Certification Practice Statement of the D-TRUST Root PKI

Version 1.13

Date of issue	23 February 2015
Effective date	23 February 2015

BUNDESDRUCKEREI | 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
1.0	18 June 2008	▸ Initial version
1.1	1 November 2008	▸ Change in terms for authorisation to submit applications with a view to legal age ▸ Adaptation of the verification methods for SSL certificates with dNS names ▸ Generalisation of the OCSP path ▸ Adaptation of verification methods of Class 1 certificates ▸ Adaptation for SSL certificates
1.2	1 June 2009	▸ Expansion of the blocking reasons of code-signing certificates ▸ Editorial changes ▸ Adaptation due to WebTrust audit
1.3	25 February 2010	▸ More detailed specification: neither renewal nor renewal with key renewal will be offered for SSL certificates
1.4	21 September 2010	▸ Update due to a new version of [ETSI-F] and [GL-BRO]
1.5	2 February 2011	▸ SSL certificates restricted to domains with mandatory registration
1.6	14 September 2011	▸ Term for SSL certificates restricted to 39 months
1.7	26 July 2012	Extension of the Class 2 validity periods ▸ Decoupling Class 2 from "LCP"
1.8	7 February 2013	Adaptation due to amendment to [ETSI-F] including Baseline Requirements of the CA/Browser Forum [BRG] and Network and Certificate Systems Security Requirements [NetSec-CAB].
1.9	30 October 2013	Definitions of subject and subscriber amended to match [ETSI-F]. Introduction of the LCP level and the related methods. Redundancies in the relationship to CP were removed by crossing off/references. Additions with technical and organisational measures according to [ETSI-F] ▸ - Section 7.4.5: Operations management ▸ - Section 7.4.6: System access management
1.10	1 May 2014	Adaptation of certificate profiles, section 7.1.2 and 7.1.3 Formal adaptation of the class notation
1.11	1 November 2014	▸ Editorial corrections ▸ Key length increased to at least 2048 bits for all certificate classes ▸ Hash algorithm SHA-1 no longer applicable
1.12	17 November 2014	▸ Change in the permitted hash algorithms
1.13	23 February 2015	Inclusion of various contents from the D-TRUST Certificate Policy as part of reorganising this certificate policy.

Contents

1. Introduction

1.1 Overview

This document is the Certification Practice Statement (CPS) of the D-TRUST root PKI operated by D-TRUST GMBH.

1.1.1 Trust service provider

These rules are laid down in the CP.

1.1.2 About this document

This CPS defines processes and procedures within the scope of the certification services throughout the entire life of the CA and end-entity certificates (EE certificates). It lays down the minimum measures which all PKI entities must fulfil.

This CPS refers to the CP (certificate policy) of D-TRUST GmbH and the ETSI Policy TS 102 042 as CP (certificate policy) and describes the implementation of the resultant requirements.

Both CA and EE certificates can contain references to CPs which define detailed requirements and restrictions.

The complete CPS 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 CPS.

Knowledge of the certification procedures and rules described in this CPS 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 CPSs.

The CPS explains or expands the methods described in the related CP; in the case of identical wording, references to the CP are used.

1.1.3 Properties of the PKI

The D-TRUST Root PKI has a multi-level hierarchy. Fig. 1 shows the set-up of D-TRUST Root PKI.

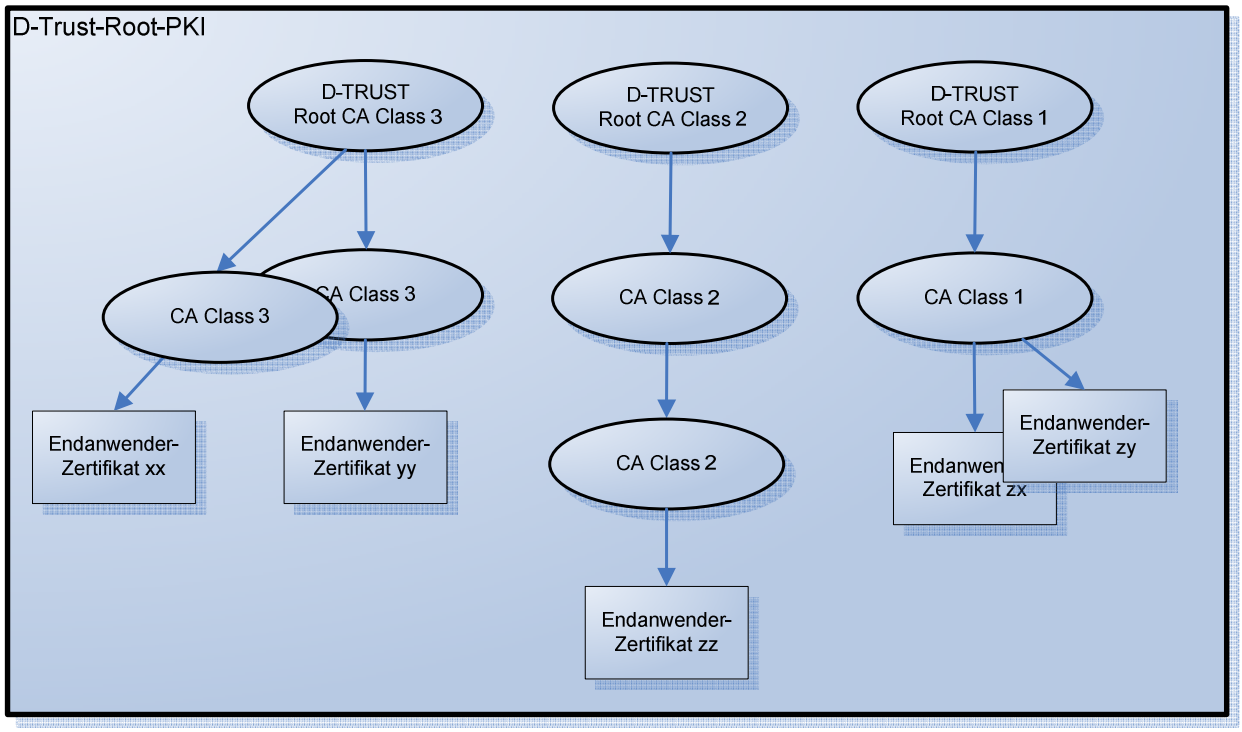

Fig. 1: Example of the set-up of the D-TRUST Root PKI

The EE and CA certificates can be assigned to one of three classes (Class 3, Class 2 or Class 1). The higher the class, the higher the quality of the certificates, so that Class 3 certificates almost have the same quality as qualified certificates according to [SigG]. Unless this document distinguishes between classes or unless certain classes are expressly ruled out, the requirements or provisions of the respective sections are applicable to all three classes.

Class 3

Class 3 certificates have a particularly high quality, however, they are not qualified certificates (according to the definition contained in the German Act on Digital Signature [SigG]) which in many respects meet the requirements of qualified certificates according to the SigG. They meet the requirements of [ETSI-F] in the versions "NCP", NCP+" or "OVCP".
SSL certificates are exclusively issued for legal entities and as "OVCP" and "EVCP" versions.

Class 3 EV certificates are not a separate class. All of the information listed here for "Class 3" is also valid for Class 3 EV certificates; in the event of any deviations, these will be additionally listed for Class 3 EV certificates.

Class 3 EV certificates, (in brief: Class 3 EV)

Class 3 SSL EV certificates are a special kind of Class 3 certificate. They are subject to the requirements of GL-BRO or ETSI-F EVCP. The fact that they are EV certificates can be recognised in the EE certificates by the EV policy OID (as described in section 1.2).
Class 3 EV certificates are not issued on smart cards.

Class 2
Class 2 certificates have a high quality, however, they are not qualified certificates.

Class 2 LCP certificates (in brief: Class 2 LCP)
Special kind of Class 2 certificate. LCP certificates have a high quality, however, they are not qualified certificates which meet the requirements of ETSI-F LCP. All of the information listed here for "Class 2" is also valid for Class 2 LCP certificates; in the event of any deviations, these will be additionally listed for Class 2 LCP certificates.
Class 2 LCP certificates are not issued on smart cards.

Class 1
Class 2 certificates are simple certificates.

1.2 Name and identification of the document

Document name:	Certification Practice Statement of the D-TRUST Root PKI
Version	1.13

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)
- Group certificates for groups of individuals, functions and IT processes (EE certificate)
- Machine certificates for IT processes and communication connections (SSL certificates/EE certificate)
- Certification instances (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)

The RA identifies and authenticates subscribers or subjects, and it collects and checks applications for different certification services.

1.3.3 Subscribers and end-entities (EEs)

Subscribers are individuals or legal entities who apply for and hold EE certificates. The subscriber can be identical to the end-entity *(subject)* whose name appears in the certificate.

Subjects (end-entities (EEs)) use the private end-entity keys (EE keys). The subject's identity is linked to the certificate and the related key pair. The end-entity can be identical to the subscriber. Valid subscribers are:

- Individuals
- Organisations (legal entities – under private and public law, other government institutions and individual companies)
- Groups of individuals
- Functions which are performed by staff of an organisation
- IT processes (such as SSL server)

Class 2
: Class 2 certificates for individuals are also issued if the subscriber and the end-entity are not identical.

Class 3, Class 2
: The subscriber is responsible for the key and certificate. In addition to this, further obligations result from ETSI-F. At the time of submitting the application at the latest, subscribers receive this CPS and the subscriber agreement as information about these obligations which they are obliged to adhere to. In the event that the subscriber and end-entity are individuals, but not identical, the subscriber is obliged to inform the end-entity about these obligations.

Class 1
: No distinction is made in Class 1 between subscriber and end-entity. In this case, whoever submits the application takes on both roles and hence bears sole responsibility for keys and certificates.

In the case of SSL certificates, this subscriber agreement applies to SSL certificates. The CSM subscriber agreement applies to all other certificates under this policy.

1.3.4 Relying parties

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

1.4 Use of certificates

1.4.1 Permitted uses of certificates

CA certificates are used exclusively and in line with their extension (BasicConstraints, PathLengthConstraint) for issuing CA or EE certificates and CRLs.

EE certificates can be used for applications which are compatible with the types of use shown in the certificate.

Certificate users are solely responsible for their acts. Certificate users are responsible for judging whether this CPS meets with the requirements of an application and whether the use of the particular certificate is suitable for a given purpose.

1.4.2 Forbidden uses of certificates

Types of use not laid down in the certificate are not permitted.

1.5 Maintenance and updating of the CPS

1.5.1 Responsibility for the document

This CPS is maintained and updated by D-TRUST GMBH. The head of the certification service provider (CSP) is responsible for acceptance of the document.

This CPS is regularly checked each year and updated by the TSP when necessary. A change is indicated by a new version number of this document.

1.5.2 Contact partner/contact person/secretariat

These rules are laid down in the CP.

1.5.3 Compatibility of CPs of external CAs with this CP

Class 3 EV certificates

The TSP warrants adherence to the latest version of the guidelines of the CA-Browser Forum for the issuance and management of extended validation certificates (http://www.cabforum.org). In the event of a contradiction between this CP and the guidelines, the guidelines of the CA-Browser Forum have precedence.

For CAs, which have a CP that provides the same security and trust standard with a view to all essential technical and legal aspects of the services, the TSP can issue a cross certificate so thereby confirming the equality of the standard of the corresponding CP. This cross certification is carried out exclusively by CAs which were not ETSI-certified or for CAs which are already ETSI-certified. Cross certificates must have the entry "path-length=1" and are published in the repository of the TSP (see section 2.1).

The TSP guarantees the correctness of the details in the cross certificates issued for the "external" CA, as well as for compatibility of the external policy with this CP at the time the cross certificate is issued. Any major change in the external policy which has an adverse effect on compatibility results in revocation of the cross certificate by the TSP.

If cross certification by other CAs is foreseen, these CAs must notify D-TRUST GmbH immediately. D-TRUST GmbH reserves the right to object to the inclusion of cross certification.

Class 3 SSL EV certificates, their sub-CAs and root CAs comply with the requirements of the CA/Browser Forum's Guidelines for Extended Validation Certificates [GL-BRO]. In the event of discrepancies between this document and the aforestated guidelines, [GL-BRO] has precedence with a view to Class 3 SSL EV CAs as well as their sub-CAs and root CAs.

1.6 Terminology and abbreviations

1.6.1 German terms and names

These rules are laid down in the CP.

1.6.2 English terms

These rules are laid down in the CP.

1.6.3 Abbreviations

These rules are laid down in the CP.

1.6.4 References

These rules are laid down in the CP.

2. Responsibility for repositories and publications

2.1 Repositories

These rules are laid down in the CP.

2.2 Publication of information concerning certificates

The TSP publishes the following information regarding the D-TRUST Root PKI:

- EE certificates if this was requested by the subscriber
- CA certificates (trust anchors)
- Certificate revocation lists (CRLs) and status information
- The CP
- This CPS
- The subscriber agreement for SSL certificates
- The subscriber agreement for all other certificates under this policy
- Cross certificates

2.3 Publication frequency

EE certificates can be published, i.e. entered in the public repository of the TSP. The subscriber can accept or refuse publication. Depending on the specific product concerned, prior consent to publication can be a precondition for applying. Published EE certificates can be retrieved until the end of their validity term plus at least one more year and until the end of the year.

CA certificates are published after their creation and maintained after the validity of the CA has expired:

- at least 5 years (Class 3) and until the end of the year or
- at least 1 year and until the end of the year (Class 1 and Class 2).

Certificate revocation lists are issued regularly and until the end of validity of the issuing CA certificate. Certificate revocation lists are published immediately following revocations. Even if no certificates were revoked, the TSP ensures that a new certificate revocation list is created at least every 24 hours. The certificate revocation lists are retained and kept for a minimum period of one year following expiration of the validity of the CA.

As described in section 2.1, this CP and CSP are published and available for retrieval for a minimum period which is at least equal to the period of validity of

certificates which were issued on the basis of this CP. The websites have high availability.

2.4 Directory access control

These rules are laid down in the CP.

3. Identification and authentication

3.1 Name rules

3.1.1 Types of names

CA and EE certificates generally contain information regarding the issuer and the subscriber and/or subject. In line with the [X.501] standard, these names are given as DistinguishedName.

Other alternative names can be registered and included in the subjectAltName extension of the certificates.

3.1.2 Need for telling names

The DistinguishedName used is unambiguous within the D-TRUST Root PKI.

Class 3, Class 2
Unambiguous assignment of the certificate to the subscriber (and to the end-entity in the case of certificates for individuals) is ensured.

In the case of alternative names (*subjectAltName*), there is no need for telling names with the exception of SSL certificates (including Class 3 EV certificates).

This information may not include any references to the certificate itself. IP addresses are not permitted.

3.1.3 Anonymity or pseudonyms of subscribers

Pseudonyms are used exclusively for individuals. Pseudonyms are generally assigned by the TSP. Freedom of choice in selecting pseudonyms can be agreed to, see section 3.1.6. The TSP reserves the right to reject assigning a particular pseudonym without having to justify the decision.

Class 3, Class 2
In the case of certificates that were created with pseudonyms too, the TSP records the subject's (and, if applicable, the subscriber's) real identity in the documentation.

3.1.4 Rules for the interpretation of different name forms

It is not necessary to use all the DN components mentioned here. Further components can be added.

Class 3 EV certificates
EE certificates contain as a minimum the subject DN components: "O", "CN" or "SubjectAlternativeName with the Domain", "BusinessCategory", "Jurisdiction of

Incorporation or Registration", "SerialNumber", "L", "State" as well as "C". "Street" and "Postal Code" can also be included.

Class 3, Class 2

Supplementary DN components must comply with [RFC 5280] and [Co PKI], i.e. attributes of the *DistinguishedNames* (DN components) of EE certificates are interpreted as follows:

DN component	**Interpretation**
G	*First name(s)* of the individual according to - Class 3 and Class 2, the document presented for identification - Class 1, the subscriber's details
SN	*Family name* of the individual according to - Class 3 and Class 2, the document presented for identification - Class 1, the subscriber's details If pseudonyms are used, SN corresponds to CN.
CN	*Common name:* The following variants are used: - Individuals without a pseudonym: "family name, name used". - Individuals with a pseudonym: "Pseudonym:PN". - Legal entities: official name of the organisation (company, public authority, association, etc.), if necessary, reduced to a meaningful name if the maximum number of 64 characters is exceeded. Special case: It is also possible to include one or more domain names in the CN. Wildcards are not permitted for EV certificates. - Function or group of individuals: Name of the function or group of individuals preceded by the abbreviation "GRP:" in order to indicate that this is a group certificate - Technical components: Name of the server, service or application using the certificate
PN	*Pseudonym*: identical to CN.
serialNumber	*Serial number*: Name suffix number to ensure unambiguity of the name (typically the application number). Special case for Class 3 EV certificates according to [GL-BRO]: Registration number, if assigned, date of registration or establishment, or a text describing the fact that the entity is a public-law institution. Other product-specific uses of the field are possible.

DN component	Interpretation
DNQ	DN Qualifier: Carrier of the *serial number* in certificates where the subject serialNumber field is used for other purposes. Ensures unambiguity of the DN (2.5.4.46 - id-at-dnQualifier) according to [ETSI-F].
O	Official name of the *organisation* to which the subscriber belongs or to which he or she is otherwise connected (company, public authority, association, etc.) according to the proof of existence; if necessary, reduced to a meaningful name if the maximum number of 64 characters is exceeded.
OU	*Organisation unit* (department, division or other unit) of the organisation.
C	The notation of the country to be stated corresponds to [ISO 3166] and is set up as follows: If an organisation O is included in the DistinguishedName, the registered office of the organisation will determine the country C. If no organisation O is entered, the country which issued the document by which the subscriber was identified will be entered.
Title	A *Title* can be included.
Street	Postal address *Street*
Locality	Postal address *City*
State	Postal address *(Federal) state*
PostalCode	Postal address *Postal code*
BusinessCategory	Business category (2.5.4.15) according to [GL-BRO]
Jurisdiction Of Incorporation Locality	Jurisdiction of the organisation according to [GL-BRO]: *City* (1.3.6.1.4.1.311.60.2.1.1)
Jurisdiction Of Incorporation State Or Province Name	Jurisdiction of the organisation: *(Federal) state* (1.3.6.1.4.1.311.60.2.1.2)
Jurisdiction Of Incorporation CountryName	Jurisdiction of the organisation according to [GL-BRO]: *Country* (1.3.6.1.4.1.311.60.2.1.3)

3.1.5 Unambiguity of names

Class 3, Class 2

The TSP ensures that the subscriber's and/or subject's ("Subject" field) name (DistinguishedName) used in EE certificates is always unambiguous within the

D-TRUST Root PKI and beyond the lifecycle of the certificate and that it is always assigned to the same subscriber or subject, respectively. Unambiguity is achieved via the serial number and/or via the DN Qualifier (2.5.4.46 - id-at-dnQualifier) if this exists. This ensures the unambiguous identification of the subscriber on the basis of the name (subject) used in the EE certificate.

The TSP ensures the unambiguity of DistinguishedNames in CA certificates.

3.1.6 Recognition, authentication and the role of brand names

The subscriber is liable for compliance with intellectual property rights in the application and certificate data (see section 9.5).

Class 3 EV certificates

The TSP takes any steps which are necessary to ensure that, at the time the EV certificate is issued, the party named in the Subject field of the certificate has the exclusive right to use the FQDNs listed in the certificate.

3.2 Initial identity verification

3.2.1 Proof of ownership of the private key

Two cases are distinguished:

1. Key pairs of subscribers are produced in the TSP's sphere of responsibility. The TSP forwards the tokens or soft PSE (LCP) and, if applicable, the PIN letters according to section 4.4.1 to the subscribers and thereby ensures that the subscribers receive the private keys.

2. Key pairs are produced in the subscriber's sphere of responsibility. Ownership of the private keys must either be technically proven or plausibly confirmed by the subscriber. By sending a PKCS#10 request to the TSP, the subscriber issues binding confirmation of being the owner of the private key.

3.2.2 Identification and authentication of organisations

Organisations which are either named in the certificate or in whose names certificates are issued must provide unambiguous proof of their identity.

Class 3
Identification and verification at a very high level. The relevant NCP, EVCP or OVCP requirements from [ETSI-F] apply to subscriber identification and application checking. Verification covers all DN components.

Class 3 EV certificates
The requirements from [GL-BRO] (see CPS Annex A) and section 12.2 [GL-BRO]

apply to identification and authentication as well as to the verification of application data.

Class 2
Identification and verification at a medium level. Subscriber identification and verification of application data are carried out on the basis of the details provided by trusted third parties (e.g. department head or HR department, as contractually agreed).

Class 2 LCP
Identification and verification at a high level. The LCP requirements from [ETSI-F] apply to subscriber identification and application checking.

Class 1
Identification and verification at a low level. Only the e-mail address and, if applicable, the domain name and/or organisation name are checked.

In the various classes, the verification procedures described are applied as follows to the DN components according to section 3.1.4 plus further attributes, if necessary and applicable. The procedures shown in the table below are described in section 4.2.1.

	Class 3	**Class 2**	**Class 2 LCP**	**Class 1**
CN O C	Register/ Non-Register/ Domain	Register/ Non-Register/ Domain	HR-DB/Register/ Non-Register/ Domain	Register/ Domain
OU STREET L State PostalCode	**C confirmation** / Register/ Non-Register	A confirmation/ Register/ Non-Register/ out-of-band mechanisms/ Domain	A confirmation/ Register/ Non-Register/ out-of-band mechanisms/ Domain	No verification
E-mail address:	No verification (confirmation by the subscriber)	No verification (confirmation by the subscriber)	No verification (confirmation by the subscriber)	No verification (confirmation by the subscriber)

	Class 3	Class 2	Class 2 LCP	Class 1
All other attributes	**C confirmation**/ A confirmation/ Dok-Ident/ out-of-band mechanisms	A confirmation/ Dok-Ident/ out-of-band mechanisms	A confirmation/ Dok-Ident/ out-of-band mechanisms	No verification

If the application is submitted on behalf of a legal entity, the representative must (in analogy to the class-specific procedure for proving affiliation with the organisation according to section 3.2.3) prove his or her authorisation to this effect and also furnish proof of his or her identity.

Documents in non-Latin characters are not accepted.

3.2.3 Identification and authentication of individuals

Individuals applying for certificates must provide unambiguous proof of their identity and, when necessary, also that their organisation has authorised them to submit the application.

Class 2
Subscribers applying for certificates for other individuals must furnish proof of their authority to submit such applications. The subscriber's data is verified.

In the various classes, the verification procedures described are applied as follows to the DN components according to section 3.1.4 plus further attributes, if necessary and applicable. The procedures mentioned are described in section 4.2.1.

	Class 3	Class 2	Class 2 LCP	Class 1
G	Pers-Ident	HR-DB/ Dok-Ident/ **C confirmatio**	HR-DB/ Dok-Ident/ **C confirmatio**	
SN				
CN				
C				
STREET				
L				
S				
PostalCode				

	Class 3	Class 2	Class 2 LCP	Class 1
Title	Pers-Ident/ Dok-Ident	**n** A confirmation/ Public bodies/ out-of-band mechanisms	**n** A confirmation/ Public bodies/ out-of-band mechanisms	
O (organisation affiliation)	**C confirmation** **C confirmation**	A confirmation/ **C confirmation** Public bodies/ out-of-band mechanisms/ HR-DB	A confirmation/ **C confirmation** Public bodies/ out-of-band mechanisms/ HR-DB	
OU (organisation affiliation)				
E-mail address	No verification (confirmation by the subscriber)	No verification (confirmation by the subscriber)	No verification (confirmation by the subscriber)	E-mail
All other attributes	**C confirmation**/ A confirmation/ Dok-Ident/ out-of-band mechanisms	A confirmation/ Dok-Ident/ out-of-band mechanisms/ HR-DB	A confirmation/ Dok-Ident/ out-of-band mechanisms/ HR-DB	

In the case of applications for certificates for groups, functions or IT processes, all attributes shown in the table for the subject (except for OU, e-mail address, all other attributes unless relevant for the certificate) are verified on a class basis. The inclusion of names for groups, functions or IT processes in the CN is subject to the class-specific procedures analogous to the "All other attributes" line.

Documents in non-Latin characters are not accepted.

3.2.4 Non-verified information concerning the subscriber

Class specific verification of the subscriber's information is carried out or skipped according to sections 3.2.2, 3.2.3 and 4.2.1. In the case of alternative names, only the e-mail addresses are generally verified. Other alternative names, such as addresses of websites and LDAP directories, etc. as well as certificate extensions, if any (AdditionalInformation, monetaryLimit, etc.), are not checked for correctness (see also section 4.9.1).

One exception to this are Class 3 SSL certificates where the alternative name is used for inclusion of further URLs. In these cases, the dNSNames are also verified.

3.2.5 Verification of authority to apply

Applications can only be submitted by individuals and legal entities.

Class 3, Class 2
In the case of individuals, the identity and, if necessary or applicable, affiliation with the organisation concerned will be determined and verified and/or confirmed using the class-specific procedures according to section 3.2.3. In the case of organisations, proof of their existence and the applicant's right to represent the organisation in question will be verified and/or confirmed on a class-specific basis according to section 3.2.2.

Class 1
Apart from economic verification, no other checks are carried out to confirm authorisation to submit applications.

3.2.6 Criteria for interoperability

See section 1.5.3.

3.3 Identification and authentication of applications for re-keying

Re-keying is equivalent to the production of new certificates and, if applicable, tokens and keys for the same subject. Re-keying is only offered for Class 3 and Class 2, but not for Class 1 and Class 3 EV certificates. In the case of Class 3 EV certificates, the complete identification and registration process which also

applies to first-time applications must be carried out. It is, however, possible to re-use existing proof and verification documents in as far as they are still valid as such according to section 8.3.2 [GL-BRO].

3.3.1 Routine re-keying applications

New certificates and, if applicable, keys and tokens are issued for the time after the validity of EE certificates (Class 3, Class 2) has expired or when requested by the subscriber. Identification does not have to be repeated in the case of re-keying applications. Re-keying applications must be provided:

- with a qualified electronic signature or
- with an electronic signature of at least the applicable class or
- with a hand-written signature.

Procedures other than the above can be agreed to on a case-to-case basis.

The conditions of section 4.7 must be fulfilled.

3.3.2 Re-keying after revocation

Re-keying on the basis of a certificate that has been revoked is not offered.

3.4 Identification and authentication of revocation requests

Before revoking an EE certificate, the TSP checks whether the party applying for revocation is authorised to do so. This procedure is defined in the CP and the CPS.

Other procedures for authenticating revocation requests can be agreed to with the subscriber. Revocation procedures are defined in section 4.9.

Revocation authorisation is verified as follows:

If a revocation request is received in a signed e-mail, revocation must be requested by the subscriber himself, or the party requesting revocation must have been named as a third party authorised to revoke whose certificate must be available to the TSP.

Class 3, Class 2
In the case of a personally signed revocation request sent by post, the comparison of the signature must prove that the individual applying for revocation is either the subscriber or a third party named and authorised to apply for revocation.

Class 3, Class 2

In the case of revocation requests submitted by telephone or in the case of a request by e-mail without a signature, the third party authorised to revoke must give the correct password.

Class 1

In the case of a personally signed revocation request sent by post, the individual applying for revocation must be the subscriber.

Other procedures for authenticating revocation requests can be agreed to with the subscriber.

Revocation procedures are defined in section 4.9.

4. Operational requirements

4.1 Certificate application and registration

4.1.1 Application authorisation

Applications can only be submitted by individuals and legal entities (their authorised representatives).

Group certificates are issued for legal entities and individual companies only.

If the TSP offers this, it can safely deposit private EE keys other than signature keys or keys for Class 3 EV certificates according to the requirements of section 6.2.3 of the CPS for future use (key escrow, re-use in a new token). The subscriber must apply for the key(s) to be deposited and state that the private EE key is to be re-used for the same subscriber and/or group of individuals. In order to re-use EE keys according to section 6.2.3 of the CPS, the subscriber must prove that he or she is authorised to re-use the key in question.

Class 3 EV certificates
Subscribers must fulfil the requirements in section 7.2 [GL-BRO].

CA certificates are exclusively issued to legal entities.

The TSP is entitled to reject applications (see section 4.2.2).

4.1.2 Registration process and responsibilities

The TSP warrants compliance with the registration process. Sub-tasks can be carried out by partners or external providers under a corresponding agreement if such partners or external providers fulfil the requirements of the CP.

Class 3, Class 2
Prior to commencing the registration process, the subscriber receives the CP, the CPS and a subscriber agreement and undertakes to abide by the terms and conditions thereof. The documents are published. The subscriber agreement fulfils the requirements from [ETSI-F]. The application also includes the subscriber's consent to the certificates being published or not. Proof is kept electronically or in printed form.

Class 3 EV certificates
The subscriber agreement corresponds to the requirements in section 9.3 [GL-BRO].

4.2 Processing the certificate application

4.2.1 Identification and authentication procedure

The identification and registration process described herein must be carried out completely on a class-specific basis and all the proof necessary must be provided.

Individuals or organisations can be authenticated and further certificate-relevant data verified before or after submission of the application, but must be completed before certificates and key material, if any, and PINs are handed over.

Class 3, Class 2
Individuals must be unambiguously identified; in addition to the full name, further attributes (such as place and date of birth or other applicable individual parameters) must be used to prevent individuals from being mistaken. If legal entities are named in the certificate or if legal entities are subscribers, the complete name and legal status as well as relevant register information must be verified.

The TSP defines the following verification methods:

Pers-Ident
Using a valid ID document, the individual must in person prove his or her identity before an RA, an authorised partner or an external service provider who fulfils the requirements of the CP. Acceptable documents are ID cards or passports of nationals of a member state of the European Union or of a country of the European Economic Area, as well as documents offering an equivalent degree of safety. Documents used as proof are filed.

Dok-Ident
The contents to be verified are compared to the application data on the basis of copies (printed copies or electronically scanned documents or fax transmissions). An out-of-band mechanism is used for random queries in order to verify the correctness of contents. Permissible documents are those specified for the Pers-Ident procedure, as well as extracts from commercial or equivalent registers which are not older than six months, doctorate or habilitation certificates as well as documents of an equivalent importance. Documents used as proof are filed.

Register
The application data is compared (or captured) manually or automatically to copies of extracts from printed or electronic registers. Acceptable registers are registers of government bodies (registration courts, German Federal Central Tax Office, processional associations under public-law or equivalent organisations) or registers organised under private law (DUNS, comparable business databases, government bodies organised under private law). Register entries are only

accepted as valid if they do not include attributes of the "invalid", "inactive" or equivalent types. Documents used as proof are filed.

Non-Register
Government bodies/institutions under public law confirm certificate-relevant information under their official seal and signature. Documents used as proof are filed.

HR-DB
The TSP enters into an agreement with an organisation (subscriber) and stipulates that only valid data is to be transmitted which meets with the requirements of the CP. An authorised employee or representative of an organisation forwards extracts from the organisation's human resource database and/or requests generated on the basis of such data to the TSP via a secure communication channel. The organisation is obliged to respect the relevant data protection requirements. The TSP trusts in the correctness and unambiguity of the data transmitted. At the time the tokens are handed over at the latest, the subscriber informs the subject about the latter's obligations under the subscriber agreement. The following items are filed:

- electronic or printed copies of the data transmitted,
- confirmation/proof of the forwarder as "authorised employee" or "authorised representative", respectively,
- proof that the data was provided for processing by an authorised employee, and
- proof that the subscriber has consented to the subscriber agreement.

C confirmation
An authorised signatory of the organisation confirms certificate-relevant information. This is carried out in writing, with the possibility of electronically signed confirmation being accepted in individual cases. The authorisation to sign must become apparent either from the proof of existence for the organisation, or it must be proven in another suitable manner. Documents used as proof are filed.

A confirmation
Authorised employees or representatives within an organisation or trusted third parties (for instance, partners of the TSP or government bodies) confirm certain certificate-relevant information which they are authorised to confirm. This is carried out in writing, with the possibility of electronically signed confirmation being accepted in individual cases. Documents used as proof are filed.

out-of-band mechanisms
The TSP uses out-of-band mechanisms in order to check the correctness of application data using communication channels and verification methods which

the subscriber is unable to influence. Documents used as proof are documented and filed electronically or in printed form.

Proof of existence of organisations or individuals can, for instance, be provided to the TSP in the form of bank transfer, direct debit or payment by credit card. The TSP trusts the bank whose customer the organisation and/or individual is. Verification by telephone by the TSP via a public telephone directory is also permitted.

In order to identify individuals, the TSP can send a letter "by registered mail with acknowledgement of receipt" to the subscriber, with the signature on the receipt being compared to the signature on the passport copy or in the application documents.

The subject's affiliation with an organisation can also be verified by way of a verification letter "by registered mail with acknowledgement of receipt" to the organisation to the attention of the subject. The signature on the registered letter is compared to the signature on the passport copy or in the application documents. Affiliation with an organisation, e-mail address, contents of extensions as well as any further certificate-relevant data can also be confirmed in the form of an enquiry by telephone to be made by the TSP using a public telephone directory.

Public bodies
The TSP enters into an agreement with public bodies and stipulates that only valid data is to be transmitted which meets with the requirements of the CP. An authorised employee or representative of this public body forwards to the TSP personal data and/or application forms created on the basis of such data via a secure communication channel. The public body is obliged to respect the relevant data protection requirements. Moreover, the same procedures corresponding to HR-DB apply.

Domain
The domain of an organisation and, if applicable, other attributes, such as e-mail addresses, are verified by a domain query in official registers (WHOIS). Class 3 and Class 2: In this case, it is questioned whether the subscriber has exclusive control of the domain. The results of the enquiry are filed. In the case of EV certificates, the domain name is additionally checked against blacklists of known phishing domains. Domain names not subject to a registration obligation (no top-level domains) are not permitted.

E-mail
The TSP sends an e-mail to the e-mail address to be confirmed, and receipt of this e-mail must be confirmed (exchange of secrets). The results of the enquiry are filed.

Identification and authentication are carried out according to sections 3.2.2 and 3.2.3.

4.2.2 Acceptance or rejection of certificate applications

An "independent second" person of the role foreseen in the security concept and commissioned by the TSP examines the application documents on the basis of the following criteria:

- Was authentication of the subscriber correctly carried out and documented?
- Was all the proof required provided?
- Are there reasons that justify rejection of the application?

Other reasons for rejection include:

- Suspected violation of name rights of third parties;
- Non-adherence to deadlines for proof of data;
- Payment arrears of the applicant in relation to the TSP or
- Circumstances justifying suspicion that the issuance of a certificate could discredit the operator of the CA.

The TSP is entitled to reject certificate applications without giving reasons.

In the event that any inconsistency occurs during identity verification by the RA or the TSP or during the check of the data in the certificate application or in the ID card and proof documents that cannot be fully resolved by the subscriber in a timely manner, the application will be rejected.

Following extensive examination as laid down in the procedural instructions, the person examining the application decides on the basis of their findings whether the application is to be rejected or processed further.

When the TSP receives PKCS#10 or other certificate requests, the contents thereof are checked by the TSP for correctness. Such check does not have to be carried out by the TSP if contractual agreements are in place with partners where commissioned, independent persons make the requests available to the TSP for production. The contents of certain certificate contents (for instance, O or OU) can be determined by agreement.

If the TSP receives certificate data in advance via a client-enabled online interface, the certificate data can be checked in advance. When the TSP then forwards the certificate request itself after checking, certificates can be issued immediately.

The application is not deemed to be unreservedly accepted until the TSP has made a positive decision regarding the certificate application and the certificate applied for and any key material has been handed over (see section 4.4).

4.2.3 Deadlines for processing certificate applications

Not applicable

4.3 Issuance of certificates

4.3.1 Procedure of the TSP for the issuance of certificates

The corresponding certificates are produced in the high-security area of the trust service provider.

Use of the correct time during certificate production is ensured.

The TSP either files the complete application documentation in accordance with section 5.5 in an auditable manner, or the TSP concludes agreements with partners pursuant to which the application documents and/or requests have to be filed in a safe manner and completely until the expiration of the period according to section 5.5.2.

4.3.2 Notification of the subscriber that the certificate was issued

The subscriber does not receive separate notification of completion of the certificate.

4.4 Certificate handover

4.4.1 Procedure during certificate handover

Similar to the procedures used for qualified signature cards, smart cards are sent either by post or courier to the address stated or handed over in person to the subscriber by the RA or an authorised employee or representative, or, if requested by the subscriber, handed over to the subject.

Soft PSEs whose private key was produced in the area of the TSP are sent, as requested by the subscriber, on a storage medium (by mail to the address shown in the application), made available for access-protected and SSL-encrypted download or sent by e-mail (the PKCS#12 file being protected by a PIN).

If a certificate is issued for a key pair that is already available at the subscriber, the certificate is either made available for downloading (for instance, published in the repository service) or sent electronically.

Other methods can be agreed to on a customer-specific basis.

In the event that the subscriber detects errors in his certificates or in conjunction with the function of the keys and tokens, he must communicate this to the TSP. The certificates are then revoked. Following revocation, the TSP can demand that the subscriber send the smart cards back to the TSP.

Incorrect data in the certificate is only deemed to be a contractual defect within the meaning of the law in as far the TSP performs a check of the functions affected by such defect according to this CP. Otherwise the relevant rules for remedial measures according to the applicable General Terms and Conditions [AGB] are applicable to defects and their existence.

Acceptance by the customer does not take place, the delivery constituting a service rather than a work within the meaning of German civil law.

4.4.2 Publication of the certificate by the TSP

If the subscriber in the certificate application has consented to publication of the certificate, the certificates will be published after production[1] in the public repository service. The certificate will not be published if the subscriber has not consented to publication.

The status can in both cases be retrieved via OCSP after production (see section 2.1)[2].

4.4.3 Notification of other PKI users concerning the issuance of the certificate

Third parties authorised to request revocation according to section 4.9.2 are notified in writing and receive the revocation password unless anything to the contrary was agreed to with the organisation or the party authorised to request revocation.

4.5 Use of the key pair and of the certificate

4.5.1 Use of the private key and of the certificate by the subscriber

Subscribers and subjects are entitled to use their private keys exclusively for those applications which are in conformity with the types of use stated in the certificate.

Class 3, Class 2
The provisions in section 1.4 apply to subscribers.

[1] If the token contains, in addition to the advanced certificates of the root PKI, further subject certificates (qualified certificates or qualified certificates with provider accreditation), these certificates are activated according to the required procedures.
[2] If the token contains, in addition to the advanced certificates of the root PKI, further subject certificates (qualified certificates or qualified certificates with provider accreditation), the status can be requested via CRLs and OCSP once the CSP has received confirmation of receipt.

4.5.2 Use of the public key and of the certificate by relying parties

The certificates of the D-TRUST Root PKI can be used by all relying parties. **They can, however, only be relied upon if:**

- the certificates are used in line with the types of use shown there (key use, extended key use, restricting extensions, if applicable),
- verification of the certificate chain can be carried out successfully right through to a trusted root certificate,
- the check of the status of the certificates via the status request service (OCSP) had a positive outcome, and
- all other precautionary measures determined in agreements or otherwise were taken and if restrictions, if any, in the certificate as well as any application-specific measures were taken by the subscriber and found to be compatible.

Note: Unlike qualified signatures, the burden of proof is reversed in courts of law for non-qualified signatures are, i.e. their validity must be proven by a corresponding expert opinion. The high level of security and quality with Class 3 and Class 2 favours the starting conditions for drawing up the expert report.

4.6 Certificate renewal

Certificate renewal is the re-issuance of a certificate that is based on the content data and keys of the original certificate and which has a different period of validity. When applying for renewal of a certificate, all of the fields can essentially be changed. The necessary proof/documents must be submitted. The CP and CPS in effect at the time of renewal apply to the renewed certificates.

Certificate renewal is generally not performed for CA keys.

Renewal of LCP certificates is subject to agreement with customers on a case-to-case basis.

4.6.1 Conditions for certificate renewal

In contrast to a new application for a certificate, the initial identification process can be omitted for certificate renewal requests.

The certificate to be renewed must still be valid at the time the electronic application for certificate renewal is submitted. When submitted in writing, the application can also be made after the certificate validity has expired.

Class 3, Class 2
This is, however, conditional upon the certificate being issued for the same subject.

Class 2
A reloading procedure can be implemented on the basis of an agreement to this effect. The application is then submitted by authorised representatives and the subscriber in person agrees to the new certificate to be reloaded into his or her card as well as new terms of use, if any, by entering the PIN as part of the reloading process.

Class 3, Class 2 and Class 1
If new certificate contents are to be added, they must be verified on a class-specific basis according to sections 3.2.2 and 3.2.3. The subscriber must confirm that no certificate contents other than those stated have changed.

If in the first application or in a previous follow-up application affiliation with an organisation was only simply confirmed and not revocably confirmed, affiliation with the organisation must be proven once again. This is carried out in analogy to the procedures described in section 3.2.3. If the affiliation with an organisation was revoked, affiliation must be proven again, if applicable. Otherwise the organisation is then no longer entered in the certificate.

In the event that any material changes in the terms of use have come into effect, the subscriber will be informed thereof. The subscriber must confirm the new terms.

The keys to be re-certified and the cryptographic algorithm must fulfil the minimum requirements of the CP in effect at the time the application is submitted (see sections 3.2.1, 6.1.1 of the CPS and 6.1.5 of the CPS) and may not be compromised.

4.6.2 Authorisation for certificate renewal

Each subscriber who is authorised (pursuant to section 4.1.1) to submit a new certificate application can apply for certificate renewal if the conditions pursuant to section 4.6.1 are fulfilled and if the TSP offers a corresponding procedure for the chosen product.

4.6.3 Processing an application for certificate renewal

Subscribers who are authorised to apply for certificate renewal use an online interface of the TSP which is made available on a product-specific basis for submitting applications.

Class 3, Class 2
A person with a corresponding role commissioned by the TSP checks whether the applicant is authorised and the signature according to the procedural

instructions. Following extensive examination, the person examining the application decides on the basis of their findings whether the application is to be rejected or processed further. If the application is to be passed on for further processing, the role in question issues new certificates. Examination and issuance can be partially or fully automated while observing all stages of checking.

Class 1
Applications are checked in a process that is partially automated and partially manual, and are either rejected or processed further.

4.6.4 Notification of the subscriber concerning the issuance of a new certificate

The rules laid down in section 4.3.2 apply.

4.6.5 Procedure in conjunction with the issuance of a certificate renewal

In the case of certificate renewal, the key pair is already available to the subscriber. Just like the method used for qualified signature cards, the certificate generated is either written onto the smart card via a secure data connection or made available via an online service. The rules laid down in section 4.4.1 are also applicable.

PINs are not changed when certificates are renewed.

4.6.6 Publication of the certificate renewal by the TSP

The rules laid down in section 4.4.2 are applicable, depending on the details of the initial application. The subscriber can change his or her decision regarding publication.

4.6.7 Notification of other PKI entities concerning the renewal of the certificate

The rules laid down in section 4.4.3 apply.

4.7 Certificate renewal with key renewal

Key renewal is the new issuance of a certificate which is based on the content data of the original certificate, but for which new keys are used and which has a different period of validity. When applying for key renewal, all of the fields can essentially be changed. The necessary proof/documents must be submitted. Personal certificates without a pseudonym are one exception. In this case, the CN field of the DistinguishedName must remain unchanged, see section 3.1.1. The CP in effect at the time of renewal applies to the renewed certificates. Key renewals are offered for Class 3 and Class 2 only. Irrespective of their class, CA keys can be renewed if they have not been revoked. In the case of SSL certificates, no certificate renewal with key renewal is offered.

Class 3 EV certificates
Certificate renewal with key renewal is not offered for EV certificates. Class 3 EV certificates are subject to the requirements of section 8.3 and 10.13 [GL-BRO].

4.7.1 Conditions for certificates with key renewal

In contrast to a new application for certificates, the initial identification process can be omitted for key renewal requests. This is, however, conditional upon the certificate being issued for the same subject.

The certificate to be renewed must still be valid at the time the electronic application for key renewal is submitted. When submitted in writing, the application can also be made after the certificate validity has expired.

Subscribers must prove in accordance with the requirements laid down in section 3.2.1 that they own the private key.

If certificate contents are to be changed, they must be verified on a class-specific basis according to sections 3.2.2 and 3.2.3. The subscriber must confirm that no certificate contents other than those stated have changed. If in the first application or in a previous follow-up application affiliation with an organisation was only simply confirmed and not revocably confirmed, affiliation with the organisation must be proven once again. This is carried out in analogy to the procedures described in section 3.2.3. If the affiliation with an organisation was revoked, affiliation must be proven again, if applicable. Otherwise the organisation is then no longer entered in the certificate.

In the event that any material changes in the terms of use have come into effect, the subscriber will be informed thereof. The subscriber must confirm the new terms.

If certificates are issued for an existing key pair, ownership of the private keys must be proven in accordance with section 3.2.1. The key material and the cryptographic algorithm must fulfil the minimum requirements of the CP in effect at the time the application is submitted (see sections 3.2.1, 6.1.1 and 6.1.5) and may not be compromised.

4.7.2 Authorisation for key renewal

Each subscriber who is authorised (pursuant to section 4.1.1) to submit a new certificate application can apply for key renewal for his certificates if the conditions pursuant to section 4.7.1 are fulfilled and if the TSP offers a corresponding procedure for the chosen product.

4.7.3 Processing of certificate applications for key renewals

Subscribers who are authorised to apply for certificate renewals use an online interface of the TSP which is made available on a product-specific basis for submitting applications.

Class 3, Class 2

A person with a corresponding role commissioned by the TSP checks whether the applicant is authorised and the signature according to the procedural instructions. Following extensive examination, the person examining the application decides on the basis of their findings whether the application is to be rejected or processed further. If the application is to be passed on for further processing, the role in question issues new certificates. Examination and issuance can be partially or fully automated while observing all stages of checking.

Class 1

Applications are checked in a process that is partially automated and partially manual, and are either rejected or processed further.

4.7.4 Notification of the subscriber concerning the issuance of a successor certificate

The rules laid down in section 4.3.2 apply.

4.7.5 Procedure for the issuance of certificates following key renewals

The rules laid down in section 4.4.1 apply.

4.7.6 Publication of certificates following key renewals by the TSP

The rules laid down in section 4.4.2 apply. The subscriber can change his or her decision regarding publication.

4.7.7 Notification of other PKI entities concerning the issuance of a successor certificate

The rules laid down in section 4.4.3 apply.

4.8 Certificate change

Certificate changes are not offered.

4.9 Revocation and suspension of certificates

4.9.1 Conditions for revocation

The revocation of a certificate is one of the contractually agreed duties of the TSP in relation to the subscriber or a third party concerned when requested. The procedures of the TSP fulfil the requirements from [ETSI-F] and [GL-BRO].

Subscribers or third parties concerned are called upon to request revocation if they suspect that private keys were compromised or that any content data of the certificate is no longer correct (for instance, termination of the subscriber's affiliation with an organisation).

A certificate is revoked in the following cases:

- when requested by the subscriber and/or the third party concerned (for instance, the organisation named in the certificate),
- if information in the certificate is invalid,
- if the TSP discontinues its activities and if such activities are not continued by another TSP,
- in the case of code-signing certificates only:
  - when it comes to the TSP's knowledge that the certificate was issued to a manufacturer of malware, or
  - when it comes to the TSP's knowledge that the certificate, if not revoked, would damage the trust status.

Notwithstanding the foregoing, the TSP can cause revocation if:

- the private key of the issuing or of a higher-level CA was compromised,
- the key pair is on a signature card which also contains a key pair belonging to a qualified certificate which is to be revoked,
- weaknesses are detected in the encryption algorithm used which constitute serious risks for the permitted applications during the certification lifecycle,
- the hardware and software used show security shortcomings which constitute serious risks for the permitted applications during the certification lifecycle,
- unambiguous assignment of the key pair to the subscriber is no longer ensured,
- a certificate was obtained on the basis of false data,
- the customer is in default with payment after two reminders,
- the contract was terminated or expired in any other manner.

Class 3 EV certificates

[GL-BRO] foresees mandatory reasons for the revocation of EV certificates (Appendix A).

The TSP operates an EV reporting unit according to section 11.3 [GL-BRO] to which PKI entities or software manufacturers can send, on a 24/7 basis, complaints, voice suspicion regarding cases of compromising of private keys of EV certificates, report cases of misuse of EV certificates as well as cases of fraud and conduct in violation of the rules for EV certificates.
Within 24 hours, the TSP begins addressing the events reported according to section 11.3.2 [GL-BRO] which can lead to revocation of the EV certificates concerned.
Suspected misuse of D-Trust EV certificates can be reported to the following e-mail address:
ev-support@d-trust.net.

Any revocation is marked with the time of revocation. Retroactive revocation is not possible. Furthermore, revocation cannot be reversed.

Parties authorised to request revocation must identify themselves according to section 3.4.

4.9.2 Authorisation for revocation

The TSP is authorised to revoke certificates. The TSP is obliged to revoke a certificate according to [GL-BRO] section 11.2.2 and/or section 11.3.3.

Subscribers are always authorised to have their certificates revoked. Agreements can be made with subscribers pursuant to which they waive this right.

In the event that a certificate contains information regarding the subscriber's power to represent a third party, such third party is also authorised to request revocation of the certificate concerned. The body (for instance, a professional chamber) responsible for other information regarding an individual (such as the information "tax advisor") can also request revocation of the certificate concerned when the basis for such information about the individual ceases to exist following its inclusion in the certificate. Additional third parties authorised to request revocation can be specified and will then always be authorised to request revocation of these certificates.

Otherwise any individual will be deemed to be authorised to request revocation from the TSP if such individual mentions the correct revocation password.

4.9.3 Revocation request procedure

A revocation request can be generally submitted by post. If a revocation password was agreed to, revocation requests can be submitted by e-mail or telephone during nation-wide working days in Germany between 9am and 5pm.

Revocation number:	+49 (0)30 / 25 93 91 - 602
E-mail address:	sperren@d-trust.net
Address for written revocation requests:	D-TRUST GMBH Kommandantenstr. 15 10969 Berlin

Class 3 EV certificates

Parties authorised to request revocation can do so on a 24/7 basis after authentication using their agreed revocation password.

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

Other revocation methods can be agreed to.

Certificate revocation requests submitted by e-mail must contain an unambiguous description of the certificate to be revoked and should hence include the following details:

- Name of the party requesting revocation,
- Subscriber's name,
- Serial number of the certificate (in decimal format, if possible) in order to enable unambiguous identification of the certificate.

Revocation is carried out in the TSP's sphere of responsibility. Notwithstanding this, the TSP can subcontract part of its tasks. The revocation service can be performed by third parties acting on the basis of the requirements of the TSP. The TSP provides suitable software and hardware as well as operating instructions and procedures.

The operating instructions and procedures set forth strict rules for performing the revocation service and include a detailed description of processes, workflows and rules for problem handling.

The reasons for revocation given by the party requesting revocation are documented. Following revocation, the subscriber and/or subject will be informed about the revocation.

Authentication of persons authorised to revoke certificates is carried out according to section 3.4.

4.9.4 Revocation request deadlines

The subject or subscriber is solely responsible for ensuring that they or a person authorised to request revocation on their behalf immediately request revocation

as soon as reasons for revocation become known. The procedure which promises fastest processing of the revocation request must be used.

4.9.5 Time span for the processing of a revocation request by the TSP

The TSP processes revocation requests on nation-wide German working days between 9am and 5pm. Revocation requested by telephone is carried out immediately. Revocation requests received by e-mail and letter are processed the next working day at the latest.

Class 3 EV certificates
Revocation is carried out following successful authorisation of the party requesting revocation by telephone.

Class 2 LCP
Revocation requests are carried out within 72 hours.

4.9.6 Methods available for checking revocation information

Up-to-date revocation information is maintained in certificate revocation lists which can be retrieved via the LDAP protocol or the link shown in section 2.1. An OCSP service is additionally available. The availability of these services is indicated in the form of URLs in the certificates. Furthermore, revocation information is also available from the TSP's website (see section 2.1). Delta-CRLs are not used.

The integrity and authenticity of the revocation information are ensured by a signature of the CRL and/or the OCSP response.

Revocation entries in certificate revocation lists will remain there at least until the expiration of the certificate's term of validity.

4.9.7 Publication frequency of certificate revocation lists

See section 2.3.

4.9.8 Maximum latency time for certificate revocation lists

Certificate revocation lists are published immediately following their generation.

4.9.9 Online availability of revocation information

An OCSP service is available for online verification. The availability of this service is indicated in the form of a URL in the certificates.

4.9.10 Need for online verification of revocation information

There is no obligation for an online verification of revocation information; however, section 4.5.2 applies.

4.9.11 Other forms for notification of revocation information

None.

4.9.12 Special requirements in the case of compromising of the private key

None.

4.9.13 Conditions for suspension

Certificate suspension is not offered.

4.10 Status request service for certificates

4.10.1 Operation of the status request service

The status query service is available via the OCSP protocol. The availability of the service is indicated as a URL in the certificates.

The formats and protocols of the services are described in sections 7.2 and 7.3.

4.10.2 Availability of the status request service

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

4.10.3 Optional services

None.

4.11 Withdrawal from the certification service

The validity of the certificate ends on the date shown in the certificate. Key renewal can be applied for according to section 3.3.1. The request to revoke a certificate by a subscriber or party authorised to request revocation leads to revocation by the TSP. The TSP's main contractual duties are thereby completely fulfilled.

4.12 Key depositing and key restoration

Apart from the exceptions listed below, a request can be submitted to deposit private EE keys.

Class 3, Class 2, Class 2 LCP
Signature keys of EE certificates are not deposited.

Class 3 EV certificates
Keys for Class 3 EV certificates are not deposited.

4.12.1 Conditions and procedures for depositing and restoring private keys

The subscriber must apply for the key(s) to be deposited and state that the private EE key is to be re-used to create certificates for the same subscriber, subject or a certain group of individuals.

If EE keys according to 6.2.3 are to be re-used, the subscriber must prove that he is authorised to re-use these keys.

4.12.2 Conditions and procedures for depositing and restoring session keys

Session keys are not offered.

5. Non-technical security measures

The descriptions contained in this section refer to Class 3 and Class 2 CAs which are operated at D-TRUST GMBH.

5.1 Structural security measures

D-TRUST GMBH is an accredited certification service provider pursuant to the German Act on Digital Signature. Detailed documentation is available for structural security measures (security concept of the certification service provider in conformity with the German Act on Digital Signature [SiKo-DTR]) the relevant parts of which can be made available for inspection to applicants proving a relevant interest in such disclosure. The security concept was audited by TÜV Informationstechnik GmbH as the audit and certification body accredited by the Federal Network Agency. The audit and accreditation are repeated following any security-relevant modifications and at regular intervals.

The security concept includes a detailed documentation of structural security and surveillance measures the relevant parts of which are open for inspection from case to case and to applicants proving a relevant interest in such disclosure.

Furthermore, TÜV-IT has certified that the security area of the trust service provider of D-TRUST GMBH applies and implements the "Infrastructure measures for high protection requirements – level 3" ["Infrastrukturmaßnahmen für hohen Schutzbedarf – Level 3"] (TUVIT-TSI66184.13 dated 22 March 2013) (according to the catalogue of audit criteria for "Trusted Site Infrastructure"). This TÜV-IT certificate for a "Trusted Site Infrastructure" audits and evaluates all infrastructure-relevant aspects. This audit is repeated every two years. The above-mentioned certificates confirm that D-TRUST GMBH fulfils this demanding security standard for its non-technical security measures.

The CAs of the root PKI which is the subject matter of this document are operated under the same conditions as the CAs of D-TRUST GMBH for the issuance of qualified certificates with provider accreditation pursuant to the German Act on Digital Signature.

5.2 Procedural rules

5.2.1 Role concept

The security concept includes a role concept [Siko-DTR] where employees are assigned to one or more roles and receive the corresponding authorisations in a managed process. The authorisations of the individual roles are limited to those authorisations which these roles need to fulfil their tasks. The assignment of authorisations is revised by security management on a regular basis, and authorisations are cancelled immediately when no longer needed.

Employees working in the area of certification and revocation services act independent and are free from commercial/financial constraints that could influence their decisions and acts. The organisation structure of the TSP considers and supports employees in the independence of their decisions.

The identity, reliability and professional qualifications of employees are verified prior to commencing their work. Regular and demand-driven training ensures competency in the respective fields of activity as well as general information security. Training and proficiency check results are documented. The TSP hence fulfils the requirements of section 12.1 [GL-BRO].

5.2.2 Four-eyes principle

The four-eyes principle is, as a minimum, required for particularly security-critical operations. This is ensured by technical and organisational measures, such as access authorisation and verification of technical knowledge.

5.2.3 Identification and authentication for individual roles

The role concept is ensured by technical and organisational measures, such as access authorisation and verification of technical knowledge. Before being allowed to access any security-critical applications, the employee concerned must have been successfully authenticated. Event logs enable the identification of employees who performed past actions; the employees are accountable for their acts.

5.2.4 Role exclusions

The role concept foresees several role exclusions in order to prevent that a single person can issue a certificate and enter this in the repository service.

5.3 Personnel employed

The TSP fulfils the requirements for employees pursuant to the [SigG] and [SigV] and describes these in the security concept [SiKo-DTR].

5.3.1 Requirements in terms of qualification, experience and reliability

The TSP ensures that persons employed in the area of the certification service have the knowledge, experience and skills necessary for this activity.

5.3.2 Security screening

The TSP fulfils the requirements pursuant to section 5 (5) of the German Act on Digital Signature [§ 5 (5) SigG] and describes these in a security concept [SiKo-DTR]. This includes, for instance, the requirement for police clearance certificates to be submitted on a regular basis.

5.3.3 Training

The TSP trains certification service personnel.

5.3.4 Frequency of training and information

The TSP trains certification service personnel at the beginning of their employment and as required.

5.3.5 Frequency and sequence of job rotation

Role changes are documented. The corresponding employees are trained. Role changes are carried out with due consideration of the security concept [SiKo-DTR] (access right, access control).

5.3.6 Measures in the case of unlawful acts

The TSP does not employ any unreliable persons in the certification service.

5.3.7 Requirements for freelance staff

Not applicable; no freelance staff are employed.

5.3.8 Documentation handed over

Comprehensive process instructions and procedures for all production steps define the relevant employee roles and rights as well as the corresponding manual and automated checks. The technical security infrastructure of D-TRUST ensures that deviations from these defined processes are not possible in the production process.

5.4 Monitoring and surveillance measures

The TSP implements comprehensive surveillance measures (for instance, video surveillance) in order to warrant the security of its certification services and the underlying IT systems and documents. These measures are described in the security concept [SiKo-DTR].

The monitoring and surveillance measures are supplemented by organisational rules. Visitor rules, for instance, require visitors to be announced and registered by their names at least 24 hours before their visit and that their ID documents be deposited during their visit. While in the area of the trust service provider's premises, visitors must at all times be accompanied by an employee of the TSP.

Another part of the security concept is a risk analysis which provides a comprehensive analysis of threats to the TSP's operation and defines requirements as well as counter-measures. The security concept also includes an

analysis of the residual risk where the appropriateness of the residual risk is identified.

5.5 Archiving of records

5.5.1 Types of records archived

A distinction is made between electronic and printed documents.

Documents archived are the complete application documents (including subsequent applications), documents concerning procedures (CP, CPS), certificates, revocation documentation, electronic files and reports/logs regarding the certificate lifecycle. Events are recorded including related time information.

5.5.2 Archiving times for data

Class 3, Class 2

Application and verification documents as well as data concerning the certificate lifecycle and the certificates themselves are filed for a period of at least five years and until the end of the year[3]. This period totals seven years for all SSL certificates, including Class 3 EV certificates. The period begins after the expiration of the term of validity of the certificate that was issued last on the basis of these documents.

5.5.3 Archive protection

The archive is located in secure rooms and is subject to the role and access concept of the TSP.

5.5.4 Archive data backup

Confidentiality and integrity of data are maintained. The documentation is set up immediately so that subsequent changes will be discovered. German data protection requirements are adhered to.

5.5.5 Request for time stamping of records

The TSP operates a time stamping service pursuant to [SigG].

5.5.6 Archiving (internally / externally)

Archiving is carried out internally at the TSP as well as externally in rooms affording equivalent protection.

[3] If the token contains, in addition to the non-qualified certificates of the root PKI, further subject certificates (qualified certificates or qualified certificates with provider accreditation), the filing periods of such certificates will then apply.

5.5.7 Procedure for obtaining and verifying archive information

The process of obtaining and verifying archive information is subject to the role concept of the TSP.

5.6 Key change at the TSP

In due time before a CA expires, new CA keys are generated, and new CA instances set up and published.

5.7 Compromising and continuation of business on the part of the TSP

5.7.1 Treatment of incidents and cases of compromising

The TSP has a contingency concept and a restart plan which are known to the roles involved and which can be implemented by these when necessary. Responsibilities are clearly distributed and are known.

5.7.2 Restoring after compromising of resources

The security concept describes the performance of recovery procedures.

5.7.3 Compromising of the private CA key

In the event of compromising or communication of uncertainty of algorithms or associated parameters by the issuers of the relevant catalogues according to section 6.1.6, the TSP initiates the following:

- The CA certificates as well as their certificates already issued and not yet expired are revoked.
- Subscribers affected are informed about the incident and its effects.
- The incident is published on the websites of the TSP including a statement that any certificates that were issued by this CA are no longer valid.

The analysis of the reasons for compromising is used, if possible, to design suitable measures in order to prevent future cases of compromising. Taking the reasons for compromising into consideration, new CA signature keys are generated and new CA certificates issued.

5.7.4 Ways of continuing business following compromising and disaster

In an emergency, the TSP decides, depending on the type of incident, whether a recovery of the backup of the CA described in section 6.2.4 is to be carried out or whether the procedure described in section 5.7.3 is to be adopted in the case of compromising.

5.8 Closing the TSP down

When the services of CAs are terminated, the TSP informs all subscribers and terminates all access possibilities for the TSP's subcontractors with regard to the CAs concerned. All certificates issued by the CAs concerned which are still valid are revoked. Private CA keys which are concerned are destroyed.

The repository service and application documents are handed over to Bundesdruckerei GmbH and continued there under equivalent conditions. Continuation of the repository service until the end of the term of validity of the EE certificates is warranted and handed over either to another TSP or to Bundesdruckerei GmbH.

The TSP has a corresponding letter of comfort regarding payment of costs in conjunction with the fulfilment of these minimum requirements should the certification authority become insolvent or unable for any other reason to cover such costs itself.

On completion of operations, the functionality of the CAs will be discontinued so that certification is no longer possible.

6. Technical security measures

The descriptions contained in this section refer to Class 3 and Class 2 CAs which are operated at D-TRUST GMBH.

6.1 Generation and installation of key pairs

At this point, a distinction is made between key pairs for

- CA certificates and
- end-entity certificates (EE certificates).

6.1.1 Generation of key pairs

CA keys are generated in a "FIPS 140-2 Level 3"-compliant hardware security module (HSM). The HSM is located in the high-security area of the trust service provider. The role concept and hence the 4-eyes principle are compulsory for key generation. Whenever CA keys are generated, an independent auditor is always present and, following key generation, the auditor can use a video recording in order to verify correctness of the key generation process.

EE keys are generated in an encrypted process by the TSP or the subscriber and according to the requirements of the CP and the CPS.

Class 3, Class 2
: If EE keys and EE certificates are loaded onto smart cards (Secure User Device (SUD) according to [ETSI-F], D-TRUST GMBH uses a confirmed SSCD as the SUD), the TSP performs procurement, storage, personalisation and PIN handling in the same manner as in qualified operations, in compliance with the German Act on Digital Signature and according to the TSP's security concept. The TSP can commission third parties to generate keys and personalise smart cards when such third parties have a security concept that complies with the German Act on Digital Signature. The TSP, for its part, operates an interface that complies with the German Act on Digital Signature with these external service providers.

Class 2 LCP
: Key pairs for certificates that are produced as a soft PSE are generated in a secure environment on the basis of trusted cryptographic applications or, if keys are generated by the TSP, using an HSM. Furthermore, suitable measures are implemented in order to ensure the integrity of the information.

6.1.2 Delivery of private keys to subscribers

If the private keys are generated at the TSP, they are delivered according to section 4.4.1. The private keys are in this case stored at the TSP until they are delivered in a safe environment.

Class 2 LCP
Since the key deposit (escrow) option is not offered, the private key is deleted at the TSP after delivery to the subscriber.

6.1.3 Delivery of public keys to certificate issuers

CA key pairs are generated at the trust service provider.

The EE key pairs which are generated in the TSP's sphere of responsibility are available to the TSP. Certificate requests can be submitted by subscribers for an existing key pair in the form of a PKCS#10 request which must be signed with the corresponding private key. The PKCS#10 request contains the public key. The corresponding PKCS#10 response returns the complete certificate.

6.1.4 Delivery of public CA keys to relying parties

The public CA key is contained in the CA certificate. This certificate is normally contained in the token which is delivered to the subscriber. Furthermore, CA certificates can be obtained from the public repository (see section 2.1) where they are published after their generation.

6.1.5 Key lengths

RSA keys with a key length of at least 2048 bits are currently used for CA certificates.

RSA keys with a key length of at least 2048 bits are currently used for EE certificates.

6.1.6 Determining the key parameters and quality control

Class 3, Class 2
CA and EE certificates are issued on the basis of keys that comply with [ETSI-ALG] in its latest applicable version in as far as compatibility in the use environment is ensured.

Class 3 EV certificates
CA and EE certificates are exclusively issued on the basis of keys that comply with [ETSI-F] and [GL-BRO] in their latest applicable version.

Class 1
The TSP determines the key parameters for CA and EE certificates.

The signature and encryption algorithms are mentioned in section 7.1.3 of the CPS.

6.1.7 Key uses

Private root CA keys are exclusively used to sign CA certificates. All other private CA keys are used to sign CA certificates, EE certificates and certificate revocation lists (see section 7.1.2).

The EE keys may only be used for the types of use stated in the certificate. The types of use are defined in the *KeyUsage* and *ExtKeyUsage* fields in the certificate and may be restricted by further extensions (see section 7.1.2).

6.2 Securing the private key and requirements for cryptographic modules

6.2.1 Standards and security measures for cryptographic modules

The cryptographic modules used by the TSP work perfectly. Throughout their entire lifecycle (including delivery and storage), the modules are protected against manipulation by suitable technical and organisational measures.

The CA keys are protected by an HSM that was evaluated according to FIPS 140-2 Level 3.

The TSP operates suitable hardware-based and software-based key generators in order to warrant the quality of the EE keys. If the private EE keys are generated in the subscriber's sphere of responsibility, the subscriber must also ensure that sufficient quality of key generation is warranted.

6.2.2 Multi-person access protection for private keys (n of m)

The HSM on which the CA keys are stored is located in the secure environment of the trust service provider. A private key must be activated by two authorised persons. Following activation, the HSM can sign any number of certificates.

Access to private EE keys is only possible in the case of keys deposited (escrow) according to section 6.2.3.

6.2.3 Depositing private keys (key escrow)

Private CA keys are not deposited.

A request can be submitted to deposit private EE keys. The keys are encrypted and stored in the trust service provider's high-security area and can only be decrypted by authorised individuals. Other options for depositing keys can be agreed to individually with the customer.

Class 3, Class 2, Class 2 LCP
Signature keys of EE certificates are not deposited.

Class 3 EV certificates
Keys for Class 3 EV certificates are not deposited.

6.2.4 Backup of private keys

A backup of the private CA keys exists. A CA key backup must be carried out at the HSM by two persons authorised for this activity and takes place in the secure environment of the trust service provider. The backup system is subject to the same requirements and protection measures as the production system. Restoring private keys also requires two authorised persons. Further copies of the private CA key do not exist.

No backup is offered for private EE keys; backups are only available in the form of the key escrow option if this has been agreed to.

6.2.5 Archiving of private keys

Private CA and EE keys are not archived.

6.2.6 Transfer of private keys to or from cryptographic modules

Transfers of private CA keys to or from the HSM are limited to backup and restoring purposes. Adherence to the 4-eyes principle is compulsory. Private keys exported to/imported from another HSM are protected by encryption.

Private EE keys can be transferred from the cryptographic module if the subscriber proves that he or she is authorised according to section 4.12.1 to re-use the key and if such transfer is technically possible. The key will never leave the module in a non-encrypted form.

6.2.7 Storage of private keys in cryptographic modules

The private keys are contained in encrypted form in the HSM.

EE keys are contained in encrypted form in a database of the CA system.

6.2.8 Activation of private keys

The private CA keys can only be activated according to the 4-eyes principle, by the authorised roles and for the permitted types of use (*keyCertSign, cRLSign*).

Private EE keys are activated by entering the PIN.

6.2.9 Deactivation of private keys

The private CA keys are deactivated by disconnecting the connection between the HSM and the application.

The respective application deactivates the private EE key, at the latest when the card is removed from the card reader or the soft PSE is deactivated or deleted.

Private EE keys on smart cards are permanently deactivated when an incorrect PIN was entered several times in succession. The card can be reactivated a limited number of times by entering the PUK. Multiple signature cards do not have a PUK.

6.2.10 Destruction of private keys

The private CA keys are deleted when their term of validity expires. This is accomplished by deleting on the HSM and simultaneous deleting of the backups on data media. When the HSM is shut down, the private keys in the device are deleted.

When the card chip is destroyed or the files containing the private EE key are deleted, the private key is then also destroyed. Destruction of keys deposited with the TSP (according to section 4.12.1) can be requested.

6.2.11 Assessment of cryptographic modules

The TSP operates suitable hardware-based and software-based key generators in order to warrant the quality of the EE keys. The HSMs used are FIPS 140-2 Level 3-compliant.

6.3 Other aspects of key pair management

6.3.1 Archiving of public keys

According to the security concept, public CA and EE keys are archived in the form of the certificates generated.

6.3.2 Validity periods of certificates and key pairs

The term of validity of the CA keys and certificates is variable and shown in the certificate. The maximum possible validity period totals 30 years.

The term of validity of the EE keys and certificates is variable and shown in the certificate. The maximum possible validity period totals:

Class 3, Class 2
61 months (SSL certificates: maximum of 39 months),

Class 3 EV certificates
27 months,

Class 2 LCP
60 months

Class 1
15 years

6.4 Activation data

6.4.1 Generation and installation of activation data

The activation data of the CA keys is requested by the HSM. The PIN is assigned during the bootstrap procedure. Adherence to the 4-eyes principle is compulsory.

Subscriber: If the key pair is generated by the subscriber, the activation secret is also produced during this process and is then available to the subscriber. If the TSP generates the keys, either a transport PIN process is used or the PINs are printed as a PIN letter that is sent or handed over to the subscriber. Installation is not necessary.

6.4.2 Protection of activation data

The activation data of the CA keys is made up of two secrets with one authorised employee each knowing one of these. Only certain, designated employees can access the activation data.

Subscriber: In the case of the transport PIN method, the transport PIN shows the card integrity. In other methods, the PINs are printed once in a specially protected PIN letter and sent to or handed over to the subscriber.

6.4.3 Other aspects of activation data

In addition to the PIN, subscribers with a signature card are also offered on a product-specific basis a Personal Unblocking Key (PUK) number to unblock the signature card (after entering an incorrect PIN three times). Multiple signature cards do not have a PUK.

6.5 Security measures in the computer systems

6.5.1 Specific technical security requirements for the computer systems

The computers, networks and other components used by the TSP ensure in their given configuration that only those actions can be carried out which are not in conflict with the CP and [ETSI-F] and, in the case of Class 3 EV certificates, with [GL-BRO].

The TSP's computer security for exposed systems is ensured, amongst other things, by multi-level security systems providing perimetric virus protection, end-point protection and integrity-protecting tools.

Subscribers and certificate users must use trusted computers and software.

6.5.2 Assessment of computer security

The computers, networks and other components used for the CA keys are checked, inspected and audited by recognised inspection and certification bodies.

6.6 Technical measures during the lifecycle

6.6.1 Security measures during development

During the course of all system development projects carried out by or on behalf of the TSP, security requirements are analysed already during the draft design phase. The results are defined as requirements for development.

6.6.2 Security measures in conjunction with computer management

Administration of computers, networks and other components is strictly limited to personnel authorised according to the role concept (of the security concept of D-TRUST GMBH as the TSP in conformity with the German Act on Digital Signature). Log files are regularly analysed with a view to rule violations, attempted attacks and other incidents. Monitoring and surveillance measures begin when a device is set into operation and end when it is disposed of.

6.6.3 Security measures during the lifecycle

Any devices used are operated in accordance with their manufacturers' instructions. Prior to being set into operation, they are meticulously checked and inspected. They are only set into operation if it is clear beyond any doubt that they were not manipulated. Sealing of hardware and software checks is, for instance, used in order to be able to detect manipulation and attempted manipulation during any activity or inspection. In the case of suspected manipulation of a component, any action planned will not be carried out and the incident is reported to the TSP manager. In order to enable immediate and co-ordinated response to any security-relevant incidents, the TSP defines clear-cut escalation rules for the individual roles.

Capacity requirements and utilisation as well as the suitability of the systems involved are monitored and adapted as required. Devices exchanged or obsolete data media are taken out of service and disposed of in such a manner that any misuse of functionalities or data is ruled out. Changes in systems, software or processes are subject to a change management process. Security-critical

changes are checked by the security officer. After the expiration of the term of validity of CAs, the private keys are destroyed.

Electronic data or printed reports are used to document all relevant events which influence the lifecycle of the CA, of the certificates issued and of the keys generated, and such electronic data or printed reports are stored on long-lived media in an auditable form. The company's media are safely protected against damage, theft, loss or compromising depending on their respective classification within the scope of the TSP's documentation guideline.

Class 3 EV
The events specified in section 13.1 [GL-BRO] are, as a minimum, logged in an auditable form.

6.7 Security measures for networks

A network concept is implemented during operation of the CAs. Detailed documentation is available for the network concept (security concept of the CSP, D-TRUST GMBH, in conformity with the German Act on Digital Signature, network concept [SiKo-DTR]) the relevant parts of which can be made available for inspection to applicants proving a relevant interest in such disclosure.

In order to protect the processes of the TSP, firewalls and intrusion detection/prevention mechanisms are used, for example. The TSP operates network segments with different protection requirements and separates networks for employees and Internet uses on the one hand from server networks on the other. The systems are subject to regular inspection and revision, the employees in charge are accountable. Anomalies are reported by technical systems and organisational processes and addressed by a defined incident handling procedure as well as related processes.

Cryptographic mechanisms are used to protect data traffic with a high protection demand outside the networks protected by the TSP for which integrity or confidentiality must be ensured.

The physical security of the networks operated and used by the TSP is ensured and adapted to the structural conditions and any changes therein.

The security concept was audited by TÜV Informationstechnik GmbH as the audit and certification body accredited by the Federal Network Agency.

6.8 Time stamp

The TSP operates a time stamping service pursuant to [SigG]. However, time stamps are not offered within the scope of this CPS.

7. Profiles of certificates, revocation lists and OCSP

7.1 Certificate profiles

7.1.1 Version numbers

Certificates are issued in the X.509v3 format.

7.1.2 Certificate extensions

The selection of the extension is primarily product-dependent.

CA certificates contain the following *critical* extensions ("mandatory field"):

Expansion	OID	Parameter
KeyUsage	2.5.29.15	*keyCertSign, cRLSign*
BasicConstraints	2.5.29.19	*Ca=TRUE, (pathLenConstraint)*

CA certificates can include the following *non-critical* extensions ("optional"):

Expansion	OID	Parameter
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 hash of the issuer key
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 hash of the subject public key
CRLDistributionPoints	2.5.29.31	Address of the CRL issuing authority
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	*accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation*
certificatePolicies	2.5.29.32	OID of the CPs to be supported
SubjectAltName	2.5.29.17	Alternative issuer name

Further extensions can be added; they must comply with [X.509], [RFC 5280] and [ETSI-ALG] or they must be described in a referenced document.

EE certificates contain the following *critical* extensions:

Expansion	OID	Parameter
KeyUsage	2.5.29.15	Possible are: *digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, decipherOnly* and combinations thereof

EE certificates can include the following non-critical extensions:

Expansion	OID	Parameter
ExtKeyUsage	2.5.29.37	Corresponding to [RFC 5280]
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 hash of the issuer key
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 hash of the subject public key
CRLDistributionPoints	2.5.29.31	CRL issuing authority as ldap address
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	*accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation* *accessMethod= Certification Authority Issuer {1.3.6.1.5.5.7.48.2}, accessLocation*
certificatePolicies	2.5.29.32	OID of the CPs to be supported *cpsURI*
SubjectAltName	2.5.29.17	Alternative issuer name

Further extensions can be added; they must comply with [X.509], [RFC 5280] and [ETSI-ALG] or they must be described in a referenced document.

7.1.3 Algorithm OIDs

The following encryption algorithm is currently used in the CA and EE certificates:

- RSA with OID 1.2.840.113549.1.1.1.

The following signature algorithms are currently used in CA and EE certificates:

- SHA256 RSA with OID 1.2.840.113549.1.1.11,
- SHA1 RSA with OID 1.2.840.113549.1.1.5.

SHA1 is not used if the CA or EE certificate is subject to certification (e.g. ETSI TS 102 042) or the German Act on Digital Signature.

7.1.4 Name formats

In the subject (here: name of the subject) and issuer (name of the issuer) fields, names are assigned according to [X.501] as DistinguishedName. The attributes described in section 3.1.4 can be assigned. Coding is carried out as UTF8 string or PrintableString for the C (Country) attribute.

The *SubjectAltName* (alternative subject name) and *Issuer-AltName* (alternative issuer name) fields can contain names according to [RFC 5280] (coded as IA5String).

7.1.5 Name constraints

"NameConstraints" is not used.

7.1.6 Certificate Policy Object Identifier

"CertificatePolicies" can contain the OID of CPs supported.

Class 3
: Class 3 certificates can contain the OID of the NCP, NCP+ and/or OVCP defined in [ETSI-F]. Further CPs can be referenced irrespective of this. This CPS fulfils the requirements from [ETSI-F].

Class 3 EV
: Class 3 EV certificates can contain the OID of the EVCP defined in [ETSI-F]. Further CPs can be referenced irrespective of this.

7.1.7 Use of the "PolicyConstraints" extension

"PolicyConstraints" is not used.

7.1.8 Syntax and semantics of "PolicyQualifiers"

"PolicyQualifiers" can be used.

7.1.9 Processing the semantics of the critical CertificatePolicies extension

In CA and EE certificates, the *CertificatePolicies* extension is not critical. Subscribers and relying parties are free to decide whether this extension is evaluated.

7.2 Certificate revocation list profiles

7.2.1 Version number(s)

Certificate revocation lists v2 according to [RFC 5280] are generated. Delta-CRLs are not foreseen.

7.2.2 Extensions of certificate revocation lists and certificate revocation list entries

Certificate revocation lists can contain the following uncritical extensions:

Expansion	OID	Parameter
cRLNumber	2.5.29.20	Number of the certificate revocation list
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 hash of the issuer key

7.3 Profiles of the status request service (OCSP)

7.3.1 Version number(s)

OCSP v1 according to [RFC 2560] is used.

7.3.2 OCSP extensions

The OCSP responder supports the extension shown below for queries:

Expansion	Parameter
RetrieveIfAllowed	If set, the certificate is delivered in the response (optional).

The OCSP responder uses the extensions shown below in the responses:

Expansion	**Parameter**
ArchiveCutoff	Period of time for which the OCSP responder makes the status information available after issuance of the certificate.
CertHash	In the case of the good or revoked status, the SHA-1 hash value of the certificate is entered.
CertInDirSince	Time of publication of the certificate in the central repository service.
RequestedCertificate	Contains the certificate if *RetrieveIfAllowed* was set.

All extensions are non-critical. Further non-critical extensions can be contained.

8. Checks and other evaluations

The CAs of the D-TRUST Root PKI 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. Revisions, revision objects and processes are described in detail in the security concept of D-TRUST GmbH [SiKo-DTR] as a certification service provider pursuant to the German Act on Digital Signature. The "role concept" section of the same security concept [SiKo-DTR] documents the qualification and position of the internal auditor.

The security concept is audited by an independent audit and certification body on a regular basis. Relevant parts of these documents can be inspected against proof of a legitimate interest.

Class 3, Class 2

Areas which, due to legal or technical differences, are not mapped analogous to qualified operation with provider accreditation (for instance, operation of a provider-internal root certificate) are audited by the internal audit department on a regular basis and in any case at least once a year.

CP and CPS fulfil for Class 3 certificates the requirements of NCP, NCP+ and/or OVCP and for Class 3 EV certificates the requirements of EVCP according to [ETSI-F] including the requirements from [BRG] and [NetSec-CAB]. Regular assessment by a qualified and competent independent party pursuant to TS 102 042 [ETSI-F], section 5.4.1 is proof of compatibility.

Class 3

The TSP issues certificates with the policy OID reference to [ETSI-F] only after initial and successfully completed auditing according to [ETSI-F] by an independent external and licensed certification body. Regular follow-up audits are conducted. When procedures and processes are found to be no longer in conformity with the current guidelines of [ETSI-F], the TSP discontinues the issuance of the above-mentioned certificates until conformity with the guidelines is restored and has been audited accordingly.

Class 3 EV certificates

The TSP only issues EV certificates if certification has taken place according to [ETSI-F] EVCP. When procedures and processes are found to be no longer in conformity with the current guidelines of [GL-BRO], the TSP discontinues the issuance of the above-mentioned certificates until conformity with the guidelines is restored and has been audited accordingly. This audit takes place annually.

Regular internal audits are additionally carried out.

9. Other financial and legal provisions

With regard to the corresponding provisions, see section 9 in the CP as well as additionally the General Terms and Conditions [AGB].

Appendix A Reasons for revocation of Class 3 EV certificates

Extract from the currently valid Guidelines for Extended Validation Certificates, CA/Browser Forum.

11.2 [GL-BRO] Revocation Events *The CA MUST revoke an EV Certificate it has issued upon the occurrence of any of the following events:*

The Subscriber requests revocation of its EV Certificate;

The Subscriber indicates that the original EV Certificate Request was not authorized and does not retroactively grant authorization;

The CA obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the EV Certificate) has been compromised, or that the EV Certificate has otherwise been misused;

The CA receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;

The CA receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the EV Certificate, or that the Subscriber has failed to renew its domain name;

The CA receives notice or otherwise becomes aware of a material change in the information contained in the EV Certificate;

A determination, in the CA's sole discretion, that the EV Certificate was not issued in accordance with the terms and conditions of these Guidelines or the CA's EV Policies;

The CA determines that any of the information appearing in the EV Certificate is not accurate.

The CA ceases operations for any reason and has not arranged for another EV CA to provide revocation support for the EV Certificate;

The CA's right to issue EV Certificates under these Guidelines expires or is revoked or terminated, unless the CA makes arrangements to continue maintaining the CRL/OCSP Repository;

The Private Key of the CA's Root Certificate used for issuing that EV Certificate is suspected to have been compromised;

Such additional revocation events as the CA publishes in its EV Policies; or

The CA receives notice or otherwise becomes aware that a Subscriber has been added

as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of the CA's jurisdiction of operation as described in Section 23 of these Guidelines.