D-TRUST-Root PKI
Certification Practice Statement

Version 1.9_EN

A word of caution:

It is always the German original, not the English translation which is authoritative.

Publication date	30.10.2013
Effective date	30.10.2013

D-TRUST EINE MARKE DER BUNDESDRUCKEREI

Copyright statement

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

Document History

Version	Date	Description
1.0	18.06.2008	Initiale Version
1.1	01.11.2008	- Änderung der Bedingungen zur Berechtigung zur Antragstellung bezüglich der Volljährigkeit - Anpassung der Prüfverfahren für SSL-Zertifikate mit *dNSNames* - Generalisierung OCSP-Pfad - Anpassung Prüfverfahren von Class-1-Zertifikaten - Anpassungen für SSL-Zertifikate
1.1_EN	17.11.2008	Translation into English
1.2_EN	01.06.2009	- revocation reasons of code-signing certificates extended - Editorial changes - Changes due to the WebTrust audit
1.3_EN	25.02.2010	Adjustment of SSL-Certificates and renewal procedures
1.4_EN	21.09.2010	Update aufgrund neuer Version [ETSI-F] und [GL-BRO]
1.5_EN	02.02.2011	Non Top-Level Domains removed
1.6_EN	14.09.2011	maximum validity for SSL-certificates defined as 39 month
1.7_EN	26.07.2012	validity period of Class 2 extended
1.8_EN	07.02.2013	- ascertainment of liability and Claim for damages - Adjustment to [ETSI-F] incl. Baseline Requirements [BRG] and Network and Certificate Systems Security Requirements [NetSec-CAB]
1.9_EN	30.10.2013	Adjustion of definitions regarding subject and subscriber. Introduction of LCP Policy and relating procedures. Redundancies related to the CP have been eliminated using links between this document and the CP. Addition of technical and organizational means according to [ETSI-F] - Chapter 7.4.5: operations management - Chapter 7.4.6: system access management

Table of contents

1 Introduction

1.1 Overview

This document is the Certification Practice Statement (CPS) to the D-TRUST Root PKI, which is operated and maintained by the D-Trust GmbH.

1.1.1 Certification Service Provider

These provisions are specified in the Certificate Policy [CP].

1.1.2 About this document

This CPS defines the possible activities and procedures within the framework of the Certification Services throughout the validity of the CA-certificates and End-Entity-certificates (EE-certificates), as well as the minimum requirements that need to be met by all PKI-participants.

CA- as well as EE-certificates may reference Certificate Policies (CPs) that define more detailed requirements and limitations.

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

This CPS explains and extends means in the [CP]. Identical phrases are explicit refered to the related chapter.

1.1.3 PKI traits

These provisions are specified in the Certificate Policy [CP].

1.2 Document name and identification

Document name:	D-TRUST_Root_PKI_CPS_v1.9_engl.doc
Version	1.9_EN

1.3 PKI-participants

1.3.1 Certification Authority (CA)

These provisions are specified in the Certificate Policy [CP].

1.3.2 Registration Authorities (RA)

These provisions are specified in the Certificate Policy [CP].

1.3.3 Subscriber

These provisions are specified in the Certificate Policy [CP].

1.3.4 Relying parties (RP)

These provisions are specified in the Certificate Policy [CP].

1.4 Certificate Usage

1.4.1 Valid usage of certificates

These provisions are specified in the Certificate Policy [CP].

1.4.2 Invalid usage of certificates

These provisions are specified in the Certificate Policy [CP].

1.5 CP/CPS maintenance

1.5.1 Document Administrator

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

1.5.2 Contact Address

These provisions are specified in the Certificate Policy [CP].

1.6 Definition of terms, Abbreviations and Acronyms

1.6.1 Terms and names

These provisions are specified in the Certificate Policy [CP].

1.6.2 Abbreviations

These provisions are specified in the Certificate Policy [CP].

1.6.3 References

These provisions are specified in the Certificate Policy [CP].

2 Responsibility for Directories and Publications

2.1 Directories

These provisions are specified in the Certificate Policy [CP].

2.2 Publication of Certificate Information

These provisions are specified in the Certificate Policy [CP].

2.3 Publication Frequency

These provisions are specified in the Certificate Policy [CP].

2.4 Directory Access Control

These provisions are specified in the Certificate Policy [CP].

3 Identification and Authentication

3.1 Naming Conventions

3.1.1 Types of Names

These provisions are specified in the Certificate Policy [CP].

3.1.2 Necessity for Unambiguous Names

These provisions are specified in the Certificate Policy [CP].

3.1.3 Subscriber Anonymity or Subscriber Pseudonyms

These provisions are specified in the Certificate Policy [CP].

3.1.4 Rules for the Interpretation of Different Naming Combinations

EU-certificate's *DistinguishedNames* (DN-components) are interpreted as follows:

DN-component	Interpretation
G	*First name(s)* of the individual named - in the identifying document (Class 2-3) - by the applicant (Class 1)
SN	*surname* of the individual named - in the identifying document (Class 2-3) - by the applicant (Class 1) If pseudonyms are assigned, SN equals CN.

DN-component	Interpretation
CN	*Common name:* The following combinations are used: - Individual without a pseudonym: „Surname, first name“. - Individual with a pseudonym: „Pseudonym:PN” - Legal entities: official name of the organization (company, agency, association etc.), or, where necessary, a sensible abbreviation in case of an exceedance of the 64-character limitation. Special case: One or multiple domain names may be included in the CN. Wildcards are not permitted for EV-certificates. - Function or a group of individuals: name of the function or group of individuals, prefixed with the abbreviation „GRP:“, indicating a group-certificate. - Technical components: Server name or name of the application or service utilizing the certificate.
PN	*Pseudonym*: identical to CN.
serialNumber	*Serial number*: name appendage to ensure a name’s uniqueness (usually the application number). Special case: Class 3 EV-certificates according to [GL-BRO]: company registration number if such has been assigned, founding- or registry date or a description depicting the nature of the organization as a public corporation.
DNQ	*DN-Qualifier: Serialnumber of certificats, whose subject serialNumber is otherwise provided. Ensures that the DN is distinct to all other certificates (2.5.4.46-id-at-dnQualifier) according to [ETSI-F]*.
O	*Organization:* official name of the organization (company, agency, association etc.), that employs the subscriber or with which the subscriber is otherwise connected (sufficient proof of the affiliation is required), or, where necessary, a sensible abbreviation in case of an exceedance of the 64-character limitation.
OU	*Organizational unit:* (department, section or other subdivision) of the organization.
C	*Country:* according to the notations specified in [ISO 3166]. The correct country to note is determined as follows: if an organization O is listed in the DistinguishedName, the country of the organization’s seat shall be listed. If there is no organization listed in the certificate, then the issuing country of the identification-document presented by the Subscriber shall be listed.
Title	A *Title* or degree may be included.
Street	*Street:* part of the postal address
Locality	*Locality:* part of the postal address
State	*State:* part of the postal address
PostalCode	*PostalCode:* part of the postal address
BusinessCategory	Business Category (2.5.4.15) according to [GL-BRO]
Jurisdiction Of Incorporation Locality	Jurisdiction of the organization according to [GL-BRO]: *Locality* (1.3.6.1.4.1.311.60.2.1.1)

DN-component	Interpretation
Jurisdiction Of Incorporation State Or Province Name	Jurisdiction of the organization: *State* (1.3.6.1.4.1.311.60.2.1.2)
Jurisdiction Of Incorporation CountryName	Jurisdiction of the organization according to [GL-BRO]: *Country* (1.3.6.1.4.1.311.60.2.1.3)

3.1.5 Uniqueness of Names

These provisions are specified in the Certificate Policy [CP].

3.1.6 Acceptance, Authentication and Brand-Names

These provisions are specified in the Certificate Policy [CP].

3.2 Initial Identity Inspection

3.2.1 Verifying Ownership of the Private Key

These provisions are specified in the Certificate Policy [CP].

3.2.2 Authentication of Organizations

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

The different validation procedures, which are described in chapter 4.2.1, are variably applied towards the DN-components as listed in chapter 3.1.4 – and possibly towards DN-components not explicitly listed in chapter 3.1.4 –, depending on the certificate's class category.

	Class 3	Class 2	Class 2 LCP	Class 1
CN O C	Register/ Non-Register/ Domain	Register/ Non-Register/ Domain	Register/ Non-Register/ Domain	Register/ Domain
OU STREET L State PostalCode	S-affirmation/ Register/ Non-Register	A-affirmation/ Register/ Non-Register/ out-of-band-mechanisms/ Domain	A-affirmation/ Register/ Non-Register/ out-of-band-mechanisms/ Domain	without verification

	Class 3	Class 2	Class 2 LCP	Class 1
E-Mail-Address	without verification (applicant affirmation)	without verification (applicant affirmation)	without verification (applicant affirmation)	without verification (applicant affirmation)
All further attributes[1]	S-affirmation/ A-affirmation/ Dok-Ident/ out-of-band-mechanisms	A-affirmation/ Dok-Ident/ out-of-band-mechanisms	A-affirmation/ Dok-Ident/ out-of-band-mechanisms	without verification

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

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

3.2.3 Authentication of Individuals

Individuals applying for a certificate must prove their identity beyond a doubt and, if applicable, prove their entitlement for applying through an organization.

Class 2
Applicants applying for a certificate meant for another individual must provide proof for their authority to do so. The data-verification is aimed at the subscriber.

The different validation procedures, which are described in chapter 4.2.1, are variably applied towards the DN-components as listed in chapter 3.1.4 – and possibly towards DN-components not explicitly listed in chapter 3.1.4 –, depending on the class category, in which the certificate falls.

	Class 3	Class 2	Class 2 LCP	Class 1
G	Pers-Ident	HR-DB/ Dok-Ident/ S-affirmation/ A-affirmation/ Statutory corporations/ out-of-band-mechanisms	HR-DB/ Dok-Ident/ S-affirmation/ A-affirmation/ Statutory corporations/ out-of-band-mechanisms	without verification
SN				
CN				
C				
STREET				
L				
S				
PostalCode				
Title	Pers-Ident/ Dok-Ident			
O (Organizational affiliation)	S-affirmation	A-affirmation/ S-affirmation/	A-affirmation/	

[1] The [GL-BRO] **Fehler! Verweisquelle konnte nicht gefunden werden.**guidelines apply for Class 3 EV-certificates.

	Class 3	Class 2	Class 2 LCP	Class 1
OU (Organizational affiliation)		Statutory corporations/ out-of-band-mechanisms/ HR-DB	S-affirmation/ Statutory corporations/ out-of-band-mechanisms/ HR-DB	
E-Mail-Address	without verification (applicant affirmation)	Without verification (applicant affirmation)	Without verification (applicant affirmation)	E-Mail
All further attributes[2]	S-affirmation/A-affirmation/ Dok-Ident/ out-of-band-mechanisms	A-affirmation/ Dok-Ident/ out-of-band-mechanisms/ HR-DB	A-affirmation/ Dok-Ident/ out-of-band-mechanisms/ HR-DB	without verification

In applications for groups of individuals, functions or IT-processes, all applicant attributes that are listed in the above table, excepting the attributes OU, e-mail-address and those not relevant to the certificate, are verified according to the class-category of the certificate. The inclusion of group-names, function-names or IT-process names in the CN is treated along the specifications set out in the table-row "All further attributes".

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

3.2.4 Unexamined Statements concerning the Subscriber

These provisions are specified in the Certificate Policy [CP].

3.2.5 Examination of Application Entitlement

Class 3 – 2

The identity and, if applicable, the organizational affiliation of individuals is ascertained and verified or confirmed along the class-specific processes indicated in chapter 3.2.3.

In the case of organizations, their existence as well as the applicant's representational authority are verified or confirmed using the class-specific process indicated in chapter 3.2.2.

Class 1

Except for a financial inspection, the entitlement for application is not verified.

[2] The [GL-BRO] guidelines apply for Class 3 EV-certificates.

3.2.6 Criteria for Interoperability

These provisions are specified in the Certificate Policy [CP].

3.3 Identification and Authentication of Re-Keying Applications

These provisions are specified in the Certificate Policy [CP].

3.3.1 Routine Re-Keying Applications

These provisions are specified in the Certificate Policy [CP].

3.3.2 Re-keying after Revocation

These provisions are specified in the Certificate Policy [CP].

3.4 Identification and Authentication of Revocation Applications

An applicant's revocation authority is verified as follows:

Class 3-1 (Class 3, Class 2, LCP and Class 1)
If a revocation application is submitted via a *digitally signed e-mail*, the applicant must either be the certificate subscriber or the preassigned third party revocation authority for the certificate in question. The third party revocation authority's digital certificate must be on record with the CSP.
Class 3-2, LCP
If a revocation application is submitted via traditional mail and a hand-signed document, then a signature comparison must show that the revocation applicant is either the certificate subscriber or the preassigned third party revocation authority for the certificate in question.
Class 3-2, LCP
If a revocation application is submitted via the telephone or a *digitally* un*signed E-Mail*, the applicant must use the correct revocation password.
Class 1
If a revocation application is submitted via traditional mail and a hand-signed document, the revocation applicant must be the certificate subscriber.
Diverging procedures concerning the validation of revocation applications may be agreed upon with the applicant.
Revocation procedures are described in chapter 4.9.

4 Operating requirements

4.1 Certificate Application and Registration

4.1.1 Application Eligibility

These provisions are specified in the Certificate Policy [CP].

4.1.2 Registration-process and Administrative Responsibility

Class 3-2

During the registration-process the applicants are made aware of the CP, the CPS and a subscriber agreement, which they must commit to observe. The documents will be published. The formal obligation follows the [ETSI-F] regulations. The application also contains the applicant's declaration of consent stating his decision on publishing the resulting certificates. The documents are stored on paper or electronically.

Class 3 EV-Certificates

The declaration of consent is consistent with "Subscriber Agreement", section 9.3 [GL-BRO].

4.2 Processing the Certificate Application

4.2.1 Identification and Authentication

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

The CSP defines the following methods of identification and authentication:

Pers-Ident
An individual must personally identify himself to an RA, an official partner or an external provider that fulfills the requirements of the [CP] with his official ID (ID-card, passport or documents with equal standing) and be authenticated in turn. A valid ID-card or passport is deemed an acceptable identification document for individuals from the European Union or from states belonging to the Schengen-Agreement. Other documents with comparable status may be submitted instead. No copies of the identification documents are made or stored at the RA or CSP.

Dok-Ident
The pertinent contents are compared through copies (paper copies or digitalized, i.e. scanned documents or faxes) with the application data. Random samples are verified through telephone calls (compare out-of-band-mechanisms). Acceptable documents are those listed in the section Pers-Ident as well as commercial register (or comparable) excerpts no older than six months, PhD documents, documents of a postdoctoral lecture qualification, certificates of appointment, or comparable documents. Copies of the identification documents are kept either as hard-copies or in digital form.

Register
A manual or automatic comparison is made between the application data and excerpts of the commercial register. Admissible are state registers (such as registration courts, public revenue offices, professional statutory corporations or comparable) or private registers DUNS, comparable financial databases and others). A registry excerpt can only be accepted as valid, if it does not have an attribute such as "invalid" or "inactive" attached to it. Copies of the documents are kept either as hard-copies or in digital form.

Non-Register
Government institutions/public corporations affirm certificate related information with an official seal and a signature. Copies of the documents are kept either as hard-copies or in digital form.

HR-DB
The CSP stipulates an agreement with an organization, so that data complying with the [CP] is transferred. An organization's authorized employee or other responsible party transfers either an excerpt from the human-resource database, or the applications that have been filled out on the basis of the data from the human-resource database to the CSP. The applicable privacy laws need to be recognized by the transferring organization. The CSP relies upon the correctness and unambiguity of the transferred data. The same takes effect for certificate-requests transferred to the CSP. The applicant or subscriber must declare a formal recognition of the obligations as detailed in chapter 9.6.3 prior to the token hand-over. Digital or hard-copy evidence is kept concerning:

- the transferred data,
- evidence of the fact that the transferring individual is an authorized employee or the designated party for this action,
- evidence, that the data was presented by an authorized employee or a designated responsible party and
- evidence that the applicant or subscriber has acknowledged his duties as detailed in chapter 9.6.3 [CP].

S-affirmation
The organization's signatory affirms certificate-related information in writing. In isolated cases a digitally signed affirmation may be accepted by the CSP. The signatory power must be evident either from the publicly available organizational documentation or the supplied proof of existence. Otherwise it needs to be proved separately. Copies of the documents are kept either as hard-copies or in digital form.

A-affirmation
The organization's authorized employee/responsible party or a trusted third party, such as one of the CSP's contractual partners or a state institution like the chamber of industry and commerce affirm certain certificate-related information that is in their sphere of competence in writing. In isolated cases a digitally signed affirmation may be accepted by the CSP. Copies of the documents are kept either as hard-copies or in digital form.

out-of-band-mechanisms
The CSP uses out-of-band-mechanisms to verify application data. Communication paths and verification methods are chosen in such a way, that the applicant can not influence the process. The evidence is documented and copies are kept either as hard-copies or in digital form.

A possible proof of existence for an organization or an individual could be a credit card deduction, the transfer from a bank account or a directly debited bank account. The CSP trusts the bank whose customer the organization or individual is. A telephoned inquiry based on the data taken from a public telephone directory is also a permissible.

An individual may also be identified through a registered letter with a returned advice of receipt sent by the CSP. The signature on the returned advice of receipt is compared with the signature on the passport copy or the application documents.

The organizational affiliation of the applicant may also be proved through a registered letter with a return advice of receipt sent to the organization to the attention of the applicant. The signature on the returned advice of receipt is compared with the signature

on the passport copy or the application documents. Organizational affiliation, e-mail-address, contents of extensions as well as any other certificate-relevant data may also be verified through a telephoned inquiry based on the data taken from a public telephone directory.

Statutory corporations
The CSP stipulates an agreement with a statutory corporation, so that the data complying with the [CP] is transferred. An organization's authorized employee or other responsible party transfers either an excerpt from the human-resource database, or the applications that have been filled out on the basis of the data from the human-resource database to the CSP. The applicable privacy laws need to be recognized by the transferring statutory corporation. In addition, the processes further detailed in the section HR-DB apply.

Domain
An organization's domain and possibly further attributes such as e-mail addresses are verified by a domain-enquiry in the official registers (WHOIS). Class 3-2: It is questioned whether the subscriber has the exclusive control of the domain. The findings are documented. With EV certificates in addition a review of the domain name for known phishing domains of blacklists is carried out. Domains that are not subject to registration (non Top-Level Domains) are not allowed.

E-Mail
The CSP sends an e-mail to the e-mail address that needs verification. The receipt must be acknowledged (exchange of secrets). The findings are documented.

Identification and authentication are achieved by following the guidelines found in sections 3.2.2 and 3.2.3 of the [CP].

4.2.2 Approval or Declination of a Certificate Application

An authorized "second, impartial" CSP employee of the appropriate security concept defined role checks if the application is in keeping with the following criteria:

- does the documentation show if the applicant has been authenticated following the correct procedures,
- have all necessary documents of proof been presented,
- are there reasons suggesting an application should be turned down.

Possible reasons for an application declination are recorded in the [CP].

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

In case of discrepancies regarding identity and correctness of application or supporting documents, the application will be rejected except the applicant is able to explain the discrepancy in time completely. The content of received PKCS#10- or other certificate-requests is verified by the CSP. This verification will not be undertaken in the case that the CSP has entered into a contractual agreement with partners that employ impartial employees to present the production requests to the CSP. Specific certificate data (i.e. O or OU) can bei defined by contract.

In case the CSP receives certificate data via a multi-cliend-enabled online-interface, pre-verificaten of certificate data is allowed. After forwarding the full application to the CSP for verification, an immediate issuance of the certificate(s) is appropriate.

4.2.3 Time Limit for Application Processing

Not applicable.

4.3 Certificate Issuing

4.3.1 CSP Approach in Issuing Certificates

After a satisfactory validation of the application or request, the certificates are produced in the high-security TrustCenter.

The CSP makes sure that the correct time is applied while producing the certificate.

The application documents are either archived in their entirety by the CSP as detailed in chapter 5.5 or by contractual partners that will archive the application documents and/or requests securely and in their entirety for the period of time mentioned in section 5.5.2.

4.3.2 Subscriber Notification Concerning Certificate Issue

These provisions are specified in the Certificate Policy [CP].

4.4 Certificate Transfer

4.4.1 Certificate Transaction Procedures

These provisions are specified in the Certificate Policy [CP].

4.4.2 Certificate Publication by the CSP

These provisions are specified in the Certificate Policy [CP].

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

These provisions are specified in the Certificate Policy [CP].

4.5 Certificate and Key-Pair Usage

4.5.1 Subscriber Certificate and Private-Key Usage

These provisions are specified in the Certificate Policy [CP].

4.5.2 Relying parties' Certificate and Public-Key Usage

These provisions are specified in the Certificate Policy [CP].

4.6 Certificate Renewal

These provisions are specified in the Certificate Policy [CP].

4.6.1 Criteria for Certificate Renewal

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

These provisions are specified in the Certificate Policy [CP].

4.6.2 Eligibility for Certificate Renewal

These provisions are specified in the Certificate Policy [CP].

4.6.3 Processing an Application for Certificate Renewal

Class 3-2, LCP

The CSP's appointed responsible party in the appropriate security-role verifies the eligibility for application as well as the signature according to the procedural instructions. After close examination, the verifier decides if the application is processed or rejected. If an application is further processed, the appropriate security-role produces the certificates. The verification or issuance can be automated in complete or partial regarding defined procedures.

Class 1

Parts of the applications are checked automatically, while other parts are manually verified. Applications are then either further processed or rejected.

4.6.4 Informing the Applicants about the Issue of a new Certificate

The regulations of chapter 4.3.2 apply.

4.6.5 Renewed-Certificate Transaction Procedures

These provisions are specified in the Certificate Policy [CP].

4.6.6 Publication of the Certificate-Renewal by the CSP

These provisions are specified in the Certificate Policy [CP].

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

These provisions are specified in the Certificate Policy [CP].

4.7 Certificate Renewal with Key-Renewal

These provisions are specified in the Certificate Policy [CP].

4.7.1 Criteria for Key-Renewal Certificates

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

Further provisions are specified in the Certificate Policy [CP].

4.7.2 Eligibility for Key Renewal

These provisions are specified in the Certificate Policy [CP].

4.7.3 Processing an Application for Key-Renewal

Class 3-2, LCP

The CSP's appointed responsible party in the appropriate security-role verifies the eligibility for application as well as the signature according to the procedural instructions. After close examination, the verifier decides if the application is processed or rejected. If an application is further processed, the appropriate security-role produces the certificates. The verification or issuance can be automated in complete or partial regarding defined procedures.

Class 1

Parts of the applications are checked automatically, while other parts are manually verified. Applications are then either further processed or rejected.

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

These provisions are specified in the Certificate Policy [CP].

4.7.5 Key-Renewed-Certificates Transaction Procedures

These provisions are specified in the Certificate Policy [CP].

4.7.6 Publication of Certificates after Key-Renewal by the CSP

These provisions are specified in the Certificate Policy [CP].

4.7.7 Notifying other PKI-participants about Follow-Up Certificates

These provisions are specified in the Certificate Policy [CP].

4.8 Certificate Changes

Certificate changes are not offered.

4.9 Revocation and Suspension of Certificates

4.9.1 Criteria for Revocation

A certificate is revoked in the following circumstances:

- upon request of the subscriber or possibly affected third parties (for example an organization that is named in the certificate),
- invalidity of data included in the certificate,
- if the CSP ceases its operations and no other CSP continues the duties.
- only code-signing certificates:
    - if the CSP becomes aware of the fact, that the certificate has been issued to a publisher of malware or
    - if the CSP becomes aware of the fact, that the certificate would damage the CSP's reputation if it remained valid

Apart from that, the CSP can arrange a revocation if:

- the private key of the issuing CA or of a higher CA is compromised,
- the key-pair is stored on a SmartCard which also holds the key-pair of a revoked qualified certificate,
- weaknesses of the used cryptographic algorithms become known that endanger the allowed applications during the validity-period of the certificate,
- the deployed hard- or software exhibits defects that endanger the allowed applications during the validity-period of the certificate,
- the unambiguous assignment of the key-pair to the subscriber is no longer possible,
- a certificate was obtained through the declaration of false data,
- the customer is in arrear after two requests for payment,
- the contractual relationship is cancelled or ends.

Class 3 EV-certificates

[GL-BRO] describes mandatory revocation reasons for EV-certificates (Annex A).

The CSP hosts the EV-reporting office according to section 11.3 [GL-BRO], where PKI-participants or software producers may report complaints 24/7, remark their suspicions about the compromise of EV-certificate private keys, report the abuse of EV-certificates, fraud or the improper behavior of EV-certificates.
The CSP will process any reported incidents in a timely manner (in the first 24 hours after the report has been issued), according to section 11.3.2 [GL-BRO], which may result in the revocation of the EV-certificates.
Abuse of D-Trust-EV-certificates can be reported under the e-mail address:

ev-support@d-trust.net.

Revocations are fitted with a date and are not issued retroactively. Revocation authorities must authenticate themselves according to chapter 3.4.

4.9.2 Eligibility for Revocation

These provisions are specified in the Certificate Policy [CP].

4.9.3 Processing a Revocation Application

These provisions are specified in the Certificate Policy [CP].

4.9.4 Deadlines for a Revocation Application

These provisions are specified in the Certificate Policy [CP].

4.9.5 CSP Revocation-Application Processing Time

These provisions are specified in the Certificate Policy [CP].

4.9.6 Methods of Validating Revocation-Information

These provisions are specified in the Certificate Policy [CP].

4.9.7 Revocation List Publication Frequency

These provisions are specified in the Certificate Policy [CP].

4.9.8 Maximum Latency Period for Certificate Revocation Lists

These provisions are specified in the Certificate Policy [CP].

4.9.9 Online Accessibility of Revocation Information

These provisions are specified in the Certificate Policy [CP].

4.9.10 Necessity of Checking Revocation Information online

These provisions are specified in the Certificate Policy [CP].

4.9.11 Other Forms of Publishing Revocation-Information

These provisions are specified in the Certificate Policy [CP].

4.9.12 Special Requirements for Compromised Private-Keys

These provisions are specified in the Certificate Policy [CP].

4.9.13 Conditions for a Suspension

These provisions are specified in the Certificate Policy [CP].

4.10 Status Monitoring Service for Certificates

4.10.1 Mechanics of the Status Monitoring Service

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

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

4.10.2 Availability of the Status Monitoring Service

These provisions are specified in the Certificate Policy [CP].

4.10.3 Optional Services

None.

4.11 Withdrawal from the Certification Service

These provisions are specified in the Certificate Policy [CP].

4.12 Key-Escrow and Key-Recovery

These provisions are specified in the Certificate Policy [CP].

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

These provisions are specified in the Certificate Policy [CP].

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

These provisions are specified in the Certificate Policy [CP].

5 Non-Technical Security Provisions

The descriptions in this chapter refer to the class 3-2 CAs operated by the D-TRUST GMBH.

5.1 Structural Security Provisions

The D-TRUST GMBH is a Certification Service Provider that is accredited for being in strict accordance with the provisions of the German signature law. The structural security provisions are documented en detail in the infrastructural security concept for signature-law-conforming Certification Service Providers [SiKo-DTR]). This may be made available on request, if a vested interest is in evidence. The security concept has been verified by the Regulation Authority's approved technical control board (TÜV Informationstechnik GmbH). The inspection and approval are reiterated periodically and following any security-relevant infrastructural changes.

Part of the security concept is a detailed documentation of the structural security- and monitoring provisions that may be made available on request, if a vested interest is in evidence.

Apart from the above, the technical control board TÜV-IT has certified the D-TRUST GMBH high-security TrustCenter for applying and implementing the "Infrastructural measures for high protection requirements – Level 3" (according to the inspection criteria catalogue for „Trusted Site Infrastructure"). All infrastructurally relevant aspects are tested and assessed in the course of this TÜV-IT-certificate "Trusted Site Infrastructure". This assessment is reiterated every two years.

These certificates attest the D-TRUST GMBH a high non-technical standard for security provisions.

The CSP operates the Root-PKI's CAs under the same conditions as the D-TRUST GMBH CAs for the issue of qualified certificates with provider accreditation according to the German signature law.

5.2 Practice Regulations

5.2.1 Role-Concept

The security concept encompasses a role-concept [SiKo-DTR], in which employees are assigned one or several roles with the appropriate permissions. The role-permissions are limited to those that need them for the completion of their duties.

Employees that work in the area of certification- and revocation services operate independently and are free of commercial/financial attachments that could influence their decisions and actions. The CSP's organizational structure encourages the employees in their independence and decisions.

Employees' identities, trustworthioness and knowledge are validated before a sensitive function is assigned. Periodic training as well as training aimed at newly arisen topics ensure the employees's competence in their functions and the companies overall informational security. The CSP thereby complies with the requirements of section 12.1 [GL-BRO].

5.2.2 Principle of Multiple Administrators

Highly critical procedures can only be performed with the help of at least two attending administrators. This necessity is implemented through technical and organizational provisions, such as restricted access rights and strict knowledge division.

5.2.3 Role Identification and Authentication

The role concept is enforced by technical and organizational provisions, such as limited access privileges, the targeted inquiry of partial passwords etc. The realizing administrator has to authenticate himself successfully before gaining access to critical applications. Any action can be retraced through event-logs and tied to the administrating employee. Employees are accountable for their actions.

5.2.4 Role-Exclusion

The role-concept arranges for certain role-exclusions that keep a single person from creating and publishing a certificate himself. No single person has the authority to undertake all necessary steps to create a certificate.

5.3 Employees

The CSP complies with the personnel requirements set out by [SigG] and [SigV] which it details in the security concept [SiKo-DTR].

5.3.1 Requirements of Qualification, Expertise and Reliability

The CSP ensures that the personnel employed in the Certification Service possess the necessary qualification, expertise and skill required by their functions.

5.3.2 Security Validation

The CSP complies with the requirements of § 5 (5) SigG. The details are described in the security concept [SiKo-DTR]. Among other provisions, the employees must periodically present valid and unblemished criminal records.

5.3.3 Training

The CSP trains people working in the Certification Service.

5.3.4 Periodicity of Training and Instructions

The CSP trains people working in the Certification Service upon the initiation of their duties and when necessary.

5.3.5 Frequency and Consequences of Job-Rotation

Role-transferences are conducted in accordance with the security concept [SiKo-DTR] (access privileges, access control) and documented. The new personnel will receive extensive training before becoming involved in production processes.

5.3.6 Consequences of Prohibited Actions

The CSP releases unreliable employees from the Certification Service.

5.3.7 Conditions for Freelancers

Not applicable; freelancers are not employed.

5.3.8 Delivered Documentation

Comprehensive procedural instructions for every production step define the appropriate personnel-role, the personnel-rights and the manual and automatic monitoring-necessities. The technical security provisions implemented in the D-TRUST infrastructure ensure that the defined production steps can not be circumvented.

5.4 Monitoring

The CSP implements extensive monitoring capabilities (through video cameras for example) to secure the Certification Services, their IT-systems and documentation. These provisions are documented in the security concept [SiKo-DTR].

The monitoring capabilities are complemented by the organizational regulations. Visitors for example are only allowed onto the premise if appointments have been made at least 24 hours prior to their visit. Additionally, visitors must deposit their ID-documentations for the period of visitation. Visitors to the TrustCenter area must always be accompanied by an employee of the CSP.

Surveying threats to the CSP's operations and defining subsequent requirements and counter measures by continuous risk-analysis is a further part of the security concept. The risk-analysis also contains a residual-risk analysis, in which the tenability of the residual risk is shown.

5.5 Archiving of Records

5.5.1 Forms of Record Archives

There are two forms of archiving: electronically and paper-based.

The complete application documents (follow-up applications included), the procedural documents (CP, CPS), certificates, revocation documentation, digital data and protocols concerning the certificate life-cycle are archived.

5.5.2 Data Archiving Period

Class 3-2, LCP

Application documents and their verifications, the data concerning the certificate life-cycle as well as the certificates themselves are stored for at least five years and always additionally for the remainder of the year in which the archiving period expires[3]. The retention period for all SSL-certificates including Class 3 EV-certificates is seven years. It starts when the last certificate that has been issued upon the basis of these documents expires.

5.5.3 Archive Security

The archive is located in secured rooms and is subject to the role- and access-control-concept of the CSP.

5.5.4 Archive Backup

Data confidentiality and integrity are observed. The documentation takes place instantly, so that retroactive altercations can not occur without detection. The German federal privacy requirements are observed.

5.5.5 Demands on Time-Stamping of Records

The CSP operates a time stamping service according to [SigG].

5.5.6 Archiving (internal / external)

Archiving takes place in the perimeter of the CSP as well as on equally secured external premises.

5.5.7 Procedures for Acquisition and Verification of Archive Information

The procedures for the acquisition and verification of archive information are subject to the role concept of the CSP.

5.6 CSP Key-Change

The CSP will generate new CA-keys an adequate time period before a CA expires. A new CA-instance will be created from the generated keys and subsequently published.

5.7 Compromise and CSP Business Takeover

5.7.1 Treatment of Incidents and Compromises

The CSP has a contingency-concept as well as a recovery-plan, which are both known to the concerned roles and can be implemented if the need arises. The responsibilities are clearly appointed and known.

[3] If the token should contain qualified EU-certificates or qualified EU-certificates from an accredited provider in addition to the non-qualified certificates of the Root-PKI, then the archiving period follows the procedure for the certificates of the highest class.

5.7.2 Recovery after Resource-Compromise

The security-concept gives a description about the recovery-procedures.

5.7.3 Compromise of the Private CA-Key

In the case of a compromise or a publication of algorithm-weaknesses or associated parameters through the relevant authorities as named in section 6.1.6 the CSP will act as follows:

- implicated CA-certificates and their issued, still valid certificates are revoked,
- involved subscribers or applicants are informed about the incident and briefed on the consequences,
- the incident is published on the CSP's web-sites, noting that the certificates issued by the implicated CA have been invalidated.

The reasons for the compromise will be analyzed so that steps may be implemented to avoid future compromises. Taking the reason for the compromise into account, new CA-signature-keys are generated and new CA-certificates are issued.

5.7.4 Possibilities for Business Continuation after Compromise and Disaster

In case of emergency the CSP will decide, depending on the kind of incident, if a recovery of the backup described in section 6.2.4 will be conducted or if in case of compromise the procedures in section 5.7.3 are implemented.

5.8 CSP Discontinuation

If CAs are discontinued the CSP informs all subscribers and terminates possible contractor's access possibilities as related to the implemented CAs. Any valid certificates that were issued by the CAs will be revoked. Implicated private CA-keys will be destroyed.

The directory service as well as the application documents will be transferred to the Bundesdruckerei GmbH and continued in an equivalent manner. The preservation of the directory service is guaranteed until the EU-certificates expire and will either be transferred to a different CSP or to the Bundesdruckerei GmbH.

The CSP has an appropriate "letter of comfort" to cover the costs of these minimum requirements in the case of illiquidity of the CSP or for the case that the CSP can not cover the costs of the transferral for any other reasons.

If CSP operation is discontinued, the CAs functionality is ceased, so that a certification is no longer possible.

6 Technical Security Provision

The descriptions in this chapter refer to the class 3-2 CAs operated by the D-TRUST GMBH.

6.1 Creation and Installation of Key-Pairs

We differentiate between key-pairs for

- CA-certificates (D-TRUST Root CA Class 3-2 and their Sub-CAs) and
- End-User certificates (EU-certificates)

6.1.1 Creation of Key-Pairs

CA-keys are created in a „FIPS 140-2 Level 3"-conforming Hardware Security Module (HSM). The HSM is situated in the high-security tract of the TrustCenter. The creation of the key-pairs is subject to the role-concept and therefore always overseen by at least two operators.

EU-keys are created in a cryptographically secure manner by the CSP or the applicant and conform to the demands of the [CP] and [CPS].

Class 3-2
If EU-keys and EU-certificate are saved to a SmartCard (Secure User Device (SUD) according to [ETSI-F], D-TRUST GMBH avails itself of certified SSCD as SUD), the CSP handles the acquisition, storage, personalization and PIN-handling as it does in its qualified, signature-law and security-concept conforming sector. The CSP may have third parties that abide by a signature-law conforming security concept generate the keys and personalize the SmartCards. The CSP has a signature-law-conforming interface to these external personalizers.

Class LCP
Keypairs of certificates that have been produced as Soft-PSE are proced in safe environments following trustable crypto-applications.

6.1.2 Delivery of Private-Keys to Subscribers

If the private keys are created by the CSP, they will be transferred as noted in chapter 4.4.1.

6.1.3 Delivery of Public-Keys to Certificate Issuers

CA-key-pairs are created in the TrustCenter.

The EU-key-pairs that are created in the CSP are known to the CSP. Certificate requests for available keys may be submitted as a PKCS#10-request by the applicant The PKCS#10-request contains the public key and must be signed by the private key.

6.1.4 Delivery of Public CA-Keys to Relying Parties

A CAs public key is contained in its certificate. This certificate is usually stored on a token that is transferred to the applicant. CA-certificates may also be downloaded from the public directory service (compare chapter 2.1), into which they are published after their creation.

6.1.5 Key Length

Class 3-2

CA-certificates are currently issued with 2048-bit RSA-keys.

EU-certificates are currently issued with 2048-bit RSA-keys.

Class 1

CA-certificates are currently issued with 2048-bit RSA-keys.

EU-certificates are currently issued with 1024-bit RSA-keys.

6.1.6 Determination of Key-Parameters and Quality-Control

Class 3-2

CA- and EU-certificates are issued on the basis of keys that comply to the currently valid [ETSI-ALG] if supported widely by a substantial portion of applications.

Class 3 EV-Certificates

CA- and EU-certificates are issued exclusively on the basis of keys that comply to the currently valid [ETSI-ALG] and [GL-BRO].

Class 1

The CSP defines key-parameters for CA- and EU-certificates.

Signature- and encryption-algorithms are named in section 7.1.3 CPS.

6.1.7 Key-Usage

Private CA-Keys are exclusively used to sign certificates and CRLs (compare chapter 7.1.2).

EU-keys may only be used for the use-cases noted in the certificate. The use-cases are noted in the certificate fields *KeyUsage* and *ExtKeyUsage* and may be restricted by additional extensions (compare chapter 7.1.2).

6.2 Securing the Private-Key and Cryptographic-Module Requirements

6.2.1 Standards and Security Provisions for Cryptographic Modules

The CSP's cryptographic Modules work flawlessly. The modules are protected through technical and organizational procedures from unauthorized manipulation throughout their life-cycle (including delivery and storage).

A FIPS 140-2 Level 3 conforming HSM is used to secure CA-keys.

The CSP has fitting hardware as well as software based key-generators in order to guarantee the quality of EU-keys.

6.2.2 Multi-Person Private-Key Access-Control (n of m)

The HSM containing the CA-keys is situated in the high-security tract of the TrustCenter. To activate a private key, two authorized employees are necessary. The HSM can sign any desired amount of certificates after the private key is activated.

Private EU-keys are only accessed in case of key-escrow as described in chapter 6.2.3.

6.2.3 Key-escrow of Private-Keys

Private CA-keys are not escrowed.

Private EU-key escrow may be applied for. The keys will be encrypted and kept in the high-security tract of the TrustCenter. Encrypted keys can only be decrypted by authorized employees.

Class 3-2
EU-certificate signature-keys are not escrowed.

Class 3 EV-certificates
Class 3 EV-certificate signature-keys are not escrowed.

6.2.4 Backup of Private-Keys

Private CA-keys are backed up. A CA-key backup is performed in the high-security tract of the TrustCenter and requires two employees that are authorized to access the HSMs. The same requirements and security procedures that apply for the productive system also apply to the backup system. A restoration of the private key also requires two employees that are authorized to access the HSMs. There are no further copies of the private CA-keys.

A backup of private EU-keys is not offered except in a possible applicant-requested key escrow.

6.2.5 Private-Key Archiving

Private CA- and EU-keys are not archived.

6.2.6 Transferring Private-Keys into/out of Cryptographic Modules

Private CA-keys are only transferred into or out of an HSMs if they are backed up or recovered respectively. The presence of at least 2 administrators is enforced. In case of the export into, or the import out of a different HSM, the private CA-key is encrypted.

Private EU-keys may be transferred out of an HSM, if the transfer is technically possible and the applicant can prove along the guidelines in chapter 4.12.1 that he is entitled to re-use the key. The key is always encrypted when transferred.

6.2.7 Storage of Private-Keys in Cryptographic Modules

The private CA-keys are encrypted and stored in the HSM.

EU-keys are encrypted and stored in a database of the CA-system.

6.2.8 Activating Private-Keys

Private CA-keys can only be activated by at least two attending administrators in the appropriate roles and only for the allowed use-cases (*keyCertSign, cRLSign*).

Private EU-keys are activated by the correct PIN input.

6.2.9 Deactivating Private-Keys

Private CA-keys are deactivated upon the disconnection between the utilizing application and the HSM.

A private EU-key is deactivated by the utilizing application or by the removal of the SmartCard from the card reader respectively the deactivation or deletion of the soft-PSE, as the case may be.

A permanent deactivation of SmartCard based EU-private keys ensues after multiple incorrect PIN inputs. PUK reactivations of a card are numbered and MultipleSmartCards are not programmed to accept a PUK.

6.2.10 Destroying Private-Keys

Private CA-keys are deleted after their expiration. The keys are deleted from the HSM as well as from the backup mediums. If an HSM is decommissioned, the private keys are deleted from it.

If a SmartCard chip is destroyed or the files containing the private EU-key are deleted, the key is irreparably lost. The destruction of keys escrowed at the CSP may be requested (according to section 4.12.1).

6.2.11 Appraisal of Cryptographic Modules

The CSP makes use of qualified hard- and software based key-generators to ensure the quality of EU-keys. The production HSMs are FIPS 140-2 Level 3 certified.

6.3 Other Aspects of Key-Pair Management

6.3.1 Archiving Public-Keys

Public CA- and EU-keys are, conforming to the security concept, archived in form of the created certificates.

6.3.2 Certificate- and Key-Pair Validity-Period

The validity-period of CA-keys and certificates is variable and may be learned from the certificates. The maximum validity period is 30 years.

The validity-period of EU-keys and certificates is variable and may be learned from the certificates.

The maximum validity period is:

Class 3-2
61 months, (maximum validity for SSL-certificates is 39 month)

Class 3 EV-certificates
27 months

Class 2 LCP
60 months

Class 1
15 years.

6.4 Activation-Data

6.4.1 Activation-Data Creation and Installation

CA-key activation-data is requested by the HSM. PINs are assigned during bootstrapping. The presence of at least two administrators is enforced.

Subscriber: if the key-pair is created by the subscriber, the activation-secret is also created and is available to the subscriber. A transport-PIN-procedure may be incorporated if the CSP creates the keys, otherwise the PINs will be printed to a PIN-letter and mailed- or given to the subscriber. An installation is not necessary.

6.4.2 Activation-Data Protection

CA-key activation-data is composed of two secrets, one and only one of which is known to one and only one authorized employee. Activation-data may only be accessed by certain designated employees.

Subscriber: If the transport-PIN-procedure is utilized, the SmartCards integrity can be verified through the transport-PIN. Otherwise the PINs are printed once to a specially secured letter and sent- or given to the subscriber.

6.4.3 Other Aspects of Activation-Data

Depending on the product in question, the subscriber may be given a Personal Unblocking Key-Number (PUK) to unlock the SmartCard in the case that the PIN should have been input incorrectly three times. MultipleSmartCards do not accept a PUK.

6.5 IT- Infrastructure Security-Provisions

6.5.1 Specific, Technical Security-Demands on the IT-Infrastructure

The computers, networks and other components employed by the CSP safeguard in their specific configuration that only those actions are permitted, that do not conflict with the

provisions laid-out in the [CP] and [ETSI-F], and in the case of class 3 EV-certificates also in [GL-BRO].

The subscriber as well as the relying parties must only use trustworthy hard- and software.

6.5.2 Computer Security Evaluation

The computers, networks and other components employed for the CA-keys are evaluated by the Regulation Agency's approved technical control board, the TÜV Informationstechnik GmbH.

6.6 Technical Provisions throughout the Life Cycle

6.6.1 Security Provisions during Development

The CSP's system developments are continuously analyzed from the design stage onward according to their adherence to the highest safety requirements.

6.6.2 Security Provisions of Computer Management

Computers, networks and other involved components may exclusively be administered by personnel after a prior authorization corresponding to the role-concept (part of the security-concept of the signature-law complying CSP D-TRUST GMBH). Log files are periodically parsed for rule-infringements, attacks and other occurrences. Monitoring starts with the start of operations and ends with the decommissioning of a machine.

6.6.3 Security Provisions throughout the Life Cycle

Machines are operated according to the manufacturer's instructions. They are minutely inspected before being deployed and are only used if a manipulation can be excluded without a doubt. Manipulations and manipulation attempts are noticed as soon as a legitimate action takes place at the machines or the machines are inspected in the course of a periodic revision, since all access possibilities of incorporated hardware (disk-slots, USB-slots, screws etc.) are sealed and periodic software-checks, among other security provisions, are automized. Should a machine's manipulation be suspected, a possibly planned action will not be carried out while the incident is reported to the head of the CSP. Clear escalation guidelines for each role have been defined in order to instantly react to eventual security-relevant incidents in a coordinated.

Capacity-requirements and –utilization as well as system suitability are monitored and adapted if necessary. Replaced systems are decommissioned such that functionality- and data misappropriations become impossible. System- or process changes are monitored by a change-management process. Critical changes are scrutinized by the security manager. The CA private-keys are destructed after CA expiration.

Relevant occurrences pertaining to a CAs life-cycle, its issued certificates and the generated keys are documented in electronic form or as hard-copy print-outs and are archived audit-compliantly (read-only revision-safe) on long-lived media.

Class 3 EV

As a minimum, the events listed in 13.1 [GL-BRO] are audit-compliantly logged or recorded.

6.7 Network Security Provisions

A network concept is inseparably linked to the operation of the CA. The network concept is documented en detail (security concept of the signature-law complying CSP D-TRUST GMBH – network concept [SiKo-DTR]), which may partially be made available on request, if a vested interest is in evidence. The CSP use firewall and IDS/IPS technologies to prevent its processes from being damaged. The CPS also divides its network into different zones according to their protection requirements. So i.e. user-networks, DMZs and backendnetworks are highliy separated. The systems are audited regularly, the roles are responsible to report. Abnormalities are also reported by technical systems and organizational processes and will be processed in definded incident procedures and affiliated processes.

Data with high protection requirements to integrity and confidentially outsite of the CSP-saved networks are secured by cryptological mechanisms.

Physical security of CSP maintained networks is ensured and continually adapted to change.

6.8 Time-Stamps

The CSP operates a Time-Stamping-Authority in accordance with the [SigG]. Time stamps however are not offered within the framework of this CPS.

7 Profiles of Certificates, CRLs and OCSP

7.1 Certificate Profiles

7.1.1 Version Number

Certificates are issued along the X.509v3 format.

7.1.2 Certificate Extensions

The choice of extensions largely depends on the product.

CA-certificates contain the following *critical* extensions:

Extension	**OID**	**Parameter**
KeyUsage	2.5.29.15	*keyCertSign, cRLSign*
BasicConstraints	2.5.29.19	*ca=TRUE, (pathLenConstraint)*

CA-certificates may contain the following *uncritical* extensions:

Extension	OID	Parameter
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash of the issuing key
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 Hash of the Subject's Public Key
CRLDistributionPoints	2.5.29.31	LDAP-address of the CRL-distribution point
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 for supporting CPs
SubjectAltName	2.5.29.17	Alternative subject name

Additionally extensions may be incorporated if they comply with [X.509], [RFC 5280], and [CO-PKI] or are described in a referenced document.

EU-certificates contain the following *critical* extensions:

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

EU-certificates may contain the following *uncritical* extensions:

Extension	OID	Parameter
ExtKeyUsage	2.5.29.37	According to [RFC 5280]
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash of the issuing key
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 Hash of the Subject's Public Key
CRLDistributionPoints	2.5.29.31	CRL- distribution point in the form of an ldap-address
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 for supporting CPs *cpsURI*
SubjectAltName	2.5.29.17	Alternative subject name

Additionally extensions may be incorporated if they comply with [X.509], [RFC 5280], and [Co-PKI] or are described in a referenced document.

7.1.3 Algorithm-OIDs

The following encryption algorithm is currently employed in CA- and EU-certificates:

- RSA with the OID 1.2.840.113549.1.1.1.

The following signature algorithms are currently employed in CA- and EU-certificates:

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

7.1.4 Name Formats

The fields *subject* (here: end-user name) and *issuer* (issuer name) are used to store names in the [X.501] DistinguishedName format. The attributes detailed in section 3.1.4 may be assigned. The attributes are encoded as UTF8-string or, in the case of the attribute C (country) as PrintableString.

The fields *SubjectAltName* (alternative subscriber name) and *IssuerAltName* (alternative issuer name) can hold names according to [RFC 5280], which are encoded as IA5String.

7.1.5 Name Constraints

The extension „NameConstraints“ is not used.

7.1.6 Certificate Policy Object Identifier

The field „CertificatePolicies“ may hold the OID of supporting CPs.

Class 3
Class 3 certificates may include the OID of the [ETSI-F] defined NCP or NCP+. Apart from these, other CPs may be referenced. This CPS complies with the [ETSI-F] guidelines.

Class 3 EV
Class 3 EV-Certificates may include the OID of the [ETSI-F] defined EVCP. Additionally other CPs may be referenced.

7.1.7 Usage of the extension „PolicyConstraints“

The extension „PolicyConstraints“ is not used.

7.1.8 „PolicyQualifiers“ Syntax and Semantics

The extension „PolicyQualifier“ is not used.

7.1.9 Processing the Semantics of the Critical Extension CertificatePolicies

The extension *CertificatePolicies* is uncritical in CA- and EU-certificates. Subscribers and relying parties may or may not evaluate this extension.

7.2 CRL Profiles

7.2.1 Version Number(s)

CRL v2 are issued according to [RFC 5280]. Delta-CRLs are not offered.

7.2.2 CRL extensions and CRL items

CRLs may incorporate following uncritical extensions:

Extension	OID	Parameter
cRLNumber	2.5.29.20	CRL number
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash of the issuing key

7.3 Status Monitoring Service (OCSP) Profile

7.3.1 Version Number(s)

OCSP v1 is employed according to [RFC 2560].

7.3.2 OCSP-extensions

In OCSP-requests, the responder supports the following extensions:

Extension	Parameter
RetrieveIfAllowed	If set, the certificate is included in the answer (optional).

The OCSP-responder uses the following extension in its answers:

Extension	Parameter
ArchiveCutoff	Time-period for which status information will be available through the OCSP-responder after a certificate has been created.
CertHash	In the cases of status = good or status = revoked, the SHA-1 hash-value of the certificate is included in this extension.
CertInDirSince	Time of certificate publication into the central directory service.
RequestedCertificate	Contains the certificate, if the request-extension *RetrieveIfAllowed* was set.

All the extensions are uncritical. Further uncritical extensions may be included.

8 Verifications and other Appraisals

These provisions are specified in the Certificate Policy [CP].

9 Other Financial and Legal Regulations

The provisions of chapter 9 are laid-out in chapter 9 of the [CP] and in the standard business terms.

Annex A Reasons for Revoking a Class 3 EV-certificate

Excerpt from the current 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.