers and relying parties must only employ trustworthy computers and software.

The procedures are defined in the [CPS].

7. Profiles of Certificates, CRLs and OCSP

7.1 Certificate Profiles

Certificates issued by D-TRUST-Root-PKI CAs comply to the stipulations detailed in the standards ITU [X.509] and IETF [RFC 5280], as well as to the Common PKI 2.0 [Co-PKI] pattern. Possible deviations must be described in a referenced document.

Class 3 EV-certificates

EV-certificates issued in the Root-PKI comply with the [GL-BRO] specifications.

The profiles are defined in the [CPS].

7.2 CRL Profiles

The issued CRLs conform to the stipulations detailed in the standards ITU [X.509] and IETF [RFC 5280], as well as to the Common-PKI 2.0 [Co-PKI] pattern.

The profiles are defined in the [CPS].

7.3 Status Monitoring Service (OCSP) Profile

The status monitoring service conforms to the standard [RFC 2560] and fulfils the pattern requirements of Common PKI 2.0 [Co-PKI].

The profiles are defined in the [CPS].

8. Verifications and other Appraisals

The D-TRUST-Root-PKI CAs are hosted in the same facilities as the D-TRUST GMBH CA for the creation of qualified certificates with provider accreditation for being in strict accordance with the provisions of the German signature law. Revisions, objects subject to revision and processes are described in the security concept of the signature-law conforming certification service providers D-TRUST GMBH [SiKo-DTR]. The part “role-concept” of the same security concept [SiKo-DTR] describes the necessary qualification and the standing of the controller.

The security concept was audited by the TÜV Informationstechnik GmbH. It may partially be made available on request, if a vested interest is in evidence.

In addition, controls by external auditors of the technical control board TÜV Informationstechnik GmbH are conducted every three years in the course of the voluntary licensing process for the CSP’s accreditation according to §15 SigG (German Signature Law) and §11 SigV (German Signature Regulation). The signature-law approved procedure attests the D-TRUST GMBH a high security standard.

Class 3-2

Areas that cannot be reproduced along the lines of the qualified operations with provider accreditation (as for example the in-house operation of a root-CA) because of legal or technical differences are checked at least once a year in the course of internal revision procedures.

This CPS as well as the [CP] comply with the [ETSI-F] “NCP” and “NCP+” requirements for class 3 certificates, with “EVCP” requirements in the case of Class 3 EV-Certificates and with the [ETSI-F] “LCP” requirements in the case of class 2 certificates. A regular assessment by a „competent independent party“ as required in TS 102 042 [ETSI-F] (section 5.4.1) proves a continued compatibility.

The CSP only issues certificates including Policy-OIDs which reference [ETSI-F] after an initial and successful inspection regarding to [ETSI-F] compliancy by an independent, external and licensed auditor. Repeat inspections are carried out on a regular basis. Should the procedures prove not to comply with the current [ETSI-F] guidelines anymore, the CSP will refrain from issuing certificates until the compliancy has been restored and audited accordingly.

Class 3 EV-certificates

The CSP issues EV-certificates only after having its procedures audited in respect to their compliance with either the guidelines of [GL-BRO] by a J 35 [GL-BRO] entitled, independent and external certified accountant in possession of a WebTrust-license or in their compliance with the guidelines of [ETSI-F] “EVCP”. Should the procedures prove not to comply with the current [GL-BRO] guidelines anymore, the CSP will refrain from issuing certificates until the compliancy has been restored and audited accordingly. The audit is held annually.

In addition to the above, internal audits are held on a regular basis.

9. Other Financial and Legal Regulations

9.1 Prices

9.1.1 Certificate Prices

D-TRUST GMBH certification-fees are published in the price list that is available under:
<https://www.d-trust.net/internet/files/2.Preisinformationen.pdf>

9.1.2 Prices for Certificate Access

Requesting Certificates from the directory service is free of charge.

9.1.3 Prices for Revocations or Status Information

Revocations as well as retrieval of certificate status information are free of charge.

9.1.4 Prices for other Services rendered

See price list according to 9.1.1.

9.1.5 Rules of Reimbursement

The standard business terms apply.

9.2 Financial Responsibilities

9.2.1 Insurance Coverage

The D-TRUST GMBH's insurance coverage complies with the German act for electronic signatures § 12 SigG:

„The Certification Service Provider is obligated to ensure an appropriate coverage so that he may meet his statutory obligations to compensate the damages that occur if he breaches the requirements of this law or of the ordinance according to § 24 or if his products for qualified electronic signatures or other technical security provisions malfunction.. [...]“

The CSP complies with the requirements of [GL-BRO] 4.c and 37a.

9.2.2 Other Resources for Maintenance of Operation and Coverage

Not specified.

9.2.3 Insurance or Warranty for End-Users

Not specified.

9.3 Confidentiality of Business Data

9.3.1 Definition of Confidential Business Data

The confidentiality of information may be agreed upon, inasmuch as it is not already defined by established law.

9.3.2 Non-confidential Business Data

The information in created and published certificates as well as the information designated in section 2.2 is deemed as public.

9.3.3 Responsibilities for the Protection of Confidential Business Data

In isolated cases, the CSP may be bound to secure transferred data that has been tagged as confidential against divulgement and theft through technical and organizational provisions as well as to refrain from using said data in non-intended ways; any such commitment will be reviewed as related to the compliance with applicable law. The CSPs appointed employees are bound to secrecy through organizational measures within the limits of the law.

9.4 Privacy of Personal Data

9.4.1 Data-Privacy Concept

The CSP operates on the basis of an auditable security concept that regulates the protection of confidential personal data. The CSP complies with the requirements set-out in § 4a, b, § 9 and §§ 27 ff of the German Federal Data Protection Act (Bundesdatenschutzgesetz).

9.4.2 Definition of Personal Data

Any information pertaining to an individual that is collected by the RA for the purpose of creating a certificate is considered personal data.

9.4.3 Non-Confidential Data

Information that is explicitly integrated into certificates, CRLs and status information is not considered confidential.

9.4.4 Responsibilities for the Protection of Privacy

The CSP ensures data protection. Every CSP employee is contractually compelled to adhere to the data protection rules. Internally, the adherence is supervised by the operational data security engineer, which is complemented by the controls of the external supervision by the Berlin Commissioner for Data Security and Freedom of Information (Berliner Beauftragter für Datenschutz und Informationsfreiheit).

9.4.5 Indication and Acquiescence for the Utilisation of Personal Data

Upon application, the applicant is shown which personal data will be included in the certificate. Certificates will only be published after the applicant has given his assent during the application process.

Upon application, the applicant is informed that the RA only collects data that is necessary for the certificate creation and the operation of the D-TRUST-Root-PKI. He is additionally informed that his personal data is protected against third-party access and that his data will only be passed on if the CSP is legally compelled to do so.

Personal data that is no longer required is deleted. Personal data required for certificate verification is liable to section 5.5.2 of the [CPS].

9.4.6 Data-Disclosure Following Legal or Governmental Directives

§ 14 (2) SigG applies:

„Upon request, the Certification Service Provider must convey identifying data of a signature-key holder to the responsible authorities, as long as this is required for the persecution of felonies or misdemeanours, for the defense of public safety or public order or if it is necessary for the realization of the lawful duties of either the federal- or a state Office for the Protection of the Constitution, the Federal Intelligence Service, the Military Counter-Intelligence Service or the Revenue Department or if it has been court-ordered in accordance with the applicable regulations over the course of pending proceedings. The provided information is to be documented. The requesting government agency must inform the signature-key owner about the data-transferal as soon as the lawful duties will no longer be impeded by the disclosure or if the signature-key owner's interest outweighs the risks of impediment.“

Application data is kept while a certificate is valid as well as within the period noted in section 5.5.2 of the [CPS] and is subsequently archived in order to comply with these legal stipulations. Disclosures are documented and stored for at least a year.

9.4.7 Other Conditions for Data-Disclosure

Data is not disclosed for any other reasons than those described in section 9.4.6.

9.5 Industrial Trademark- and Copyrights

9.5.1 CSP

Endurance and content of the copyright and the rights to other intangible goods are based on the general statutory provisions.

9.5.2 Applicant

The applicant assumes responsibility for the compliance with intellectual property in the application- and certificate data.

9.6 Assurances and Guarantees

9.6.1 CSP Range of Services

The general terms and conditions apply. Insofar guarantees are not explicitly assured, the CSP grants no guarantees or assurances in the legal sense.

Class 3-2

The CSP ensures the conclusive, first hand identification of the applicant and the subscriber's correlation to the public key.

The CSP ensures the application of the procedures described in sections 4, 3.2 and 3.3 [CPS].

The CSP makes sure that the name used in the certificates (*DistinguishedName* in the field *subject*) will be unique inside of the D-TRUST-Root-PKI throughout its validity period and beyond and will irrefutably and uniquely correlate with the original subscriber. The explicit identification⁶ of the subscriber based on the certificate's name is ensured.

The CSP operates the CAs, a directory service and provides certificate status information.

Class 3 EV-certificates

The CSP assumes no warranties in the legal sense but does honor the terms of [GL-BRO] section 3 according to "Legal Existence", "Identity", "Right to Use Domain Name", "Authorization for EV Certificate", "Accuracy of Information", "Subscriber Agreement", "Status" and "Revocation". Apart from that, the CSP hosts an EV-reporting service according to section 28 [GL-BRO]. Relying parties may use the reporting service to flag suspicious EV-certificates. The CSP will investigate the relying party's suspicions.

The CSP may outsource subtasks to partners or external providers, while ensuring that the regulations laid-out in this CP and the [CPS] are met.

⁶ Compare footnote 1 on page 17.

9.6.2 Registration-Authority Range of Services

The CSP operates Registration Authorities (RA). The RA identifies and registers. The general terms and conditions, as well as the regulations in this CP apply.

9.6.3 Subscriber Confirmations and Guarantees

The CSP's general terms and conditions, as well as this CP apply.

Class 3

Upon application, the applicant (possibly in lieu of the subscriber) signs a subscriber agreement that contains the subscriber's confirmations and guarantees. The subscriber agreement complies with the [ETSI-F] regulations.

Class 3 EV-certificates

The subscriber agreement complies with the regulations in section E 12 [GL-BRO].

9.6.4 Relying parties Confirmations and Guarantees

Confirmations and guarantees of the relying parties are not regulated in this CP. The CSP and the relying parties do not incur a contractual relationship. Apart from that, the general terms and conditions, as well as legal requirements apply.

9.6.5 Confirmations and Guarantees of other PKI-participants

Not applicable.

9.7 Non-Liability

9.7.1 CSPs exclusion of liability

The general terms and conditions apply.

Class 3 EV-certificates

Inasmuch as Class 3 EV-Certificates are issued, the following additional regulations from section K 37 [GL-BRO] apply:

If the CSP issued the Class 3 EV-Certificate in full accordance to this CP, its liability for any damages incurred by the certificate's employment is naught.

9.8 Limitation of Liability

The general terms and conditions apply.

Insofar as the terms of this CP are violated in the production of Class 3 EV-Certificates, the following limited liability applies in accordance to the provisions of chapter K37 [GL-BRO]:

The CSP is accountable for the correct application screening and the resulting Class 3 EV-Certificate content only within the boundaries of its assessment feasibilities. The issue of a Class 3 EV-Certificate only proves that the necessary proof of identification or, as the case may be, proof of legitimization was provided to D-TRUST according to this CP at the time of application. If an external Registration Authority is contractually commissioned to conduct the identification process of the applicant, the RA's

identification process must be in accordance with the terms of this CP. If the RA disregards the terms of conduct, it must release D-TRUST from the resulting entitlements to damages that the subscriber or third parties may procure. The same is true for all occurrences in which the applicant acts as the Registration Authority in identifying subscribers that belong to the same organization.

The applicant is liable for any damages to D-TRUST that result from faulty information that is transferred to the Class 3 EV-Certificate, as well as the faulty usage of the Class 3 EV-Certificate.

In the above mentioned cases the CSP's liability is limited to 2000.00US\$ (two thousand dollars) - or the correlating amount in EUROS at the day that the damages are induced - per Class 3 EV-Certificate.

9.9 Compensation

9.9.1 CSP Claims towards Applicants/Subscribers

If the applicant gives the RA fraudulent information, the CSP can claim compensation according to legal regulations.

9.9.2 Subscriber Claims towards the CSP

The general terms and conditions apply.

9.10 CP validity period and expiration

9.10.1 CP validity period

This CP is valid from the date of publication and remains valid as long as certificates that have been issued on the basis of this CP remain valid.

9.10.2 CP Expiration

See chapter 9.10.1.

9.10.3 Consequences of CP Expiration

See chapter 9.10.1.

9.11 Individual Announcements for and Agreements with PKI-participants

CSP announcements for the subscriber are mailed to the last D-TRUST GMBH known address or e-mail address (digitally signed).

9.12 Addendums

9.12.1 Procedures for Addendums

Addendums to this CP are incorporated into this document and published under the same OID. Editorial changes will be highlighted.

9.12.2 Notification-mechanisms and -deadlines

Not specified.

9.12.3 Conditions for OID-Changes

Not specified.

9.13 Dispute-Mediation Regulations

Complaints regarding the fulfillment of this CP need to be submitted to the CSP in writing (D-TRUST GMBH, Kommandantenstr. 15, 10969 Berlin, Germany). If no redress has occurred within 4 weeks after the complaint has been filed, the following applies: Disputes may be addressed through legal action according to German law. Additionally, the CSP also provides an EV-reporting station as stated in 9.6.1. A suspected misuse of D-TRUST EV-Certificates can be reported via e-mail under: ev-support@d-trust.net.

9.14 Competent Court of Jurisdiction

The general terms and conditions apply.

9.15 Abidance of Applicable Law

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

9.16 Miscellaneous Regulations

9.16.1 Letter of Representation

The following documents are part of the standing agreements between CSP and PKI-participants:

- contract-documentation as well as application documentation,
- the general terms and conditions valid at the point of time of PKI-application use,
- the CP valid at the point of time of PKI-application use.

For class 3 SSL CAs, their Sub- as well as Root-CAs, the above holds true, and in addition, the [GL-BRO] valid at the time of PKI-application is also part of the standing agreements.

9.16.2 Delimitations

Not applicable.

9.16.3 Salvatorius Clause

If a regulation of this CP or its application is found null and void or not feasible for any reason and in any scope, the rest of the CP (as well as the application of the non-feasible or voided regulation in regard to other individuals or other circumstances) should be interpreted in such a way, that the agendas of the affected parties are taken into account to the maximum possible degree.

9.16.4 Enforcement (Attorney Fees and Waiver of Appeal)

The general terms and conditions apply.

9.16.5 Acts of God

The general terms and conditions apply.

9.17 Other Regulations

9.17.1 Conflicting Regulations

The regulations under 9.16.1 are conclusive. They apply in the order as listed in 9.16.1.

9.17.2 Complying with Export Laws and -Regulations

The export of certain software that is incorporated in the public certification services offered by D-TRUST GMBH may be subject to the prior approval of the appropriate government agencies. The parties will uphold the pertinent export-laws and –regulations.

The usage of the D-TRUST GMBH public certification services is subject to multiple laws of the Federal Republic of Germany. For any case of noncompliance with the public certification services, D-TRUST GMBH reserves the right of filing charges for criminal prosecution.