Deutsche Telekom Security GmbH
Trust Center Certificate Policy

Version: 03.00

Valid from: 24.01.2023

Status: Released

Last Review: 20.01.2023

HISTORY

Table 1 - Change history

Version	Date	Changes / Comment
01.00	15.03.2021	Initial version based on [BR] 1.7.3, [NCSSR] 1.5, [EVCG] 1.7.4, [ETS401] 2.2.1, [ETS411-1] 1.2.2, [ETS411-2] 2.2.0, [ETS412-1] 1.1.1, [ETS412-2] 2.1.1, [ETS412-3] 1.1.1, [ETS412-4] 1.1.1, [ETS412-5] 2.2.3, [ETS312] 1.3.1, [TR3145] 1.1, [TR3145VS] 1.0
01.01	15.04.2021	Update: [BR] 1.7.4 *- not published -*
01.02	13.07.2021	Update: [ETS411-1] 1.3.1, [ETS412-1] 1.4.4, [ETS412-2] 2.2.1, [ETS412-3] 1.2.1, [ETS412-5] 2.3.1 *- not published -*
01.03	30.08.2021	Update: [BR] 1.7.5 - 1.7.9, [NCSSR] 1.6 - 1.7 *- not published -*
01.04	13.09.2021	Update: [EVCG] 1.7.5 - 1.7.8 *- not published -*
01.05	25.10.2021	Update: [BR] 1.8.0 *- not published -*
01.06	02.12.2021	Update: [ETS411-2] 2.4.1, [ETS412-4] 1.2.1 *- not published -*
02.00	02.03.2022	Annual review, update: [BR] 1.8.1
03.00	24.01.2023	Annual review, update [BR] 1.8.2 – 1.8.6, [EVCG] 1.7.9 – 1.8.0

TABLE OF CONTENTS

LIST OF TABLES

1 INTRODUCTION

1.1 Overview

Deutsche Telekom Security GmbH (hereinafter referred to as "Telekom Security") provides several Trust Services for issuing certificates to support PKI products offered on the market and customer-specific PKI solutions and thus acts as a Trust Service Provider (TSP).

As a TSP, Telekom Security operates various certification authorities (CAs) in its Trust Center. These are both Root Certification Authorities (Root CAs) and Subordinate Certification Authorities (Sub CAs) for issuing certificates, both for customers and employees of the Deutsche Telekom AG Group.

In addition, Telekom Security has issued public Sub CA certificates to the "Verein zur Förderung eines Deutschen Forschungsnetzes e. V." (hereinafter referred to as "DFN" for short), which DFN as an independent TSP uses to issue certificates for its affiliated institutions.

Note: There are currently no plans to issue further Sub-CA certificates to DFN or other organizations not affiliated with Deutsche Telekom, so this CP no longer addresses any requirements in this regard. However, the requirements to be met in ongoing operations continue to apply to DFN, so that in the following the term TSP refers to both Telekom Security and DFN, if applicable.

This document is the Certificate Policy (CP) of the Telekom Security Trust Center. It summarizes in the structure of [RFC3647][1] all relevant requirements from the documents referenced in Appendix B that must be implemented by the Trust Services within the scope of this CP.

The scope of this CP comprises all Telekom Security Trust Services via which certificates are issued below the

- public and qualified Root CAs of Telekom Security,
- internal Root CAs of Telekom Security that have committed to this CP,
- Root CAs issued by the German Federal Office for Information Security (“Bundesamt für die Sicherheit in der Informationstechnik”, BSI) in accordance with [TR3145].

The following semantics apply to the requirements listed in this document:

- Requirements that are not specifically marked apply in general for all certificate types.
- Framed requirements that begin with the specification of one or more certificate types in square brackets apply only to those certificate types.

The following certificate types are differentiated in this document:

- [TLS] identifies all TLS authentication certificates issued under the Telekom Security public Root CAs integrated in the Root Stores of Microsoft [MSRP], Mozilla [MOZRP], Google [GCRP] and Apple [APLRP], in accordance with "CA/Browser Forum Baseline Requirements" [BR].
  Note: unless explicitly stated otherwise, the requirements of [TLS] also implicitly apply TLS certificates issued in accordance with [DVCP], [OVCP], [IVCP], [EVCP], [QNCP-w] or [QEVCP-w].

[1] In addition to the sections recommended in [RFC3647#6], the following chapters have been added to this CP
- 3.2.7: Validation of control over a domain
- 3.2.8: Validation of control over an email address

- [SMIME] identifies all S/MIME certificates for email security that are issued under the Telekom Security public Root CAs integrated in the Root Stores of Microsoft [MSRP], Mozilla [MOZRP], Google [GCRP] and Apple [APLRP].
- [3145] identifies all certificates issued by Telekom Security in accordance with the [TR3145] under the BSI Root CAs.
- [VS-NfD] identifies all certificates that are issued in accordance with [3145] and also meet the requirements for “VS-NfD” in accordance with the add-on [TR3145VS].
- [LCP] identifies all certificates issued according to the "Lightweight Certificate Policy" defined in ETSI EN 319 411-1 [ETS411-1].
  Note: Unless explicitly stated otherwise, the requirements of [LCP] also implicitly apply to [DVCP], [IVCP] and [OVCP].
- [NCP] or [NCP+] identify all certificates issued according to the "Normalized Certificate Policy" or the "Extended Normalized Certificate Policy" defined in [ETS411-1]. Notes:
  - Unless explicitly stated otherwise, the requirements of [NCP] also implicitly apply to [NCP+], [QCP-n], [QCP-l], [QNCP-w] and [EVCP].
  - Unless explicitly stated otherwise, the requirements of [NCP+] also implicitly apply to [QCP-n-qscd], [QCP-l-qscd]
- [EVCP] identifies all certificates issued according to the "CA/Browser Forum Extended Validation Certificate Guidelines" [EVCG] and the "Extended Validation Certificate Policy" defined in [ETS411-1].
  Note: Unless explicitly stated otherwise, the requirements of [EVCP] implicitly apply to [QEVCP-w].
- [DVCP] identifies all certificates issued according to the "Domain Validation Certificate Policy" defined in [ETS411-1].
- [IVCP] identifies all certificates issued according to the "Individual Validation Certificate Policy" defined in [ETS411-1].
- [OVCP] identifies all certificates issued according to the "Organizational Validation Certificate Policy" defined in [ETS411-1].
- [QCP] identifies all EU qualified certificates according to [eIDAS] issued in accordance with ETSI EN 319 411-2 [ETS4112]. In detail, these are:
  - [QCP-n] qualified certificates for natural persons.
    Unless explicitly stated otherwise, the requirements of [QCP-n] also implicitly apply to [QCP-n-qscd].
  - [QCP-l] qualified certificates for legal persons.
    Unless explicitly stated otherwise, the requirements of [QCP-l] also implicitly apply to [QCP-l-qscd].
  - [QCP-n-qscd] qualified certificates for natural persons with use of the private key in a QSCD.
  - [QCP-l-qscd] qualified certificates for legal persons with use of the private key in a QSCD.
  - [QNCP-w] qualified web server certificates based on [TLS] and [NCP].
  - [QEVCP-w] qualified web server certificates based on [EVCP].
- [ETSI] identifies all certificates issued according to [LCP], [NCP], [NCP+] or [QCP].

The options or obligations to implement the requirements are described by the keywords according to [RFC2119]:

- SHALL indicates an absolute requirement.
- SHALL NOT indicates an absolute prohibition.
- SHOULD indicates a requirement, which can only be omitted if there are good reasons.
- SHOULD NOT indicates a prohibition, unless there are good reasons for implementation.
- MAY indicates that an item is truly optional.

Trust Services SHALL describe the implementation of the applicable requirements of this CP in their Certification Practice Statements (CPS), also structured according to [RFC3647]. The CPS SHALL address all aspects of this CP and consider all chapters of [RFC3647]. Subchapters that are not applicable SHALL be marked "No stipulation", i.e., these SHALL NOT be left blank or omitted.

Compliance with the requirements of this CP, in its current version, SHALL be explicitly confirmed in the CPS.

[TLS] Compliance with the then current version of the [BR], the [NCSSR] and, if applicable, the [EVCG] SHALL be explicitly confirmed in the CPS and the links to the documents of the CA/Browser Forum (http://www.cabforum.org) SHALL be included.

In the event of a conflict between this CP or the CPS and the [BR] or [EVCG], the regulations from [BR] or [EVCG] prevail.

[TLS] [SMIME] Compliance with the requirements to the policies of the relevant Root Stores [MSRP], [MOZRP], [GCRP], and [APRP] SHALL be explicitly confirmed in the CPS.

In the event of a conflict between [MOZRP] and the [BR], the regulations from [MOZRP] shall prevail.

The CPS SHALL be published under a Creative Commons license (CC-BY 4.0, CC-BY-SA 4.0, CC-BY-ND 4.0, CC-0 1.0 or newer versions).

1.2 Document name and identification

This document is named "Certificate Policy of the Telekom Security Trust Center" and is identified by the OID 1.3.6.1.4.1.7879.13.42. The OID is composed as follows:

{iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) T-Telesec (7879) PolicyIdendifier (13) Certificate policy of the Telekom Security Trust Center (42)}

1.3 PKI participants

1.3.1 Certification Authorities

Telekom Security operates several public as well as internal Root and Sub CAs. It also issues its own Cross Certificates, but not cross certificates to Root or Sub CAs of other TSPs.

The scope of this document also includes the public Sub CAs of the DFN issued by Telekom Security.

The complete hierarchies, i.e., all relevant Root and/or Sub CA certificates in the scope of a CPS, SHALL be listed in the respective CPS.

Note: For the sake of simplicity, the term "CAs" is used below as a synonym for "Root and Sub CAs", i.e., the requirements for "CAs" refer to both Root and Sub CAs, unless otherwise specified. The same applies to the term "CA certificates", which also includes cross certificates.

1.3.2 Registration Authorities

The Registration Authorities (RA) used MAY be both the TSP's internal RAs and external RAs acting on their behalf. The requirements for RAs set out in this document SHALL be implemented equally for internal and external RAs, where applicable.

When using external RAs, the structures, relevant processes as well as their rights and obligations SHALL be described in the respective CPS and appropriate agreements SHALL be met.

[TLS] [SMIME] The validation of domain names and IP addresses SHALL NOT be handed over to external RAs, see Section 4.2.

1.3.3 Subscribers

Note: Due to the partially different use of terms in the documents referenced in Annex B, the terms as used in this document are described below.

Subscribers in the context of this CP are natural persons or organizations to whom a certificate is issued and who are legally bound by acceptance of the Terms of Use. A certificate subscriber may also be the subject of a certificate and/or the applicant at the same time.

Organizations in the context of this CP are legal persons or organizational units identified in association with a legal person. Organizations may be:

- Private Organizations: Non-governmental legal persons whose existence was created by a filing with or an act of the Incorporating Agency or equivalent body
- Government Entities: Government-operated legal persons, agencies, departments, or other related organizational units
- Non-Commercial Entities: International organizations created under a charter, agreement, convention, or equivalent instrument signed by or on behalf of more than one government of a country
- Business Entities: Organizations that are not one of the previously mentioned organizations

Subject of a certificate in the context of this CP is the user of the private key named in the certificate in the attributes of the `subjectDN` or the extension `subjectAltName`.

Within the scope of this CP, subjects are

- natural persons,
- natural persons identified in association with an organization,
- organizations,
- devices[2] operated by or on behalf of a natural person or an organization.

The subscribers and subjects in the scope of a CPS SHALL be listed in the respective CPS.

Applicant in the context of this CP is the person who submits the application to the TSP. This is always a natural person who is either

- the subscriber and/or the subject itself,
- an authorized representative of the subscriber (in the case of an organization) or
- another person authorized by the subscriber.

[2] the term "devices" hereinafter also subsumes systems, functions and IT processes, unless explicitly stated otherwise

[EVCP] Subscribers MAY only be the above-mentioned organizations.

Note: “Applicant” as used in this CP is synonymous with “Certificate Requester” as per [EVCG].

In addition to the applicant, the following roles SHALL be implemented:

- **Contract Signer**: A natural person who is explicitly authorized to represent the certificate subscriber and to sign certificate requests on its behalf.
- **Certificate Approver**: A natural person who is explicitly authorized to represent the certificate subscriber and to approve certificate requests on its behalf.

A person MAY be entrusted with more than one of the listed roles and the roles MAY be filled by more than one person.

1.3.4 Relying parties

No stipulation.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The allowed uses of the certificates SHALL be described in the CPSs, the Terms of Use and, if applicable, the PKI-Disclosure Statements (PDS).

1.4.2 Prohibited certificate uses

The prohibited uses of the certificates SHALL be described in the CPSs, the terms of use and, if applicable, the PDSs.

[EVCP] Certificates SHALL NOT be used for purposes other than TLS server authentication of web servers.

1.5 Policy administration

1.5.1 Organization administering the document

This document is administered by:

Deutsche Telekom Security GmbH
Trust Center & ID Security
Untere Industriestraße 20
57250 Netphen, Germany

1.5.2 Contact person

The contact for this CP is the Trust Center's PKI Compliance Management, which can be reached via email under trustcenter-roots@telekom.de.

[TLS] [SMIME] To report suspected key compromise, misuse, or other types of fraud or inappropriate behavior, well-defined processes SHALL be established. These SHALL be described/published on the TSP's public web pages as well as in the CPSs in Section 1.5.2.

[VS-NfD] Contacts are the Trust Center's Information Security Officer and his deputy, who can be reached via email under FMB-ISMS-TrustCenter@telekom.de.

1.5.3 Person determining CPS suitability for the policy

Responsible for determining the conformity of a CPS to this CP is the Trust Center's PKI Compliance Management, for contact see Section 1.5.2.

1.5.4 CPS approval procedures

New versions of this CP SHALL be approved by the Trust Center management.

New versions of a CPS based on this CP SHALL first be reviewed by the Trust Center's PKI Compliance Management to determine the conformance to this CP and then be approved by the Trust Center management.

1.6 Definitions and acronyms

Definitions, abbreviations and references are listed in the appendix of this document:

- Appendix A: Abbreviations
- Appendix B: References
- Appendix C: Definitions

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

It SHALL be described in the CPSs who maintains which directories containing information about the certificates in the scope of the respective CPS.

2.2 Publication of certification information

The currently valid version of this document and the relevant superseded versions are published on the web pages of the Telekom Security Trust Center at the following address: https://www.telesec.de/de/service/downloads/pki-repository/

At a minimum, for each Trust Service the following information SHALL be published via suitable online services that can be accessed around the clock:

- Terms of Use in a generally understandable language
- CPS
- CA certificates
- status information according to Sections 4.9 and 4.10 for all unexpired certificates issued by them

The Terms of Use, CPSs as well as the CA certificates SHOULD be published in the above-mentioned PKI repository analogously to this CP, unless otherwise specified.

The Terms of Use and CPSs SHALL be versioned and provided with validity dates so that they can be easily associated with the certificates issued.

In addition, the certificates MAY be published with the subscriber's consent (see Section 4.4.2).

[TLS] The CPSs and the audit attestations SHALL (also) be published in English. The translated CPSs SHALL have the same version number as the original CPSs and SHALL NOT differ significantly from them in content. It SHALL be defined for each CPS which version is authoritative in case of dispute.

All issued certificates or alternatively all "pre-certificates" (see Section 4.3.1), including at least all Sub CA certificates (Root CA optional) from its chain, SHALL be published in a sufficient number of "Certificate Transparency Logs" (CTLogs). For the number of CTLogs, see Section 7.1.2 (40).

For each public Root CA certificate, below which TLS server certificates are issued, test web pages SHALL be provided that are equipped with corresponding TLS server certificates that chain up to the respective Root CA. Web pages with one valid, one expired and one revoked certificate SHALL be provided.

If TLS server certificates according to [EVCG] are also issued below a Root CA, at least the above-mentioned test websites SHALL be provided and be equipped with TLS server certificates according to [EVCG].

[TLS] [SMIME] The information of all CA certificates SHALL be published in the "Common CA Database" (CCADB) in accordance with the CCADB policy (see https://www.ccadb.org) and kept up to date.

The CPSs SHALL be published on the TSP's official website. The entire history of the CPSs associated with a Root CA and its issued Sub CAs SHALL be kept for the entire time that the Root CA is included as trustworthy in the above-mentioned Root Stores.

[QCP] In addition to the CPS a PKI Disclosure Statement (PDS) in the structure according to Annex A of [ETS4111] SHALL be published for each Trust Service.

A PDS SHALL indicate that the trust anchor for validating a certificate must be specified in the `ServiceDigitalIdentity` of the TSP's entry in the EU-TL.

The EU Trust Mark MAY be used by the Qualified Trust Services.

2.3 Time or frequency of publication

New versions of this CP and the CPSs based on this CP SHALL be published before they become effective.

[TLS] [SMIME] New Root CA certificates SHALL be published at the latest when applying for Root inclusion with one of the Root Stores listed in Section 1.1.

New Sub CA certificates under the Root CAs included in the above-mentioned Root Stores SHALL be published before they are put into operation, but no later than 7 days after their issuance.

Audit attestations SHALL be published no later than 7 days after their issuance.

The time or frequencies of the publications listed in Section 2.2 SHALL be described in the CPSs.

2.4 Access controls on repositories

The directories SHALL be publicly available in a read-only manner and SHALL be protected against unauthorized manipulation as well as data loss.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The subject names SHALL be included in all certificates at least in the form of a distinguished name in the attribute of the `subjectDN` in accordance with [X500] , see Section 7.1.4.

Depending on the certificate type, requirements for subject name elements to be included in the `subjectAltName` extension SHALL also be taken into account, see Section 7.1.2.

[DVCP] The `subjectDN` MAY be omitted.

3.1.2 Need for names to be meaningful

Certificates issued for testing purposes SHALL be clearly identified as such in the `subjectDN`.

[ETSI] `commonName` in Sub CA certificates SHALL include a common name of the TSP (not necessarily the full registered name) and be chosen in a language common to the TSP's market.

In certificates issued to natural persons in association with an organization, the certificate attributes `organizationName`, `organizationalUnitName` and `organizationIdentifier`, if set, SHALL reflect the organization but the subject in the certificates SHOULD otherwise be the natural person.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

The `subjectDN` of all certificates issued by a CA SHALL be unique and assigned to one subscriber each. However, multiple certificates with the same `subjectDN` MAY be issued for one subscriber.

[DVCP] An exception to this is the `subjectDN` in domain-validated certificates. Here, a `subjectDN` MAY also be assigned to another subscriber if the subscriber has proven his legal ownership of the domain.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

[TLS] Trademarks, trade names or DBAs SHALL NOT be included in the `subjectDN` in certificates issued by Telekom Security.

3.2 Initial identity validation

Either direct evidence or attestations from appropriate and authorized sources SHALL be used to initially validate the identity of a natural person or an organization.

Evidence MAY be submitted in paper form or electronically.

The authenticity of the evidence provided SHALL be checked for alteration and falsification to the extent possible.

Only evidence necessary for verification of identity MAY be requested. Applicants SHOULD be advised to obscure non-required information in submitted supporting documentation (e.g., non-required data fields in copies of identity documents).

The information collected from the subscribers and, if applicable, any deviating applicants, as well as its validation SHALL be described in the CPSs.

3.2.1 Method to prove possession of private key

No stipulation.

[TLS] As part of the application process, an electronic certificate request in PKCS#10 format ("Certificate Signing Request", CSR) SHALL be submitted as proof of possession of the private key, containing at least one domain name or IP address to be included in the certificate.

[3145] For key pairs generated by the subscriber, at least the public key and the subject attributes SHALL be signed with the private key.

3.2.2 Authentication of organization identity

The methods for authenticating the identity of organizations SHALL be described in the CPS.

To verify the relevant data of a Private Organization or a Business Entity, one of the following independent sources SHOULD be queried:

- Government registers, e.g. commercial registers, registers of associations, directories of foundations, etc. ("QGIS", Qualified Government Information Source)
- Data from independent third parties that are considered reliable data sources, e.g. Dun&Bradstreet ("QIIS", Qualified Independent Information Source)

Alternatively, the correctness of the data MAY also be certified in writing by a trustable third party (e.g. notary, lawyer, auditor) ("VPL", verified professional letter).

In the case of Government Entities, the above-mentioned QGIS or QIIS MAY also be used to verify the relevant data. Alternatively, the correctness of the data MAY also be confirmed by an official attestation of the entity itself or of an entity superior to it.

Authentication of the identity of non-commercial Organizations SHALL be done via appropriate methods, considered on a case-by-case basis.

As an alternative to the methods listed above, authentication of the identity of all organization types MAY also be done through an on-site visit by an authorized representative of the TSP.

[OVCP] The identity of an organization SHALL be validated through the sources listed above.

[NCP] In addition to the methods listed above, to authenticate the identity of an organization, the applicant SHALL be identified according to a method for [NCP] listed in Section 3.2.3. In addition, if the applicant is not a direct representative of the organization, the applicant's authorization SHALL be verified according to Section 3.2.5.

[EVCP] QGIS, VPL, or official attestations SHALL be used to authenticate the identity of an organization.

Furthermore, the requirements mentioned above regarding the identification and, if applicable, authorization of the applicant according to [NCP] apply. Provided that the organization is of the type "Business Entity", the application SHALL be submitted by the Principal Individual of the organization and this Principal Individual SHALL be identified as described above.

Sufficient information about the QGIS used, such as name, jurisdiction, and website, as well as the allowed values to the attributes listed below and to be included in the certificates, SHALL be published :

- `jurisdictionOfIncorporationLocalityName (1.3.6.1.4.1.311.60.2.1.1)`
- `jurisdictionOfIncorporationStateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2)`
- `jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3)`

This information SHALL be published online, including version history, in an appropriate and easily accessible manner. The CPS SHALL describe in Section 3.2 where this information is published.

[QCP-l] [QEVCP-w] [QNCP-w] Analogously, the requirements mentioned above for [NCP] apply, but the methods applicable to [QCP-n] according to Section 3.2.3 SHALL be used to identify the applicant.

Alternatively, the following methods MAY also be used to authenticate the identity and relevant attributes of an organization, if applicable:

- Verification of a qualified electronic seal of the organization to be identified by means of its qualified seal certificate, which in turn is not issued on the basis of a verification of a qualified electronic seal of this organization.
- Use of a method confirmed as equivalent by a conformity assessment body and which is recognized at national level.

3.2.3 Authentication of individual identity

The methods for authenticating the identity of natural persons SHALL be described in the CPS.

[NCP] [3145] The identity of a natural person as applicant or subscriber SHALL be verified either directly, in the physical presence of the person, by presenting an official identification document, or indirectly, by using means that provide security equivalent to physical presence.

The identity of a natural person as a subscriber MAY alternatively be verified by an authorized representative upon presentation of a legible copy of a valid official identification document of the subscriber. In this case, the identity of the representative SHALL additionally be verified according to one of the methods above as well as his authorization according to Section 3.2.5.

[IVCP] [SMIME] The identity of a natural person as a subscriber SHALL be verified at least by means of a legible copy of a valid official identification document.

[QCP-n] Analogously, the requirements above for [NCP] apply, but one of the following methods SHALL be used to identify the applicant if this is not done in direct physical presence:

- Remote identification by means of an electronic identification means notified according to [eIDAS#9] with the security level "substantial" or "high" according to [eIDAS#8].
- Verification of a qualified electronic signature of the person to be identified by means of his qualified signature certificate, which in turn is not issued on the basis of a verification of a qualified electronic signature of this person.
- Use of a method confirmed as equivalent by a conformity assessment body and which is recognized at national level.

3.2.4 Non-verified subscriber information

The CPS SHALL specify information used but not verified, if applicable.

3.2.5 Validation of authority

To validate an authorization to apply for and manage certificates on behalf of a natural person or an organization, a legally valid signed power of attorney SHALL be obtained from the natural person or organization to be represented:

- In the case of representation of a natural person who is not related to an organization, a power of attorney from the natural person.
- In the case of representation of an organization or a natural person in association with an organization, a power of attorney of the organization.

[EVCP] Alternatively, to validate an authorization to sign or approve certificate requests, confirmation MAY be obtained from an authorized representative of the organization via a verified communication method.

3.2.6 Criteria for interoperation

No stipulation.

[TLS] All cross-certificates in which Telekom Security is included as the subject SHALL be published, provided that Telekom Security has initiated or accepted these cross-certifications.

3.2.7 Validation of control over a domain or IP-address

No stipulation.

[TLS] Each fully qualified domain name (FQDN) to be included in a certificate SHALL be validated as follows:

- If the FQDN is not an onion domain name, the FQDN SHALL be validated using one of the following methods described in more detail in [BR#3.2.2.4]:
  - Email, fax, SMS, or mail to the domain contact in accordance with [BR#3.2.2.4.2]
  - Constructed email to the domain contact in accordance with [BR#3.2.2.4.4]
  - DNS change in accordance with [BR#3.2.2.4.7]
  - IP address validation in accordance with [BR#3.2.2.4.8]
  - Validation of the applicant as a domain contact in accordance with [BR#3.2.2.4.12]
  - Email to the DNS CAA email contact in accordance with [BR#3.2.2.4.13]
  - Email to the DNS CAA TXT record email contact in accordance with [BR#3.2.2.4.14]
  - Telephone call to the domain contact in accordance with [BR#3.2.2.4.15]
  - Telephone call to the DNS TXT Record contact in accordance with [BR#3.2.2.4.16]
  - Telephone call to DNS CAA contact in accordance with [BR#3.2.2.4.17]
  - Agreed change of web page v2 in accordance with [BR#3.2.2.4.18]
  - Agreed change of web page ACME in accordance with [BR#3.2.2.4.19]
  - TLS using ALPN in accordance with [BR#3.2.2.4.20]
- If the FQDN is an onion domain name, the FQDN SHALL be validated in accordance with [BR#Appendix B].

After a successful validation of an FQDN according to one of the methods from [BR#3.2.2.4] listed above, the validation of further FQDNs or Wildcard Domain Names ending with the domain labels of the validated FQDN MAY be omitted. This does not apply to validations according to [BR#3.2.2.4.8], [BR#3.2.2.4.18], [BR#3.2.2.4.19] and [BR#3.2.2.4.20].

For each Wildcard Domain Name to be included in a certificate, it SHALL be verified that the FQDN part is of type "registry-controlled" or "public suffix". A regularly updated "public-suffix-list" (PSL) MAY be used for this check. If such a PSL is used for checking, only the "ICANN domains" SHOULD be accepted.

Validation of control over an IP address SHALL be performed according to one of the following methods described in more detail in [BR#3.2.2.5]:

- Agreed upon change to the web site in accordance with [BR#3.2.2.5.1]
- Email, fax, SMS, or mail to the IP address contact in accordance with [BR#3.2.2.5.2]
- Reverse address lookup in accordance with [BR#3.2.2.5.3]
- Phone call to IOP address contact in accordance with [BR#3.2.2.5.5]
- ACME "http-01" method for IP addresses in accordance with [BR#3.2.2.5.6]
- ACME "tls-alpn-01" method for IP addresses in accordance with [BR#3.2.2.5.7]

In order to prevent the use of IP addresses assigned in countries other than the actual location of the applicant, a proxy server verification procedure SHOULD be implemented.

The methods used according to [BR#3.2.2.4] or [BR#3.2.2.5] SHALL be listed in the CPSs including a reference to the relevant Section of the [BR].

3.2.8 Validation of control over an email address

No stipulation.

[SMIME] Appropriate and secure methods SHALL be used to verify the applicant's control over the email address referenced in the certificate or the applicant's authorization to act on behalf of the actual owner of the email address. After a successful validation of the Authorization Domain Name (ADN, according to [BR]) of the domain portion of email addresses of an organization, the validation of sub-domains of this ADN MAY be waived when validating further email addresses of this organization. The verification methods used SHALL be described in the CPSs.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The requirements according to Section 3.2 apply. Existing evidence MAY be reused for the validation of identity, taking into account the applicable legal situation and the remaining validity of the evidence (see Section 4.2.1).

3.3.2 Identification and authentication for re-key after revocation

Revoked certificates SHALL NOT be renewed. After a revocation, a new certificate SHALL be requested and validation SHALL be performed as for the initial request.

3.4 Identification and authentication for revocation request

The methods for identification and authentication of revocation requests SHALL be described in the CPSs.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The requirements of this Section SHALL be implemented for all certificates, including certificates issued by the TSPs for themselves or their employees.

Unless explicitly stated otherwise, the requirements apply to the certificates of all hierarchy levels.

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

The persons entitled to apply for certificates as well as their possible roles SHALL be described in the CPSs.

To avoid conflicts of interest, the TSPs SHALL NOT be the applicants for subscriber certificates. This excludes organizations that perform registration activities and issue certificates for themselves or persons associated with them. Exceptions SHALL be described in the CPSs.

4.1.2 Enrollment process and responsibilities

The application processes including the interfaces to be used SHALL be described in the CPSs.

From applicants shall be requested:

- a physical address or other contact information
- any attributes to be included in the certificate in the `subjectDN` or `subjectAltName`

This data SHALL either be provided by the applicant at the time of application or confirmed by the applicant after querying reliable sources.

Before entering into a contractual relationship with a subscriber, the subscriber SHALL be informed about the Terms of Use for the use of the certificates according to Section 9.6.3 and

- a confirmation of knowledge and acceptance of the Terms of Use,
- a consent to the recording of the data collected in the certificate management process, and
- if applicable, a statement regarding the publication of the certificate

shall be obtained from the subscriber.

Note: If the subscriber and the subject of a certificate are different persons or organizations and the subject of the certificate is not a device, both persons/organizations SHALL accept certain parts of the Terms of Use, for details see Section 9.6.3.

Certificate applications MAY be submitted in electronic form. In this case, however, the applications, including acceptance of the Terms of Use, SHALL be confirmed by a traceable action (e.g. checking a box in the web application form) or signed electronically.

[EVCP] If not all required information is included in an application, the missing information SHALL be confirmed by the Certificate Approver or Contract Signer.

[QCP] Electronically submitted certificate applications SHOULD be provided with at least an advanced electronic signature or an advanced electronic seal.

[VS-NfD] The application process SHALL be released by the security officer.

4.2 Certificate application processing

Certificate applications SHALL be checked for correctness, completeness and authorization.

The manual processing steps listed below SHALL be performed by trusted personnel (see also Section 5.2.1).

The processing of applications or parts thereof MAY be outsourced to external RAs. In this case, it SHALL be ensured that the process as a whole meets the requirements of this CP. Accordingly, the external RAs SHALL be identified and authenticated and it SHALL be ensured that information is securely exchanged between the external RAs and the TSP.

[TLS] This excludes validation over control of a domain or IP address according to Section 3.2.7, which SHALL be performed by the TSP itself.

[SMIME] This excludes the validation of the Authorization Domain Name (according to [BR]) of the domain part of the email address, which SHALL be performed by the TSP itself.

4.2.1 Performing identification and authentication functions

The subjects of the certificates and, if different, the applicants SHALL be identified and authenticated according to the methods described in Section 3.2. The processes and specifications for performing identification and authentication including verification of all data requested by the applicant for inclusion in the certificate SHALL be described in the CPSs.

If the subject of a certificate is a natural person, then the following SHALL be validated:

- Full name of the person
- Date and place of birth or reference to an official identity document or other attributes that can be used for unique identification

If the subject of a certificate is a natural person identified in association with an organization, then the following SHALL additionally be verified:

- Full name and legal status of the organization
- Relevant registration information of the organization
- Affiliation of the natural person with the organization
- Confirmation by the organization and the natural person that the attributes also identify the organization

If the subject of a certificate is an organization, the following SHALL be verified:

- Full name of the organization to be included in the certificate
- Any relevant registration information of the organization, including a nationally recognized identity number or other attributes that can be used to distinguish the organization as much as possible from others with the same name
- If applicable, the organization's affiliation with the organizational unit identified in association with that organization

If the subject of a subscriber certificate is a device or system operated by a natural person or an organization, then the identifier of the device or system (e.g., Internet domain name) SHALL additionally be verified.

[TLS] [SMIME] All information to be included in a certificate SHALL be verified.

[TLS] A validation performed MAY be used to issue further certificates within the following time periods:

- Validations of data according to Section 3.2 (without Section 3.2.7): 825 days
- Validations according to Section 3.2.7: 398 days

[IVCP] To verify the authenticity of an application, confirmation SHALL be obtained from the applicant via a verified method of communication.

[OVCP] As part of the validation of the organization's identity according to Section 3.2.2, the organization's address SHALL also be verified.

To verify the authenticity of an application, confirmation SHALL be obtained via a verified method of communication with an entity of the organization that is considered reliable.

Organizations SHALL be offered the opportunity to nominate authorized persons to apply for certificates. If an organization has designated eligible individuals in writing, applications SHALL NOT be accepted from individuals other than the designated individuals. Upon written request from an organization, a list of the organization's designated eligible individuals SHALL be provided.

[3145] When validating an identity, it SHALL be checked whether the subscriber has already been registered before. In this case, all further certificates SHALL be assigned to the registered subscriber, so that in case of suspension of the subscriber, all certificates of this subscriber can be suspended or revoked simultaneously according to the Terms of Use.

[VS-NfD] The subscriber's security clearance SHALL be verified with respect to the use of the PKI.

[EVCP] As part of the authentication of the organization's identity according to Section 3.2.2, the type of organization SHALL also be defined and its legal, physical and operational existence SHALL be verified. The verification of the legal existence also includes, if applicable, the verification or acquisition of registration numbers or dates of incorporation, representative authorities or persons in charge and, if applicable, relationships between organizations and parent or subsidiary companies or shareholdings. The verification of physical and operational existence also includes the verification of the organization's address.

Furthermore, it SHALL be verified that the application is signed by an authorized Contract Signer and an authorized Certificate Approver. For this purpose,

- their authorization according to Section 3.2.5 SHALL be verified, if they are not directly authorized to represent the organization,
- it SHALL be verified via a verified method of communication, that the signatures were actually executed by these designated persons in the assigned roles.

As an alternative to the handwritten signature of the application by the Contract Signer and the Certificate Approver, the following methods MAY also be accepted:

- advanced or qualified electronic signatures of the persons mentioned above
- confirmation by the persons mentioned above via a web front-end, provided that they have been appropriately registered before and authenticate themselves via a secure procedure on the web front-end.

In these cases, the additional confirmation of the signature provided by means of verified communication MAY be waived.

After successful completion of all validations, a thorough cross-check of all validations performed SHALL be performed by another RA employee who was not involved in the validations themselves.

Validations performed according to chapter 3.2 MAY be used for the issuance of further certificates, but the validations SHALL NOT have been performed longer than 398 days prior to the issuance of the certificate.

4.2.2 Approval or rejection of certificate applications

Applications MAY only be approved after successful identification and authentication in accordance with Section 4.2.1.

If a key generated by the subscriber is submitted for an application, the possession or control of the private key SHALL be checked. In the case of a key being submitted in the form of a PKCS#10 request, its signature SHALL be checked. In addition, it SHALL be checked whether the presented key meets the requirements of Sections 6.1.5 and 6.1.6. In case of a negative verification result, the application SHALL be rejected.

[QCP-l-qscd] [QCP-n-qscd] If a key is submitted that is not guaranteed to be from a key pair generated in a QSCD, the application SHALL be rejected.

[3145] Certificate requests from suspended subscribers SHALL be rejected.

[TLS] If a key is submitted in an application whose corresponding private key

- was demonstrably generated by means of a faulty method or
- can be easily calculated with a proven or established method, e.g. if it is a "Debian weak key" or
- is known to be compromised or
- was previously generated by the TSP,

the application SHALL be rejected.

Within 8 hours before issuing a certificate, it SHALL be checked for each domain name to be included in the certificate whether the TSP is listed as an authorized issuer in the CAA records as follows:

- For requests for certificates with one or more FQDN: in the "issue" field of each FQDN
- For requests for certificates with wildcards: in the "issuewild" field of the FQDN part

The certificate MAY only be issued if the TSP is listed with one of its issuer domain names in the fields above or if the fields above are empty.

After a failed query of a CAA record, a certificate MAY still be issued if

- the error is outside the infrastructure of the TSP,
- the query has been repeated at least once and
- the zone of the domain does not have a DNSSEC validation chain to the ICANN root.

In Section 4.2 of the CPSs the issuer domain names accepted by the TSPs SHALL be listed.

If this check has been performed for a pre-certificate that has been logged in at least two CTLog servers, then a recheck MAY be omitted when issuing the corresponding leaf certificate. Likewise, the CAA check MAY be omitted if the issuer of the certificates is a technically constrained Sub CA with corresponding name restrictions and the omission of the CAA check was explicitly agreed in the contract with the subscriber.

Where applicable, additional required validations for "high risk certificate requests" SHALL be implemented and described in the CPS.

In addition, it SHALL be verified that both the applicant organization and the acting persons are not included in the denied lists to be considered.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The integrity and authenticity SHALL be ensured with appropriate (technical, organizational or personnel).

The process of issuing the certificates SHALL be securely linked to the associated registration and, to the public key provided by the applicant resp. the keys generated by the TSP.

4.3.1.1 CA certificate issuance

CA certificates SHALL be issued in the secure environment of the Trust Center during a ceremony. The roles involved as well as their tasks and responsibilities before, during and after the ceremony SHALL be defined and documented.

The individual steps of the ceremony SHALL follow a defined protocol and SHALL be documented in it.

The issuance SHALL be performed by at least two trusted employees of the Trust Center, and the following requirements apply:

- Each of the two employees SHALL have knowledge of only a portion of the activation data required for certificate issuance.
- The two employees SHALL act in different roles.

When issuing Sub CA certificates, the hash value of the public key or the CSR containing the public key SHALL be verified to prove the authenticity and integrity of the key.

An internal auditor (see Section 8.2) SHALL monitor the ceremony and confirm its correct execution in the protocol.

[TLS] [SMIME] Both an internal and a qualified external auditor (see Section 8.2) SHALL monitor the ceremony and confirm its correct execution in the protocol. In addition, the external auditor SHALL confirm in his report that all requirements have been met and that the integrity and confidentiality of the keys have been maintained.

4.3.1.2 Subscriber certificate issuance

In the case where the keys for the subscribers are generated by a TSP, the confidentiality of the keys SHALL be ensured in the generation process.

[TLS] Subscriber certificates

- SHALL be verified by appropriate lint tools and
- SHALL be published as "pre-certificates" in a sufficiently large number of CTLog servers (Certificate Transparency according to [RFC6962])

before issuance. The time-stamped confirmations returned from the CTLog servers SHALL be included in the “leaf certificates” as „Embedded Signed Certificate Timestamps“ (SCT). Regarding the number of CTLogs see Section 7.1.2.

[3145] If the use of cryptographic tokens is required

- it SHALL be ensured by technical measures that the supplied public key is correctly assigned to the token and the registration data,
- it SHALL be ensured that the correct public key of the selected token is included in the certificate and that the certificate is stored on the correct token,
- it SHALL be ensured that the personalized token is sent to the correct recipient,
- the handover of the token SHALL be designed in such a way that a token intercepted by an attacker cannot be used, e.g. by an activation required to use the token, which can only be performed by the authorized recipient using activation data passed to him via a separate channel.

[VS-NfD] The specifications from [VSA] SHALL be considered for the protection of the keys according to their classification.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Subscribers SHALL be informed about the issuance of the certificates.

If applicable, the certificates SHALL be handed over to the subscribers in a usable form, eventually at a later date.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

Certificates MAY be published with the consent of the subscriber but they SHALL NOT be published without consent.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

[TLS] CA certificates SHALL be published in the CCADB, subscriber certificates resp. the corresponding pre-certificates in multiple CTLog servers (see Section 4.3.1).

4.5 Key pair and certificate usage

4.5.1 Private key and certificate usage

The purposes of use of the private keys and certificates SHALL be described in the CPSs.

[QCP-n-qcsd] [QCP-l-qcsd] If a TSP manages a subscriber's QSCD, the use of the private key SHALL be restricted to the generation of electronic signatures or electronic seals.

4.5.2 Relying party public key and certificate usage

Relying parties SHOULD comply with the requirements for the use and verification of certificates and public keys set out in the Terms of Use.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

The circumstances under which a renewal is allowed SHALL be defined in the CPSs. Among others, the aspects of key weakening as well as the requirement for sufficient key lengths and permissible algorithms until the end of the validity of the new certificate, SHALL be considered.

Certificates SHALL NOT be renewed if they have been revoked.

Certificates SHALL NOT be renewed if any information in the certificates has changed.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

If the current Terms of Use have been changed from the Terms of Use in effect at the time the preceding certificate was applied for, acceptance of these new Terms of Use SHALL be obtained from the subscriber prior to issuance of a new certificate.

Prior to renewal, the validity of the preceding certificate and the original submitted identification data and attributes of the subject SHALL be verified. Applications SHALL be complete, accurate, up-to-date, and authorized.

4.6.4 Notification of new certificate issuance to subscriber

See Section 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

See Section 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

See Section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

See Section 4.4.3.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

The circumstances under which re-keying is permitted SHALL be described in the CPSs.

Re-keying SHALL NOT be allowed for certificates that have been revoked.

Re-keying SHALL NOT be allowed if any information in the certificates has changed.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

If the current Terms of Use have been changed from the Terms of Use in effect at the time the preceding certificate was applied for, the new Terms of Use SHALL be accepted by the subscriber before issuing a new certificate.

Prior to re-keying the validity of the expiring certificate and the original submitted identification data and attributes SHALL be verified. Applications SHALL be complete, accurate, up-to-date, and authorized.

[EVCP] In the new certificate, the same expiration date and `subjectDN` SHALL be set as in the preceding certificate

4.7.4 Notification of new certificate issuance to subscriber

See Section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See Section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

See Section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

See Section 4.4.3.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

The circumstances under which a modification of certificate data is allowed or required SHALL be described in the CPSs.

If the original key is to be reused when modifying certificate data, the aspects of key weakening and the requirement for sufficient key lengths and permissible algorithms until the new certificate expires, SHALL be considered.

If there is suspicion or evidence of compromise of the key or the preceding certificate has been revoked due to a security incident, the key SHALL NOT be reused.

Subscribers SHALL be required to notify the TSP of the change of registered data in the validity period of the certificates issued based on the registered data. Subscribers SHALL be informed about the processes in case of change of certificate data.

4.8.2 Who may request certificate modification

See Section 4.1.1.

4.8.3 Processing certificate modification requests

If the current Terms of Use have been changed from the Terms of Use in effect at the time the preceding certificate was applied for, the acceptance of these new Terms of Use SHALL be obtained from the subscriber before issuing a new certificate.

Before modifying certificate data, the validity of the expiring certificate and any unmodified subject identification data and attributes originally submitted SHALL be verified. Modified information SHALL be validated and registered according to Section 3.2. The data SHALL be complete, accurate, up-to-date, and authorized.

[3145] The generation of new keys SHALL be enforced.

4.8.4 Notification of new certificate issuance to subscriber

See Section 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

See Section 4.4.1.

4.8.6 Publication of the modified certificate by the CA

See Section 4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

See Section 4.4.3.

4.9 Certificate revocation and suspension

Subscribers SHALL be informed about the revocation reasons as well as the available interfaces for requesting revocation in the Terms of Use.

Agreements SHALL be made with the RAs authorized to revoke, describing the reasons for revocation and the available interfaces for requesting revocation.

Note: The requirements listed below do not apply to "short-term certificates" marked by the extension `id-etsi-ext-valassured-ST-certs if` these are generally not revoked due to their short validity (less than the revocation period according to Section 4.9.5).

If such short-term certificates are issued, it SHALL be described in the CPSs which certificates are short-term certificates and how they are handled.

[TLS] [SMIME] The requirements listed below also apply to pre-certificates, if applicable.

4.9.1 Circumstances for revocation

In addition to the revocation reasons listed below, additional revocation reasons MAY be specified in the CPSs.

4.9.1.1 Reasons for revoking a Sub CA certificate

A Sub CA certificate SHALL be revoked if

- a written revocation request, even without giving reasons, has been made by the TSP,
- it is determined that the original certificate request was not authorized and cannot or should not be authorized retrospectively,
- it is determined that the private key of the Sub CA has been compromised or disclosed to an unauthorized person or organization or no longer complies with the requirements (see Section 6.1.5 and 6.1.6),
- it is determined that the certificate has been misused,
- it is determined that the Sub CA certificate has not been issued in compliance with this CP or that the operation is not in compliance with this CP,
- it is determined that any information in the certificate is incorrect or misleading,
- the operation of the Root CA or the Sub CA will be terminated and no arrangements have been made for the continuation of the revocation service,
- the right of the operator of the Root CA or Sub CA to issue certificates in accordance with the requirements of this CP expires or is revoked or terminated and no arrangements have been made for the continued operation of the revocation services.

4.9.1.2 Reasons for revoking a subscriber certificate

A certificate SHALL be revoked if

- an authorized revocation request, even without giving reasons, has been received from the subscriber or, if applicable, from the respective RA,
- relevant information in the certificate is not (or no longer) correct,
  Note: allowed deviations SHALL be described in the CPS.
- no authorization of the certificate exists (anymore), this includes:
  - an information from the subscriber is available that the original application was not authorized and cannot or should not be authorized retroactively
  - [TLS] control over a FQDN or IP address specified in the certificate can no longer be trusted
  - [TLS] the use of a FQDN or IP address specified in the certificate is no longer allowed
  - [SMIME] the use of an email address specified in the certificate is no longer permitted
- a key weakness or compromise is demonstrated, this includes:
  - the TSP is proven that the private key has been compromised or given to an un-authorized person
  - the TSP is proven that a weak private key is used, which can be easily computed based on the public key (e.g., "debian weak key") or generated using a flawed method or other methods are known to compromise the private key
  - the private key no longer meets the requirements according to Sections 6.1.5 and 6.1.6
- a violation of the CP, CPS or the Terms of Use is proven, this includes:
  - the certificate has not been issued in accordance with the relevant CPS
  - the certificate has been misused
  - [TLS] a wildcard certificate has been used to authenticate a fraudulently misleading Sub-FQDN
  - the subscriber has been suspended or revoked, as applicable

In addition, all affected certificates SHALL be revoked if

- the TSP ceases operation and has not taken precautions for continuing operation of the revocation services,
- the TSP loses the authorization to issue certain certificate types and has not taken precautions for continuing operation of the revocation services,
- the private key of a CA has been compromised or
- [QCP-l-qscd] [QCP-n-qscd] the certification of the QSCD used expires or the QCSDs have unacceptable security deficiencies.

4.9.2 Who can request revocation

The revocation of a Sub CA SHALL always be requested by an authorized representative of the operator of the Sub CA. If one of the revocation reasons listed in Section 4.9.1.1 is identified by or reported to Telekom Security as operator of the Root CA, the revocation MAY also be initiated by Telekom Security without an existing revocation request.

[3145] The revocation of a Sub CA in the scope of TR-03145 is not in the scope of this CP, since the Sub CA certificates are not issued by a Telekom Root CA. The revocation of the Sub CAs SHALL be performed according to the specifications of the responsible operator of the Root CA and SHALL be described in the CPS.

The revocation of a subscriber certificate SHALL be requested by the subscriber himself or a responsible RA. If one of the reasons for revocation listed in Section 4.9.1.2 is identified or reported by a third party and is verified by the TSP, the revocation SHALL be initiated by the TSP. The further organizational and procedural requirements SHALL be described in the CPSs.

[QCP-n] [QCP-l] If a certificate contains information about a third party's power of representation or profession-related or other information pursuant to [VDG§12], the third party or the body responsible for the profession-related or other information about the person MAY also request revocation if

- the power of representation or
- the prerequisites for the profession-related or other information on the person after being included in the qualified certificate

cease to exist.

[VS-NfD] In addition, subscriber certificates SHALL be revoked upon a justified request by the security officer.

4.9.3 Procedure for revocation request

For revocation of certificates of all hierarchy levels, permanently available interfaces (7x24h) for submitting revocation requests or problem messages, that may lead to the revocation of certificates, as well as guidelines for using the interfaces, SHALL be provided.

Revocation requests SHALL NOT be processed if they are not submitted by authorized applicants or are based on problem reports that are not verified as legitimate revocation reasons.

The subscriber and, if different, the applicant SHALL be informed, if possible, of the revocation.

Revoked certificates SHALL NOT be unrevoked again.

[VS-NfD] The processes for revoking certificates including the specified timelines SHALL be approved by the security officer.

4.9.4 Revocation request grace period

As soon as a revocation reason according to Section 4.9.1 is determined, a revocation request SHALL be submitted.

4.9.5 Time within which CA must process the revocation request

In addition to the time limits listed below, shorter time limits MAY be specified in the CPSs for certain revocation reasons.

Sub CA certificates SHALL be revoked within a reasonable period of time depending on the circumstances.

[TLS] [SMIME] Sub CA certificates SHALL be revoked within seven days after receipt of an authorized revocation request. This period includes the time to handover the revocation status to the certificate status services. After revocation of a Sub CA certificate, the corresponding entry in the CCADB SHALL be updated. If the revocation of the Sub CA certificate is required due to a security incident, the CCADB SHALL be updated within 24 hours, otherwise within 7 days.

Subscriber certificates SHALL be revoked as soon as possible, but no later than within 24 hours after receipt of an authorized revocation request. This period includes the time to handover the revocation status to the certificate status services.

This does not apply to revocations requested for a later date, e.g., due to a planned termination of participation. In this case, the desired date for revocation of the certificate listed in the revocation request MAY be set as the date of receipt of the authorized revocation request, provided that this procedure is described in the CPSs.

For revocations that are not based on authorized revocation requests but on other reasons for revocation listed in Section 4.9.1.2, the CPS SHALL specify the revocation periods.

[TLS] [SMIME] Certificates SHALL be revoked within 24 hours if a key weakness or compromise or a missing authorization of a certificate is proven or the TSP loses its authorization to issue certificates according to [BR].

Certificates SHOULD be revoked within 24 hours and SHALL be revoked within 5 days if a violation of the CP, CPS or Terms of Use is proven.

However, the TSP SHALL also be able, in justified cases, to revoke certificates on a date specified by a Root Store operator that deviates from the above deadlines.

The TSP SHALL be able to respond to high-priority problem messages 24 hours a day and, if necessary, forward a message to law enforcement authorities and/or revoke the certificates affected by the problem.

Within 24 hours of receipt of a problem report, the facts and circumstances SHALL be investigated and initial feedback on the findings available until then SHALL be provided to the subscriber and the reporting person. Subsequently, the results of the analysis SHALL be discussed with the subscriber and the reporting person and a decision SHALL be made as to whether a revocation is required.

If revocation is required due to a problem report, the timing of revocation SHALL be determined, taking into account the requirements mentioned above and considering the following aspects:

- the nature of the alleged problem (scope, context, severity, extent, damage potential)
- the effects of revocation (direct and collateral effects on subscribers and relying parties)
- the number of problem messages for a certificate or subscriber
- the entity that set the message
- the relevant legislation

4.9.6 Revocation checking requirement for relying parties

Relying parties SHOULD use the certificate status services according to Section 4.10 to check the status of certificates.

Relying parties MAY waive to check the status of short-term certificates.

4.9.7 CRL issuance frequency

Certification Authority Revocation Lists (CARLs) SHALL be updated within 24 hours after revocation of a Sub CA certificate and regularly at least every 12 months.

Certificate Revocation Lists (CRL) SHALL be updated regularly at least every 24 hours.

[3145] CRLs SHALL also be updated following the revocation of a subscriber certificate in addition to the regular issuance.

4.9.8 Maximum latency for CRLs

No stipulation.

4.9.9 On-line revocation/status checking availability

See Section 4.10.

4.9.10 On-line revocation checking requirements

Relying parties should consider the OCSP response processing specifications in [RFC6960] when checking a certificate status via OCSP.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements related to key compromise

No stipulation.

[TLS] [SMIME] Accepted methods for evidence of key compromise SHALL be described in the CPSs in Section 4.9.12.

Regarding the reporting of suspected key compromise, see Section 1.5.2.

4.9.13 Circumstances for suspension

No stipulation.

[TLS] Certificates SHALL NOT be suspended.

[3145] In addition to the revocation or suspension of certificates, subscriber SHALL also be suspended if it is determined that they are no longer fulfilling their obligations within the PKI, e.g., in the event of certificate misuse.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate status services

At least for the validity period of all issued Sub CA and subscriber certificates, authentic and integrity-assured certificate status services SHALL be provided in the form of revocation lists and/or OCSP information.

OCSP information SHOULD be provided for the subscriber certificates.

[TLS] [SMIME] Revocation lists and OCSP information SHALL be provided for Sub CA and subscriber certificates, this also applies to pre certificates.

[QEVCP-w] Certificate status services SHALL be provided beyond certificate validity, the providing time SHALL be described in the CPS. The integrity of the status information SHALL be guaranteed over the entire time period.

[QCP-n] [QCP-l] Certificate status services SHALL be provided over the entire time of operation of the trust service. The integrity of the status information SHALL be guaranteed over the entire time period.

4.10.1 Operational characteristics

Certificate status services (revocation lists and OCSP) SHALL be time-synchronized (UTC) at least every 24 hours.

If revocation lists and OCSP information are provided, they SHALL be consistent after 24 hours at the latest, taking into account the different update times of both methods. Differing update timelines, if any, SHALL be listed in the CPSs and a description SHALL be provided of how differing verification results are to be interpreted.

4.10.1.1 Operational characteristics for the provision of the OCSP responder

The OCSP responders SHALL be operated in conformance with [RFC6960].

Concretizing to [RFC6960], requests for certificates with unknown certificate serial numbers SHALL NOT be answered with the status `good`.

The response to be selected depends on the way the OCSP responder operates:

- For preproduced OCSP responses, such requests SHALL be answered with the error message `unauthorized`.
- For ad hoc generated OCSP responses such requests SHOULD be answered with the status `unknown`, they MAY also be answered with the status `revoked`, but then the extension `id-pkix-ocsp-extended-revoke` according to [RFC6960 #4.4.8] SHALL be set.

OCSP requests for unassigned serial numbers SHOULD be logged.

OCSP responses MAY be cached and reused within their validity[3] for further requests.

[TLS] [SMIME] OCSP responses to Sub CA certificates SHALL NOT exceed a maximum validity of 12 months. After a revocation of a Sub CA certificate, updated information SHALL be retrievable in the OCSP responder within 24 hours.

OCSP responses to subscriber certificates SHALL have a validity of at least 8 hours but no more than 7 days. However, they SHALL NOT exceed the validity period of the issuing Sub CA certificate or the OCSP Signer certificate included in the `certs` attribute of the OCSP response.

The following conditions apply to the update of OCSP responses:

- If OCSP responses have a validity of less than 16 hours, they SHALL be updated no later than halfway through their validity period.
- If OCSP responses have a validity of 16 hours or more, they SHALL be updated no later than 4 days after generation and no later than 8 hours before expiration.

[QCP-n] [QCP-l] A validity end MAY be set.

4.10.1.2 Operational characteristics for the provision of revocation lists

All revocation lists SHALL be valid[4] beyond the time of the next regular update.

The validity period of a last revocation list to the certificates in its scope SHOULD be set to `99991231235959Z`.

Revoked certificates MAY in principle be removed from the CRLs after expiring, but they SHALL still be in the next regular CRL after their expiry date.

[TLS] [SMIME] CARLs SHALL NOT exceed a validity of 12 months. CRLs SHALL NOT exceed a validity of 10 days.

[3] "validity" in this context refers to the specification of a date in the attribute `nextUpdate`, i.e. the time at which a new status information can be retrieved via OCSP at the latest.
[4] "validity" in this context refers to the specification of a date in the attribute `nextUpdate`, i.e. the time at which a new revocation list can be retrieved at the latest.

[QCP] If CRLs and OCSP information are provided, expired certificates SHOULD NOT be removed from the revocation list. If only CRLs are provided, expired certificates SHALL NOT be removed from the CRLs.

If CRLs are provided, a final CRL SHALL NOT be issued until all certificates in its scope have expired or been revoked.

4.10.2 Service availability

The certificate status services SHALL be available 7x24h. In case of an incident, the greatest possible efforts SHALL be made to eliminate the incident within the specified service level agreements.

[TLS] [SMIME] Sufficient capacity SHALL be provided to ensure that the response time does not exceed 10 seconds under normal operating conditions.

[3145] [NCP] The maximum downtime of the systems SHALL be specified in the CPSs.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

If key escrow is offered,

- encryption keys MAY be escrowed,
- authentication keys and signature keys SHALL NOT be stored in a form that allows decryption of these keys without control of the subscriber,
- it SHALL be ensured that all copies of the private keys are subject to the same security level as the original and are only handed over to authorized recipients,
- only the necessary number of copies of the private keys to ensure continuity SHALL be created,
- a private key used by the TSP or a specified role to decrypt the escrowed keys SHALL NOT be used for other purposes.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT AN OPERATIONAL CONTROLS

The approach to information security management SHALL be defined in an information security policy approved by management and an appropriate information security management system (ISMS, e.g., following ISO 27001) SHALL be established that, among other things,

- manages the development, implementation and maintenance of security concepts including regular risk analyses for the Trust Services,
- inventories the information and classifies it according to the risk management,
- is involved in change management for security-critical changes und
- includes regular auditing of the Trust Services.

The information security policy SHALL be reviewed and communicated to all employees on a regular basis as well as when needed.

The security concepts SHALL meet the following requirements:

- Protection of the confidentiality, integrity and availability of the certificate data and the certificate management process
- Protection against possible threats and hazards to the confidentiality, integrity and availability of certificate data and the certificate management process
- Protection against unauthorized or unjustified access, use, disclosure, substitution or destruction of certificate data or the certificate management process
- Protection against loss or malicious destruction of certificate data or manipulation in the certificate management process
- Compliance with legally required security needs

The security concepts SHALL in particular take into account the following aspects:

- Physical security (building and environment)
- Integrity protection of systems (including configuration management) and trusted code used
- Malware detection and prevention
- Network security and firewall management
- User and role management including the processes for assigning trusted roles
- Employee training, awareness and education
- Logical access control
- Logging
- Automatic locking of workstations in case of inactivity

Risk analyses, that identify, analyze, and assess foreseeable internal and external threats that could lead to unauthorized access, disclosure, misuse, exchange, or destruction of certificate data or the certificate management process, SHALL be performed on an annual basis.

The risk analyses SHALL consider the probabilities and potential damages of these threats, taking into account the sensitivity of the certificate data and the certificate management process, and assess the adequacy of the policies, procedures, information systems, technologies, and other precautions taken to address the threats.

Based on the risk assessment, appropriate and adequate risk management measures (e.g., structural, organizational, personnel and state-of-the-art technical security measures) SHALL be developed and their implementation shall be managed and controlled by the ISMS.

The risk assessment and any residual risks identified SHALL be approved by the management.

[VS-NfD] Before IT systems are used for VS-NfD, they SHALL be checked for compliance with the required classified security protection measures according to [VSA].

5.1 Physical controls

In order to prevent loss, theft, damage, or compromise of assets, media, and information, physical measures SHALL be taken.

5.1.1 Site location and construction

Systems SHALL be operated in appropriate locations in secure premises with adequate physical protection. Potential natural disasters (e.g., floods) as well as disaster recovery SHALL be considered when selecting locations.

If premises are shared with other organizations, the other systems SHALL be operated outside the area where the TSP's CA and status service systems are operated. The different areas SHALL be separated from each other by appropriate physical barriers.

The TSP's systems MAY be operated in different security zones according to the criticality resulting from the risk assessment or the security requirements assigned. In particular, the Root CA's systems SHALL be operated in a high-security zone, separated from regular operations.

[VS-NfD] The instructions for the protection of VSIT rooms according to § 29 VSA [VSIT] SHALL be considered as guidance.

5.1.2 Physical access

Access to the rooms, where the TSP's systems are operated, SHALL be restricted to authorized persons in trusted roles via appropriate access controls. Where non-authorized persons require access to these rooms, they SHALL always be accompanied by an authorized person.

The rooms where the TSP systems are operated SHALL have an intrusion alarm system to detect unauthorized entry.

The granted access authorizations SHALL be checked regularly.

5.1.3 Power and air conditioning

Uninterruptible power supply as well as air conditioning of the systems according to the criticality resulting from the risk assessment as well as the agreed service levels SHALL be ensured.

5.1.4 Water exposures

The rooms in which components of the TSP are operated SHALL be protected from water exposure according to the criticality resulting from the risk assessment.

5.1.5 Fire prevention and protection

The rooms in which components of the TSP are operated SHALL be protected against destruction by fire according to the criticality resulting from the risk assessment.

5.1.6 Media storage

Measures SHALL be taken to protect against accidental use outside the secured environment, damage, theft, unauthorized access, and obsolescence of the relevant TSP media. These measures SHALL take into account the retention period of the media. All media SHALL be handled securely according to the classification of the information stored on it.

5.1.7 Waste disposal

In order to prevent unauthorized use or access to information, secure disposal processes SHALL be established. In particular, media containing sensitive data SHALL be disposed of securely when no longer needed.

5.1.8 Off-site backup

No stipulation.

5.2 Procedural controls

5.2.1 Trusted roles

To ensure secure operation, the TSP SHALL have an appropriate organization that includes at least the following trusted roles:

- Head of Trust Center: has the overall responsibility for the services of the TSP
- Head of qTSP: is the contact and information person for the national supervisory authorities for the qualified Trust Services
- Solution Manager: is responsible for and manages a Trust Service
- Trust Center Information Security Officer: plans and monitors the implementation of security controls
- Registration staff/Validation Specialist: reviews and processes applications for certificate-issuance, -suspension, -revocation or -renewal
- Administrator: installs, configures and maintains the systems of the Trust Services
- Internal Auditor: checks for example log data, databases and paper-based documentation of the Trust Services on a regular basis as well as in case of discrepancies

The relevant roles including an overview of the assigned activities SHALL be described in the CPSs.

5.2.2 Number of persons required per task

At least one substitute SHALL be appointed for all roles listed in Section 5.2.1.

Security-relevant or -critical activities, such as generation, backup and recovery of CA keys, SHALL be performed in dual control by persons in trusted roles. The number of employees performing such security-relevant or -critical activities SHALL be kept to a minimum.

The security-relevant and -critical activities for which a dual control principle (or more) is required SHALL be described in the CPSs.

[EVCP] Certificate applications SHALL be validated and approved using the dual control principle, see Section 4.2.1. In order to ensure the dual control principle, auditable security controls SHALL be implemented.

5.2.3 Identification and authentication for each role

The identification of suitable persons to fill roles, the transfer of roles, and their withdrawal SHALL follow a documented process.

Role owners SHALL be officially appointed to the trusted role by the management of the TSP.

Prior to the delegation of a trusted role, acceptance to the delegation of the role and its associated responsibilities, as well as the resulting duties to ensure security, SHALL be obtained from the individual to whom the role is to be delegated.

Furthermore, it SHALL be ensured that no conflicts of interest arise from the assignment of a role and that independence is maintained, i.e., that

- the areas entrusted with generating and revoking certificates SHALL be independent of other organizations in their decisions to establish, provide, maintain, and suspend Trust Services in accordance with applicable certificate policies,
- that all employees involved in certificate generation and revocation SHALL be free from financial or other pressures in the performance of their tasks that could affect trust in the Trust Services. This applies to all employees in trusted roles as well as senior managers and executives.

The structure that ensures impartiality of operation SHALL be documented.

Role owners SHALL be made aware that they may only act in the assigned role when performing tasks assigned to the role.

The assignment of the required permissions SHALL follow the "least privilege" principle, i.e., all permissions SHALL be limited to the required minimum.

Upon termination of employment of an employee in a trusted role, his access privileges SHALL be revoked within 24 hours.

If trusted roles or parts thereof are transferred to third parties (e.g., external RAs, see Section 1.3.2), responsibilities and regulations SHALL be clearly defined and corresponding agreements SHALL be made to ensure that all regulations specified by the TSP are also complied with by the third parties.

5.2.4 Roles requiring separation of duties

Conflicting duties and responsibilities SHALL be separated from each other.

The following roles SHALL be separated:

- Head of Trust Center and/or Head of TSP
- Trust Center Information security officer and/or internal auditor
- Registration staff
- Administrator

In addition, the persons in the roles above SHALL NOT also be applicants for subscriber certificates. Exceptions to this are

- applications for the TSP's own certificates and certificates for the TSP's employees,
- applications for an organization's own certificates that operates an external RA, as well as certificates for that organization's employees.

Exceptions SHALL be described in the CPSs.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The management of the TSP SHALL have

- experience or training related to the Trusted Services,
- familiarity with security procedures for personnel with security responsibilities, and
- experience with information security and risk assessment sufficient to perform management functions.

TSP employees SHALL have sufficient expert knowledge and qualifications to perform their tasks based on their experience and/or appropriate training. In addition, the employees SHALL be adequately trained on general security and data protection regulations as well as the specific requirements of the TSP's ISMS for the performance of their tasks.

5.3.2 Background check procedures

Before hiring a person, their identity and trustworthiness SHALL be verified.

[EVCP] Identification of persons to be entrusted with a trusted role SHALL be done face-to-face and by presenting an official identification document and a background check SHALL be done, that includes checking of

- previous employment,
- professional references,
- educational qualifications, and
- an official certificate of good conduct.

[QCP] The reliability of personnel SHALL be verified by regular submission of official certificates of good conduct.

[3145] It SHALL be ensured that individuals, who are to be entrusted with critical or security-related processes have successfully completed a security check. If the security check reveals that a person has been convicted to a crime, that affects his suitability for the intended role, that person SHALL NOT be entrusted with that role.

[VS-NfD] The above-mentioned security check according to [3145] SHALL be done according at least to [SÜG] level “Ü2 / Sabotageschutz”.

5.3.3 Training requirements

See Section 5.3.1.

[TLS] All registration staff SHALL be trained on the following topics:

- basic knowledge of PKI, authentication and verification policies and procedures
- common threats to the information verification process, including phishing and social engineering
- relevant CP and CPSs as well as the [BR] and the [EVCG], if applicable.

Evidence of these trainings SHALL be kept and it SHALL be documented that each employee involved in validation has the required know-how before taking on the activities.

In addition, registration staff SHALL be required to pass an examination provided by the TSP on the information verification requirements outlined in the [BR] and the [EVCG], if applicable.

5.3.4 Retraining frequency and requirements

Personnel SHOULD be trained regularly (at least annually) on current threats and security practices.

Through appropriate regular training SHALL be ensured, that personnel in trusted roles maintain the required know-how at all times.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Personnel SHALL be accountable for their actions. Appropriate sanctions SHALL be imposed when violating the requirements of the TSP.

5.3.7 Independent contractor requirements

The requirements listed in Section 5.3 apply by analogy to third parties assigned by the TSP, if applicable.

[TLS] Third party personnel involved in the issuance of certificates SHALL be checked for compliance with the training and qualification requirements according to Sections 5.3.1 and 5.3.3.

5.3.8 Documentation supplied to personnel

Role owners SHALL be provided with role descriptions that describe the responsibilities and duties resulting from the respective role, taking into account the requirements listed above (Section 5.3).

Where required, the role descriptions SHALL differentiate between general and specific roles.

The security roles and responsibilities defined in the information security policy SHALL be described in job descriptions or in documents available to all affected employees.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The following events including the precise time, the identity of the trigger (if applicable) and the description of the event SHALL be logged in the respective system logs:

- All significant events of the certificate and key management systems as well as status services, which are at least (if applicable)
  - key generation, backup, storage, recovery, archiving and destruction,
  - certificate application including renewal,
  - validations, approvals and rejections,
  - issuance of certificates,
  - certificate revocation application,
  - revocation of certificates,
  - generation of revocation lists and
  - signing of OCSP responses.
- All security relevant events on the PKI and security systems, in particular
  - changes to the systems' security policies,
  - system startup and shutdown,
  - system crashes and hardware failures,
  - time synchronization events,
  - firewall and router activities and
  - successful and unsuccessful PKI system access attempts.
- Installation, update and deinstallation of software on the PKI systems.

In addition, all physical entries and exits to/from the security zones SHALL be logged in the access systems.

5.4.2 Frequency of processing log

Log data SHALL be evaluated as follows:

- Security relevant events SHALL be evaluated as described in Section 6.6.2.
- All other records SHALL be evaluated when necessary, e.g. for troubleshooting or analysis activities.

5.4.3 Retention period for audit log

Log data SHALL be retained for a reasonable period of time. The retention periods SHALL be described in the CPSs, see also Section 5.5.2.

[TLS] Log data SHALL be retained for at least two years after its occurrence.

5.4.4 Protection of audit log

Log data SHALL be kept confidential, integrity-secured and protected in such a way that they cannot be easily destroyed or deleted, see also Section 5.4.6. It SHALL be described in the CPSs how the protection of these records is ensured.

Log data SHALL be made available in case of need, e.g., in legal proceedings or upon request of internal and external auditors.

Log data retention SHALL be monitored (e.g., in internal audits).

5.4.5 Audit log backup procedures

No stipulation.

5.4.6 Audit collection system (internal vs. external)

Log data SHALL be collected in a separate tamper-proof system, i.e., not only in the system where the events are logged. The system SHALL be designed in such a way that entries can only be added but not deleted during the specified retention period, the storage capacity of the system SHALL be designed accordingly.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

For each certificate, the application/certificate history SHALL be recorded, including date, time and, if applicable, the identity of the acting person. This includes the following activities of subscribers as well as internal and, if applicable, external RAs:

- all activities related to the application, registration, validation and approval or rejection of applications for issuance, renewal and revocation of certificates of all hierarchy levels
- all activities related to the lifecycle of keys and certificates of all hierarchy levels. This includes at least, if applicable,
  - the generation, storage, backup, recovery, archiving and destruction of keys, including the preparation or provision of QSCD or other cryptographic devices, and
  - the issuance, acceptance, publication and revocation of certificates.

Furthermore, for each certificate, the relevant information and documents submitted by the applicant or provided to the applicant as part of the application for issuance, renewal, modification or revocation SHALL be recorded resp. retained ("registration information"). This shall include at least

- the information regarding the identity and other attributes, if any, of the subscriber, including, if applicable, a reference to the documents or sources used for verification.
  Note: If the identity or attributes were verified against a public and permanently accessible source, information on which source was used and whether the data matched is sufficient. An extract from the source does not have to be kept.
- the agreement concluded with the subscriber, if any, but at least acceptance of the Terms of Use in force at the time of application.

In addition, the following information and documents SHALL be recorded resp. retained:

- all published CP, CPS, and Terms of Use
- certification documents and audit reports
- relevant documentation related to the security of the systems from the
  - change management,
  - vulnerability management,
  - role management,
  - lifecycle management of cryptographic modules
- if applicable, other information required to ensure continuity of services or needed as evidence in legal proceedings.

Taking into account the relevant privacy aspects, additional data MAY be recorded. In the CPSs and Terms of Use SHALL be described which data are recorded.

[TLS] For each certificate, the method used to validate the domain name or IP address according to [BR#3.2.2.4] or [BR#3.2.2.5] including the version of the [BR] on which the validation was based, SHALL also be recorded.

[3145] Records SHALL be archived in such a way that all certificates can be uniquely assigned to a registered subscriber. In addition, tracking SHALL be possible to prevent fraudulent or manipulated certificates from being generated.

5.5.2 Retention period for archive

In addition to the certificates themselves, the following of the records listed in Section 5.5.1 SHALL be archived for at least 7 years after the expiration of the validity of the affected certificates:

- Application/certificate history
- Registration information
- CP, CPS and Terms of Use
- Certification documents and audit reports

All other records SHALL be retained for a minimum of 2 years.

The retention period (if applicable per certificate type) SHALL be described in the CPSs as well as in the Terms of Use.

The obligation to retain records also applies beyond the termination of a Trust Service. The termination plan SHALL therefore specify which information is transferred where and how this information can be accessed, see also Section 5.8.

[QCP-l] [QCP-n] The certificate history and registration information SHALL be kept permanently.

5.5.3 Protection of archive

Records SHALL be maintained in confidence, with integrity, and protected from destruction or deletion.

[EVCP] Retention of information and documents SHALL be monitored (e.g., in internal audits).

[QCP] Electronically retained records that are integrity-secured using QES or time stamps SHALL be re-protected by appropriate measures to ensure long-term preservation of evidence if the previous protection weakens over time.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for timestamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

Archived information SHALL be evaluated and made available when needed, e.g., in case of problem reports, in legal proceedings, or upon request of internal and external auditors. Access to the archived information SHALL be defined and documented internally within the TSP.

5.6 Key changeover

Prior to the expiration of a CA certificate, a new CA certificate SHALL be issued in good time in accordance with the current versions of this CP and the CPSs, provided that the affected Trust Service is to be continued. In doing so, the period between the publication of the new CA certificate and the taking out of service of the expiring CA certificate SHOULD be sufficiently long so that there is no interruption in operation for the subscribers.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The procedures for notification and handling of incidents and compromises and for recovery from outages or disasters SHALL be described in the emergency documentation.

Emergency documentation SHALL include the following aspects:

- emergency prevention:
  - requirements to back up critical cryptographic material at another location
  - requirements to regularly back up all relevant data needed to reestablish CA operations after a disaster at secure, preferably remotely located sites
  - distance from the primary site to sites that can be used to reestablish CA operations
- naming of all roles involved and escalation levels
- responsibility of all parties involved
- conditions under which an incident becomes an emergency
- emergency processes
- fallback processes
- recovery processes
- processes for reporting
  - security breaches to the supervisory authorities (within 24 hours) or other relevant stakeholders,
  - security breaches that disadvantageously affect natural persons or organizations to the affected persons or organizations (without delay),
  - privacy incidents to the responsible authorities or other relevant stakeholders (within 24 hours)
- recovery time targets
- follow-up incl. root cause analysis to avoid recurrence
- review cycles of the emergency plan (at least annually)
- awareness and training requirements
- regular emergency exercises (at least annually)
- plan for resuming operations after interruption or failure of critical business processes
- establishment of acceptable downtime and recovery times
- procedures for securing the impacted site to the maximum extent possible during the period following a disaster and prior to recovery at the original site or at another site

The emergency documentation SHALL be disclosed to auditors upon request.

Procedures for notifying incidents SHALL be established and it SHALL be ensured that they are known and used by employees.

In order to minimize potential damage, it SHALL be responded in a timely manner to incidents reported by individuals and alarms reported by systems (see Section 6.6.2). Potentially security-critical incidents SHALL be investigated immediately by personnel in trusted roles.

[TLS] [SMIME] Violations of the relevant Root Store Policies SHALL be immediately reported to the appropriate Root Store operators and issuance of the affected certificate types SHOULD be stopped until the cause of the violation is resolved.

[VS-NfD] The emergency plan SHALL be approved by the security officer.

5.7.2 Computing resources, software, and/or data are corrupted

See Section 5.7.1.

5.7.3 Entity private key compromise procedures

Compromise, suspected compromise, and loss of a CA private key SHALL be defined as an emergency in the emergency documentation and the resulting activities SHALL be described.

In the event of a CA key compromise, the corresponding CA certificate SHALL be revoked and all affected parties (subscribers as well as all others with whom the TSP has agreements) SHALL be informed. In addition, the information SHALL be made available to relying parties and it SHALL be indicated that the certificates and status information issued by the affected CA no longer can be trusted.

Furthermore, all subscriber certificates (with the exception of short-term certificates) SHOULD be revoked.

[QCP] The procedures for providing status information on subscriber certificates in case of compromise of a CA key SHALL be described in the CPS.

[3145] In the event of a suspected compromise of a CA key, the affected key SHALL not be used until final clarification.

5.7.4 Business continuity capabilities after a disaster

In the event of an emergency, operations SHALL be reinstated within the time period specified in the emergency documentation after all causes have been eliminated by appropriate mitigation measures.

5.8 CA or RA termination

When terminating a Trust Service, potential disruptions for subscribers and relying parties SHALL be minimized as far as possible.

If possible, the provision of the Trust Service for existing subscribers SHOULD be transferred to another TSP, otherwise a secure termination of the Trust Service SHALL be ensured.

Prior to termination or transfer of a Trust Service, the following SHALL be done:

- All affected parties (subscribers, relevant supervisory authorities if any, affected Root Store operators or other affected parties with whom the TSP has contracts) are informed,
- Relying parties are provided with the information about the termination or transfer,
- Agreements with subcontractors, e.g., external RAs, are terminated.

Prior to termination of a Trust Service, the following SHALL be done:

- A reliable organization is obligated to retain all information necessary to demonstrate the operation of the TSP for a reasonable period of time, as agreed upon with subscribers and others, if applicable. At a minimum, this includes
  - registration information,
  - certificate status information,
  - event log archives,
  - CA certificates.
- The private CA keys are destroyed or taken out of service in such a way that they cannot be reused.
- All certificates that are still valid and not yet revoked are revoked.

Prior to transferring a Trust Service, appropriate agreements SHALL be concluded with the acquiring TSP.

Upon termination or transfer of a Trust Service and transfer of the information to another entity, all keys, certificates and customer data SHALL be deleted.

The arrangements made to terminate or transfer a Trust Service SHALL be defined in a maintained termination plan.

Furthermore, the CPS SHALL describe how to proceed in case of termination of a Trust Service, at a minimum this includes

- the information of all affected parties,
- the handling of status information on unexpired certificates, and
- if applicable, the transfer of duties to others.

[QCP] The CPS SHALL also describe the procedures for providing status information for all expired certificates in accordance with Section 4.10.

[QCP-l] [QCP-n] The termination plan SHALL take into account,

- that the subscribers are informed, as far as possible, two months in advance about the termination and the transfer of the certificates,
- that all certificates, their status information as well as the relevant information according to Section 5.5.1 are handed over, if possible, in electronic form according to the state of the art, either to another qualified TSP or to the Federal Network Agency as the responsible supervisory authority.

`cessationOfOperation` SHALL be specified as the revocation reason for the revoked certificates in the status services.

Prior to the termination of an RA, it SHALL be defined and described in the CPS, which information (e.g., certificate applications kept or archived at the RA or other registration information) must be handed over to the TSP.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

All keys SHALL comply with the algorithms, key lengths and quality requirements listed in Sections 6.1.5 and 6.1.6. The keys SHALL be considered suitable for the entire lifetime and intended uses at the time of generation.

6.1.1.1 CA key pair generation

CA key pairs SHALL be generated in a crypto module according to Section 6.2.1 in the secure environment of the Trust Center as part of a key ceremony, it SHALL be the crypto module in which the private key will be used later, so that no import or export of the keys is required except for backup purposes.

The roles involved as well as their tasks and responsibilities before, during and after the key ceremony SHALL be defined and documented.

The individual steps of the key ceremony SHALL follow a defined protocol and be documented within it.

Generation SHALL be performed by at least two Trust Center employees acting in trusted roles.

The following requirements apply for the generation of Root CA keys:

- Each of the two employees SHALL have knowledge only of a part of the activation data required for key generation.
- The two employees SHALL act in different roles.

The following requirements apply for the generation of Sub CA keys:

- To prove authenticity and integrity, the hash value of the generated public key or of the CSR containing the public key SHALL be included in the generation protocol and handed over during certificate application (see Section 4.1).

An internal auditor (see Section 8.2) SHALL monitor the key ceremony and confirm its correct performance in the protocol.

[TLS] [SMIME] Both an internal and a qualified external auditor (see Section 8.2) SHALL monitor the key ceremony and confirm its correct execution in the protocol. In addition, the external auditor SHALL confirm in his report that all requirements are met and that the integrity and confidentiality of the keys are maintained.

6.1.1.2 OCSP Signer key pair generation

OCSP Signer key pairs SHALL be generated in cryptographic modules according to Section 6.2.1, it SHALL be the crypto module in which the private key will be used later, so that no import or export of the keys is required except for backup purposes.

6.1.1.3 RA key pair generation

RA key pairs SHALL be generated in cryptographic modules according to Section 6.2.1.

6.1.1.4 Subscriber key pair generation

Subscriber key pairs MAY be generated either by the TSP or the subscriber itself.

If the keys are generated by the subscribers, the subscribers SHALL be informed about the permitted algorithms and key lengths to be used.

If the keys are generated by the TSP, the keys SHALL be generated in a secure manner and SHALL be maintained until certificate generation, ensuring integrity and confidentiality.

[TLS] Subscriber keys SHALL NOT be generated by the TSP.

[QCP-n-qscd] [QCP-l-qscd] Subscriber key pairs SHALL be generated by a certified QSCD (see Section 6.2.1).

[3145] If subscriber keys for cryptographic token as a storage medium of the keys are generated by the TSP, the keys SHOULD be generated by the token itself. Keys generated outside the token SHALL be deleted immediately after they are stored in the token unless a backup of the subscriber keys is provided.

6.1.2 Private key delivery to subscriber

The procedures for handing over the keys SHALL be described in the Terms of Use and the CPSs.

If subscriber keys are generated by the TSP, the following requirements SHALL be considered:

- The keys SHALL be handed over to the subscriber in such a way that the preservation of confidentiality and integrity is ensured and unauthorized use is impossible unless the TSP manages the keys on behalf of the subscriber.
- After the keys have been handed over to the subscriber, all copies of the keys SHALL be deleted from the TSP's systems, unless the keys are to be escrowed with the TSP on behalf of the subscriber (see Section 6.2.3).

[NCP] If subscriber keys are generated by the TSP and managed on behalf of the subscriber and the key usage in the corresponding certificates is set to `nonRepudiation`, it SHALL be ensured that the subscribers have sole control over the keys. In the case that a TSP other than the one that generated the keys and issued the certificates manages the keys of the subscribers on their behalf and the key usage in the corresponding certificates is specified as `nonRepudiation`, the TSP that generated the keys and issued the certificates SHALL obtain confirmation that the TSP managing the keys ensures that the subscribers have sole control over the keys. Conformance to [ETS431-1] SHOULD be used to demonstrate that a TSP managing keys on behalf of subscribers meets the requirements to ensure sole control of the keys.

[NCP+] If subscriber keys are generated by the TSP, it SHALL be ensured that they are handed over to the registered subscribers on secure cryptographic devices (e.g., smartcards) in a secure manner. In the case that a subscriber has its keys managed by a TSP other than the one that generated the keys and issued the certificates, the device SHALL be handed over to this TSP in a secure way.

[QCP-n-qscd] [QCP-l-qscd] The private keys SHALL be handed over to the subscribers in certified QSCDs according to Section 6.2.1 or managed by the TSP on behalf of the subscribers.

If the TSP is managing the subscribers QSCD, it SHALL be ensured that they can be used only under the sole control of the subscriber.

[3145] The procedures for issuing tokens SHALL be described in the terms of use and the CPSs.

If the TSPs generate the keys for the subscriber certificates, it SHALL be ensured that

- the keys are delivered to the correct recipient,
- the confidentiality of the keys is guaranteed during delivery,
- keys are deleted in the systems of the TSPs after delivery to the correct recipient, unless the keys are to be escrowed with the TSP on behalf of the subscriber

6.1.3 Public key delivery to certificate issuer

No stipulation.

[TLS] Formats and methods of accepted CSRs SHOULD be specified in the CPSs or in documents referenced by the CPSs.

6.1.4 CA public key delivery to relying parties

CA certificates SHALL be made accessible to the general public in an authentic and integrity-protected form (see Section 2.2)

For Root CA certificates, additional validation mechanisms SHALL be provided, such as a validation option of the hash value of the certificate against a trusted source.

6.1.5 Key sizes

The keys of all certificates of all hierarchy levels SHALL meet the requirements from [SOGIS]. Accordingly, the following minimum requirements SHALL be applied:

- RSA: Keys SHOULD have a length of at least 3,000 bits (recommendation according to [SOGIS]). Keys with a length of more than 1,900 bits and less than 3,000 bits MAY still be used until 2025 (Legacy according to [SOGIS]).
- ECC: Keys from the following curves SHOULD be used (recommendation according to [SOGIS]):
  - BrainpoolP256r1
  - BrainpoolP384r1
  - BrainpoolP512r1
  - NIST P-256
  - NIST P-384
  - NIST P-521

If the key lengths used are no longer sufficient for the intended use due to new knowledge or requirements, the subscribers and relying parties SHALL be informed and a schedule SHALL be set to revoke the certificates and migrate to sufficiently long keys.

[TLS] [SMIME] The following requirements apply to RSA keys:

- They SHALL have a minimum length of 2048 bits.
- The length of the modulus SHALL be divisible by 8.

EC keys SHALL be used from the following curves:

- NIST P-256
- NIST P-384

[VS-NfD] Requirements from [TR2102-1] SHALL be applied.

6.1.6 Public key parameters generation and quality checking

No stipulation.

[TLS] Keys submitted by subscribers SHALL be checked for compliance with the following characteristics:

- RSA: The value of the exponent SHALL be an odd number greater than or equal to 3 and SHOULD be in the range of 2^{16} und 2^{256}-1.
- RSA: The value of the module SHALL be an odd number that is not the power of a prime and has no factors smaller than 752.
- ECC: The keys SHOULD be validated using either the ECC routine for full public key validation or the ECC routine for partial public key validation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The usage of a private key SHALL be restricted to the purposes listed in the corresponding certificate in the `keyUsage` and, if set, in the `extendedKeyUsage` (see Section 7.1.2).

The usage of Root CA's private keys SHALL be limited to the signing of

- its own Root CA certificate,
- Sub CA certificates,
- OCSP Signer certificates,
- if applicable, CRL Signer certificates and
- revocation lists.

The usage of Sub CA's private keys SHALL be limited to the signing of

- Sub CA certificates,
- subscriber certificates,
- OCSP Signer certificates,
- if applicable, CRL Signer certificates,
- revocation lists and
- if applicable, OCSP responses.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

To protect the private keys of all levels of the hierarchy, sufficient security measures SHALL be taken, or, in the case of subscriber keys that are not managed by the TSP, sufficient security measures SHALL be required.

6.2.1 Cryptographic module standards and controls

Cryptographic modules used SHALL be either evaluated to CC EAL 4 or higher or to a comparable standard or certified to FIPS 140-2 level 3 or FIPS-140-3 level 3 and SHALL be operated according to the specifications of the certification documentation or in a comparable configuration with the same security level.

Manipulation of cryptographic modules during storage and transport SHALL be prevented.

[QCP-n-qscd] [QCP-l-qscd] QSCDs SHALL comply with the requirements set out in [eIDAS#Art.29] and be certified in accordance with [eIDAS#Art.30]. The certification status of the QSCDs SHALL be monitored until the expiration of the validity of the subscriber certificates and appropriate measures SHALL be taken if the certification status changes before expiration of the subscriber certificates.

[VS-NfD] Cryptographic modules in which the keys of the Sub CAs and, if applicable, the subscribers are generated and operated SHALL be approved by the German Federal Office for Information Security for VS-NfD use.

6.2.2 Private key (n out of m) multi-person control

When importing and exporting CA keys for backup and recovery purposes (see Sections 6.2.4 and 6.2.6), a multi-person control SHALL be implemented.

6.2.3 Private key escrow

No stipulation.

6.2.4 Private key backup

Private keys of CAs and, if applicable, subscriber keys generated by the CA and intended to be backed up, SHALL be backed up in a secure environment, with the same level of security for access, tampering and loss as for the private keys in use.

Backup as well as restore of CA keys SHALL be performed within the scope of a key ceremony. The same conditions apply as for the key generation (see Sections 6.1.1.1 resp. 6.1.1.2), the presence of an external auditor MAY be waived. In addition, it SHALL be ensured that access to the backups requires at least two trusted employees of the TSP.

[3145] If keys are backed up on behalf of subscribers

- they SHALL be stored encrypted with individual secrets generated by the Sub CA,
- the individual secrets used for encryption SHALL also be encrypted and SHALL be securely stored separately from the subscriber keys, ensuring their integrity and confidentiality,
- the subscribers SHALL be securely identified in the event of a restore application (along the lines of identification at the time of application, (see Section 4.2.1),
- the restored keys SHALL be handed over to the subscriber in the same way as the original keys (see Section 6.1.2)

[VS-NfD] If keys are backed up on behalf of subscribers,

- in addition to the guidance on [3145] above, the restore actions and policies SHALL be approved by the security officer and
- other than the encryption keys SHALL NOT be backed up.

6.2.5 Private key archival

No stipulation.

[TLS] Private keys of Sub CAs SHALL NOT be archived by other parties without the permission of the TSP. Likewise, private keys of a subscriber SHALL NOT be archived without the permission of the subscriber.

6.2.6 Private key transfer into or from a cryptographic module

Import and export of keys SHALL be subject to a key ceremony with at least dual control. The same conditions apply as for key generation (see Sections 6.1.1.1 resp. 6.1.1.2), the presence of an external auditor MAY be waived.

Private keys SHALL NOT be exported in plain text, but the functions provided by the cryptographic module SHOULD be used to encrypt the exported keys.

[3145] In case of a defect of a cryptographic module used to store and use private keys of a Sub CA, the private keys SHALL be transferred to a new cryptographic module according to the requirements above.

6.2.7 Private key storage on cryptographic module

Keys stored in cryptographic modules SHALL be stored securely using the functions provided by the cryptographic module .

6.2.8 Method of activating private key

Activation of CA private keys SHALL be performed by persons in trusted roles using the functions provided by the HSM.

If keys for subscribers are generated by the TSP it SHALL be ensured that the activation by the subscribers is done in a secure manner.

[QCP-n-qscd] [QCP-l-qscd] The use of private subscriber keys SHALL be in the sole control of the subscriber, regardless of whether the subscriber owns the QSCD or has it managed by a TSP on its behalf.

6.2.9 Method of deactivating private key

The deactivation of CA private keys SHALL be performed by persons in trusted roles using the functions provided by the HSM.

If keys for subscribers are generated by the TSP and handed over by means of cryptographic modules (e.g., smart cards). It SHALL be ensured that their deactivation and, if necessary, reactivation by the subscribers is done in a secure manner.

6.2.10 Method of destroying private key

Private CA keys SHALL be destroyed at the end of the life cycle of the corresponding CA certificate, i.e., upon expiration, revocation or taking out of service of the CA certificate, or termination of the Trust Service. The destruction of the keys SHALL be performed in a key ceremony and all copies of the keys SHALL be considered. The same requirements apply here as for the generation of the keys, if applicable (see Sections 6.1.1.1 resp. 6.1.1.2).

If cryptographic modules are taken out of service, all private keys stored in the module SHALL be destroyed.

6.2.11 Cryptographic Module Rating

Cryptographic modules SHALL be evaluated for usability and compliance with all requirements prior to purchasing.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys (i.e., certificates) SHALL be retained according to Section 5.5.2.

6.3.2 Certificate operational periods and key pair usage periods

The validity period of a certificate SHALL not exceed the validity period of the issuing CA certificate.

[QCP-n] [QCP-l] Certificates MAY be valid longer than the issuing CA certificate.

[TLS] [SMIME] The validity period of Root CA certificates SHALL NOT be greater than 25 years. The validity period of Sub CA certificates SHOULD NOT be greater than 10 years and SHALL NOT be greater than 20 years.

[TLS] Subscriber certificates SHOULD NOT be valid for more than 397 days and SHALL NOT be valid for more than 398 days.

[SMIME] Subscriber certificates SHOULD NOT be valid for more than 825 days (i.e., two years plus a grace period of max. three months) and SHALL NOT be valid for more than 1185 days (i.e., three years plus a grace period of max. three months).

[3145] The use of the private key of a Sub CA SHALL be disabled, e.g., by deactivation, if the key ▪ is not to be used until a defined point in time (e.g., commissioning of a new Sub CA certificate planned for the future) or ▪ is not to be used for a certain period of time due to a special use case.

6.4 Activation data

6.4.1 Activation data generation and installation

The activation data of the HSM SHALL be generated and installed during commissioning of the HSM in a four-eyes-principle within the scope of a defined change process, using the functions provided by the cryptographic module .

If subscriber keys are stored in cryptographic modules (e.g., smartcards) that are provided with individual activation data (e.g., PINs), the activation data of the cryptographic modules SHALL be generated and set in a secure manner.

6.4.2 Activation data protection

Knowledge of HSM activation data SHALL be restricted to persons in trusted roles, and the group of knowing persons SHALL be strictly limited to what is absolutely necessary.

If activation data for subscriber keys are generated by the TSP (see Section 6.4.1) they SHALL be protected from generation to handover to the subscriber in such a way that their integrity and confidentiality are ensured and they SHALL be handed over to the subscriber in such a way that it is time-shifted and via a different communication channel to the cryptographic module itself.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Note: The requirements listed below apply by analogy to third parties contracted by the TSP, where applicable.

Systems required for certificate management as well as status and directory services SHALL be protected according to the potential for damage.

The accounts of the trusted roles (see Section 5.2.1) required to operate the critical systems SHALL be managed in such a way that

- access to the systems and data is restricted to the persons identified and authenticated for these roles (see Section 5.2.3) with the minimum required permissions,
- they are changed or deleted within a reasonable time.

Multi-factor authentication SHALL be implemented for the accounts that can directly initiate issuance of certificates.

The required separation of trusted roles (see Section 5.2.4) SHALL be technically supported by the systems.

Administration systems used to implement security policies SHALL NOT be used for other purposes.

Trusted systems that ensure the technical security and reliability of the processes supported by the systems SHALL be used.

The CA, certificate management, security and frontend systems and, if applicable, other internal systems supporting operation, SHALL be hardened, i.e., they SHALL be configured to disable the accounts, services, protocols and ports that are not required for operation of the CAs.

Systems SHALL be equipped with integrity protection that protects against viruses, malicious code and the import of unauthorized software.

Systems SHALL be sized to ensure sufficient performance and uninterrupted operation.

Data collected for certificate generation and, if necessary, revocation, including the log data in accordance with Section 5.4.1, SHALL be protected in such a way that their integrity, confidentiality, and availability are ensured over the entire retention period.

[TLS] [SMIME] Accounts of those authorized to access the system SHALL be reviewed at least every three months. Accounts that are no longer needed SHALL be deactivated.

Multi-factor authentication SHALL be implemented on all systems that support multi-factor authentication.

Authentication keys and passwords of the privileged accounts of the CA systems SHALL be changed when a person's authorization for administrative access to the systems changes or is revoked.

For trusted roles, login into the systems with personal accounts for traceability SHALL be ensured.

For trusted roles that log in to the systems using username and password, the measures listed below SHALL be implemented, if technically possible:

- For accounts that can only be accessed in secure environments, passwords SHALL be required to be at least 12 characters in length.
- For authentications that cross a zone boundary into a secure zone, multi-factor authentication is required.
- For accounts that can be accessed from outside a secure zone, passwords of at least eight characters that are not one of the user's previous four passwords are required, and account lockout is required after five failed access attempts (see below).
- When developing password policies, TSPs SHOULD consider the password policies in NIST 800-63B Appendix A.
- If a TSP has a password policy that requires routine periodic password changes, this period SHALL NOT be less than two years.

Individuals in trusted roles SHALL be required to log out of their account or lock their workstation when they are no longer in the role.

Workstations SHALL be either configured to automatically lock out after a specified period of user inactivity, or the relevant applications SHALL be configured to automatically log out of the account after a specified period of user inactivity.

Access to CA systems SHALL be disabled after five failed login attempts, provided that the CA system supports this measure, the measure cannot be used for denial-of-service attacks, and the measure does not weaken the security of this authentication control.

Multi-factor authentication or multi-person authentication SHALL be ensured for administrative access to critical systems.

Multi-factor authentication SHALL be ensured for all accounts of trusted roles on CA systems accessible from outside the secure environments.

Remote access to critical systems SHALL only be allowed if it originates from systems owned or controlled by the TSP and is temporarily established over an encrypted channel based on multifactor authentication to a secured system on the TSP's network that mediates the connection to the critical systems.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

Already in the design and requirements specification phase of a system development project a security requirements analysis SHALL be performed to ensure that systems security is addressed from the very beginning.

Separate systems SHALL be used for the production, test and development environment.

6.6.2 Security management controls

All releases, patches and short-term bug fixes as well as configuration changes that affect the security policy, SHALL be handled and documented via regulated change management processes.

Any changes that impact the level of security established by the TSP, SHALL be approved by the management and if necessary, the ISMS.

It SHALL be ensured that

- security patches are applied in a reasonable amount of time, but within 6 months at the latest,
- security patches are not applied, if they introduce additional vulnerabilities or instabilities that outweigh the benefit of the patch,
- the reasons for not applying security patches are documented.

The following activities SHALL be monitored continuously and appropriate alarming capabilities SHALL be implemented:

- security relevant system events according to Section 5.4.1
- availability and use of the required services
- configuration changes that were not made on the basis of an authorized change

Monitoring SHOULD consider the sensitivity of any information collected or analyzed.

Backups SHOULD be tested on a regular basis to ensure that they meet the requirements of the emergency plan. The data backup and restore functions SHALL be performed by the designated trusted roles.

[TLS] [SMIME] In addition to the events above, the following activities SHALL be monitored:

- changes to security profiles
- installation, update and removal of software on a certificate system
- system crashes, hardware failures, and other anomalies
- firewall and router activities
- entries into and exits out of certificate management system operating rooms

[NCP] System capacity needs SHALL be monitored and forecasts for future capacity needs SHALL be made to ensure adequate processing and storage capacity is available.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

Internal networks and systems SHALL be protected from unauthorized access and attacks, e.g., by firewalls. Network components (e.g., firewalls, routers) SHALL be configured in such a way that all protocols and accesses are deactivated that are not required.

Networks SHALL be segmented based on a risk assessment considering the functional, logical, and physical (including location) relationship between trustworthy systems and services.

All systems critical for the operation of the TSP SHALL be located in secure or high secure zones. Root CA systems SHALL be located in high secure zones and SHALL be operated offline or separate from all other networks. Security procedures that protect the systems and communications between systems within secure zones SHALL be implemented.

Local network components (e.g., routers) SHALL be installed in physically and logically secure environments. Their configurations SHALL be regularly checked for compliance with the requirements defined.

Networks for administration of the systems SHALL be separated from the operational networks.

Within a zone, the same security requirements SHALL apply to all systems.

Security systems SHALL be implemented between zones to protect the systems and communications within the secure zones as well as communications with the systems outside the zones. Connections SHALL be restricted to allow only those connections required for operation. Connections not required SHALL be explicitly prohibited or disabled. All network devices at the zone boundaries (firewalls, routers, switches, gateways, or other devices) SHALL be configured to allow only those services, protocols, ports, and communication relationships that are required for the operation of the CAs.

These rules SHALL be reviewed on a regular basis.

For communication between different trusted systems, trusted channels SHALL be used that are logically distinct from other communication channels and ensure secure identification of their endpoints and integrity and confidentiality of the transmitted data.

If high availability of external access is required, the external network connections SHALL be redundant.

Vulnerability scans on public and private IP addresses identified by the TSP SHALL be performed at least quarterly. Vulnerability scans SHALL be performed by individuals or organizations with the skills, tools, abilities, ethics, and independence necessary to provide a reliable report. The execution of the vulnerability scans SHALL be documented, indicating the qualifications of the person or organization conducting the assessment.

Penetration tests of the systems SHALL be performed when systems go live or when significant changes are made to the infrastructure or applications. They SHALL be performed by individuals or organizations with the skills, tools, abilities, ethics, and independence necessary to provide a reliable report. The execution of the penetration tests SHALL be documented, indicating the qualification of the person or organization performing the tests.

Within 48 hours after the discovery of a critical vulnerability

- the vulnerability SHALL be remediated, or
- if remediation of the vulnerability is not possible within 48 hours, a mitigation plan for the vulnerability, including prioritization based on the affected systems SHALL be prepared or
- the factual basis for the TSP's decision that the vulnerability does not need to be remediated, because either the TSP disagrees with the rating or it is not a vulnerability ("false positive") or exploitation of the vulnerability is prevented by compensating controls or the absence of threats, or other similar reasons SHALL be documented.

[TLS] [SMIME] Intrusion detection (IDS) and intrusion prevention systems (IPS) that are under the control of the TSP or delegated to trusted third parties SHALL be implemented.

The vulnerability scans mentioned above SHALL be performed

- within one week upon request of the CA/Browser Forum and
- in case of significant changes to the infrastructure or applications.

[3145] If an IDS is used, the log files recorded by the IDS SHALL be evaluated each time an incident occurs and periodically in a time period determined by the TSP.

[VS-NfD] [ISI LANA] SHALL be used as a guide in network separation.

6.8 Timestamping

All systems SHALL be regularly, at least once a day, synchronized with exact time information (UTC) via a time server and the Network Time Protocol (NTP), so that the timestamps on logs and records are reliable.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profiles

Certificate profiles SHALL comply with [RFC5280] and [X.509] and be described in the CPSs.

Note: Pre-certificates according to [RFC6962] ("Certificate Transparency") are not considered valid certificates in the sense of [RFC5280].

The certificate profiles apply to all certificates issued as of the effective date of this CP. Certificates already issued with profiles in accordance with older requirements retain their validity unless explicit reference is made to their invalidity.

Certificate serial numbers SHALL be generated using a cryptographically secure random number generator.

The validity start date of a certificate SHALL NOT be before its date of issue, but it MAY be set to a later date if necessary.

[TLS] [SMIME] Certificate serial numbers SHALL have at least 64 bits of entropy.

7.1.1 Version number(s)

All X509 certificates SHALL be issued in version 3.

7.1.2 Certificate extensions

The following table provides an overview of mandatory and optional certificate extensions for CA, subscriber and OCSP Signer certificates[5].

Extensions that are not listed there SHALL NOT be used in principle, exceptions SHALL be described in the CPS.

The following conventions apply:

- **M** (mandatory): this extension SHALL be set.
  (M) this extension SHALL be set under certain circumstances.
- **O** (optional): this extension MAY be set.
- **S** (should): this extension SHOULD be set
- **SN** (should not): this extension SHOULD NOT be set.
- **N** (not allowed): This extension SHALL NOT be set.
- **c** (critical): This extension, if set, SHALL be marked as critical.
  (c) This extension MAY be marked as critical.
  Note: extensions SHALL NOT be marked as critical if it is not explicitly allowed or requested.
- **(<No.>)** Reference to the description of the contents to be set following the table.

[5] CRL signer certificates are not listed because actually the CRLs are always issued directly by the CAs.

Table 2 - Certificate extensions

Extension acc. to [RFC5280] (OID)	Root CA	Sub CA	Subscriber	OCSP-Signer
authorityKeyIdentifier (2.5.29.35)	O	M (01)	M (01)	M (01)
subjectKeyIdentifier (2.5.29.14)	M (02)	M (02)	S	S
keyUsage (2.5.29.15)	M c (03)	M c (03)	M c [TLS] O (04)(05)	M c
certificatePolicies (2.5.29.32)	O [TLS] N (06)	O [TLS] M (06)(07)(08)(09)	M (06)(10) (11)(12)(13)	N
subjectAltName (2.5.29.17)	O (14)	O (14)	O [TLS] [SMIME] M (14)(15)(16)(17)	N
basicConstraints (2.5.29.19)	M c (18)	M c (18)	O (c) (19)	O (c) (19)
nameConstraints (2.5.29.30)	N	O [TLS] [SMIME] (M) c (20)	N	N
extendedKeyUsage (2.5.29.37)	N	SN [TLS] [SMIME] M (21)(22)(23)(24)(25)	O [TLS] [SMIME] M (21)(25)(26)(27)	M (21)(28)
cRLDistributionPoints (2.5.29.31)	N	(M) [TLS] [SMIME] M (29)(30)	(M) [TLS] [SMIME] M (29)(30)(31)	O[6] [TLS] N
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	N	(M) [TLS] [SMIME] M (32)(33)	(M) [TLS] [SMIME] M (32)(33)(34)	O[6] [TLS] SN
qcStatements (1.3.6.1.5.5.7.1.3)	N	N	N [QCP] M (35)(36)	N
validityModel 1.3.6.1.4.1.8301.3.5	N	N [QCP] O	N [QCP] M	N
issuerAlternativeName (2.5.29.18)	SN	SN	O	SN
subjectDirectory-Attributes (2.5.29.9)	SN	SN	O	N
id-pkix-ocsp-nocheck (1.3.6.1.5.5.7.48.1.5)	N	N	N	(M)[6] [TLS] M
cabfOrganization-Identifier (2.23.140.3.1)	N	N	N [EVCP] (M) (37)	N
signedCertificate-TimestampList (1.3.6.1.4.1.11129.2.4.2)	N	N	N [TLS] M (38)	O
id-etsi-ext-valassured-ST-certs (0.4.0.194121.2.1)	N	N	(M) (39)	N

In the following, the contents to be set in the extensions are listed, if there are supplementary requirements for this beyond the standards.

[6] See section 7.3.

authorityKeyIdentifier

(01) In Sub CA, subscriber and OCSP-Signer certificates the `keyIdentifier` according to [RFC5280#4.2.1.1] SHALL be set.

subjectKeyIdentifier

(02) In CA certificates, the `subjectKeyIdentifier` SHALL match the `authorityKeyIdentifier` in the certificates issued by that CA.

keyUsage

(03) In CA certificates, `keyCertSign` or `cRLSign` SHALL be set. `digitalSignature` SHALL be set if OCSP responses are also to be signed with this certificate. Other values SHALL NOT be set.

(04) In subscriber certificates, `keyCertSign` and `cRLSign` SHALL NOT be set, other values SHALL be set according to [RFC5280#4.2.1.3]. If the `extendedKeyUsage` is set, the `keyUsage` SHALL be set consistently to the parameters of the `extendedKeyUsage` according to [RFC5280# 4.2.1.12].

(05) [ETSI] In subscriber certificates for natural persons or organizations, one of the following variants of the `keyUsage` SHALL be set:
a) `nonrepudiation`
b) `nonRepudiation` and `digitalSignature`
c) `digitalSignature`
d) `digitalSignature` and [`keyEncipherment` or `keyAgreement`]
e) `keyEncipherment` or `keyAgreement`
f) `nonrepudiation` and `digitalSignature` and [`keyEncipherment` or `keyAgreement`]
To avoid mixed use of keys, only variants a), c) or e) SHOULD be used. In certificates confirming the commitment to signed content, one of the variants a), b) or f) SHALL be used, of which variant a) SHOULD be used.

certificatePolicies

(06) In principle, only OIDs SHOULD be set in the `certificatePolicies`. If the sole use of OIDs is insufficient, `cPSuri` with a valid http-URL or `userNotice` MAY be set additionally. An OID SHALL NOT be set multiple.

(07) [TLS] In Sub CA certificates, `certificatePolicies` MAY be set with an OID that confirms compliance with the [BR]. Either the OIDs reserved by the CA/Browser or the TSP's own OIDs described in the relevant CPS of the TSP MAY be used for this purpose. `anyPolicy` MAY be set.

(08) [SMIME] In Sub CA certificates `anyPolicy` SHOULD NOT be set.

(09) [TLS] [SMIME] The `certificatePolicies` set in Sub CA and subscriber certificates SHALL correspond to each other, i.e., subscriber certificates SHOULD NOT be issued by a Sub CA with OIDs that are not contained in the Sub CA certificate itself, unless `anyPolicy` is set in the Sub CA certificate ("policy chaining").

(10) [ETSI] Subscriber certificates for natural or legal persons (not SSL server certificates) SHALL include at least one OID that reflects the practices and procedures performed by the TSP. The following OIDs reserved by ETSI SHOULD be used:
- [NCP] `0.4.0.2042.1.1`
- [NCP+] `0.4.0.2042.1.2`
- [LCP] `0.4.0.2042.1.3`
- [QCP-n] `0.4.0.194112.1.0`
- [QCP-l] `0.4.0.194112.1.1`
- [QCP-n-qscd] `0.4.0.194112.1.2`
- [QCP-l-qscd] `0.4.0.194112.1.3`

`anyPolicy` SHALL NOT be set.

(11) [TLS] Subscriber certificates SHALL contain at least one of the following OIDs reserved by the CA/Browser Forum:
- [EVCP] `2.23.140.1.1`
- [DVCP] `2.23.140.1.2.1`
- [OVCP] `2.23.140.1.2.2`
- [IVCP] `2.23.140.1.2.3`

If the certificates are qualified website certificates, one of the following OIDs SHOULD also be included:
- [QEVCP-w] `0.4.0.194112.1.4`
- [QNCP-w] `0.4.0.194112.1.5`

In addition, the TSP's own OIDs described in the TSP's relevant CPS and/or subsequent ETSI reserved OIDs MAY be used:
- [EVCP] `0.4.0.2042.1.4`
- [DVCP] `0.4.0.2042.1.6`
- [OVCP] `0.4.0.2042.1.7`
- [IVCP] `0.4.0.2042.1.8`

Furthermore, `cPSuri` MAY be set with a reference (http URL) to the CPS or other online available information of the TSP. `userNotice` SHALL NOT be set.

(12) [EVCP] In subscriber certificates, `cPSuri` SHALL be set with a reference (http URL) to the CPS.

(13) [3145] In subscriber certificates, `cPSuri` MAY be set with a reference (http URL) to the CPS, `userNotice` SHALL NOT be set.

subjectAltName

(14) subjectAltName MAY be set in the certificates of all hierarchy levels. If set, all verifiable content SHALL have been validated.

(15) [TLS] In CA certificates the subjectAltName SHALL NOT be set. In subscriber certificates, at least one entry SHALL be included in the subjectAltName. Permitted entries are FQDNs or Wildcard Domain Names as dNSName or IPv4 or IPv6 addresses as iPAddress. The FQDNs as well as the FQDN portions of Wildcard Domain Names SHALL consist exclusively of "P-Labels" or "Non-Reserved LDH-Labels". Reserved IP addresses or internal names (according to Annex C) SHALL NOT be included.

(16) [EVCP] FQDNs included in subscriber certificates SHALL be owned or controlled by the subscriber and associated with its service. Wildcard Domain Names SHALL NOT be included.

(17) [SMIME] In subscriber certificates, at least one rFC822Name SHALL be included in the subjectAltName.

basicConstraints

(18) In CA certificates, cA SHALL be set to true. In Sub CA certificates a maximum path length SHOULD be indicated in pathLenConstraints, In Root CA certificates this indication SHOULD NOT be made.

(19) In subscriber and OCSP-Signer certificates, cA SHALL be set to false. pathLenConstraints SHALL NOT be set.

nameConstraints

(20) [TLS] [SMIME] In Sub CA certificates, nameConstraints MAY be included. nameConstraints SHALL be included if the certificates are to be technically constrained. For further details, please refer to Section 7.1.5.

extendedKeyUsage

(21) If set, the extendedKeyUsage SHALL be set consistently with the keyUsage according to [RFC5280#4.2.1.12].

(22) [TLS] In Sub CA certificates[7], `id-kp-serverAuth` SHALL be set. In addition, `id-kp-clientAuth` MAY be set. `id-kp-emailProtection`, `id-kp-codeSigning`, `id-kp-timeStamping`, and `anyExtendedKeyUsage` SHALL NOT be set, other values SHOULD NOT be set.

(23) [SMIME] In Sub CA certificates[8], `id-kp-emailProtection` SHALL be set. Other values MAY be set, but `anyExtendedKeyUsage`, `id-kp-codeSigning`, `id-kp-timeStamping` and `id-kp-serverAuth` SHALL NOT be included.

(24) In Sub CA certificates below the public Telekom Security Root CAs, which are not used to issue TLS certificates, `id-kp-serverAuth` SHALL NOT be set.

(25) [TLS] [SMIME] The `extendedKeyUsage` set in Sub CA and subscriber certificates SHALL correspond to each other, i.e., subscriber certificates SHALL NOT be issued by a Sub CA with values that are not contained in the Sub CA certificate itself ("EKU chaining"). This does not apply to OCSP Signer certificates, which MAY also be issued by Sub CAs that do not contain `id-kp-OCSPSigning`.

(26) [TLS] In subscriber certificates, `id-kp-serverAuth` or `id-kp-clientAuth` SHALL be set. Both values MAY also be set. Further values SHALL NOT be set.

(27) [SMIME] In subscriber certificates, `id-kp-emailProtection` SHALL be set. In addition, other values MAY be set, but `anyExtendedKeyUsage`, `id-kp-codeSigning`, `id-kp-timeStamping` and `id-kp-serverAuth` SHALL NOT be set.

(28) In OCSP Signer certificates, `id-kp-OCSPSigning` SHALL be set. Other values SHALL NOT be set.

`cRLDistributionPoints`

(29) In all certificates for which revocation lists are offered, `cRLDistributionPoints` SHALL be set

(30) [TLS] [SMIME] In Sub CA and subscriber certificates, `cRLDistributionPoints` SHALL be set with at least one http URL in `distributionPoints` .

(31) [3145] [ETSI] In subscriber certificates, the `cRLDistributionPoints` extension SHALL be set with at least one publicly accessible http or ldap URL in `distributionPoints`.

[7] This requirement does not apply to cross certificates
[8] This requirement does not apply to cross certificates

authorityInfoAccess

(32) In all certificates, which are OCSP-verifiable, `authorityInfoAccess` SHALL be set and SHALL contain at least the http URL of the OCSP responder in `id-ad-ocsp`.

(33) [TLS] In Sub CA and subscriber certificates, the http URL to download the issuing CA certificate SHOULD also be included in `caIssuers`.

(34) [ETSI] In subscriber certificates, the http URL to download the issuing CA certificate SHALL also be included in `caIssuers`.

qcStatements

(35) [QCP] In subscriber certificates, the following `qcStatements` SHALL be set :
- `qcs-QcCompliance(0.4.0.1862.1.1)`
- `qcs-QcPDS (0.4.0.1862.1.5)`
- `qcs-QcType (0.4.0.1862.1.6)` with one of the following values:
  - `qct-esign (0.4.0.1862.1.6.1)`
  - `qct-eseal (0.4.0.1862.1.6.2)`
  - `qct-web (0.4.0.1862.1.6.3)`

In addition, the following `qcStatements` MAY be set:
- `qcs-QcLimitValue (0.4.0.1862.1.2)`
- `qcs-QcRetentionPeriod (0.4.0.1862.1.3)`

`qcs-qcCClegislation (0.4.0.1862.1.7)` SHALL NOT be set.

Regarding the syntax of the `qcStatements`, [ETS4125] SHALL be considered.

(36) [QCP-n-qscd] [QCP-l-qscd] In subscriber certificates, `qcs-QcSSCD (0.4.0.1862.1.4)` SHALL be set.

cabfOrganizationIdentifier

(37) [EVCP] In subscriber certificates, the `cabfOrganizationIdentifier` SHALL be set if the `organizationIdentifier` is set and SHALL contain a reference to the registration of the organization according to [EVCG].

signedCertificateTimestampList

(38) [TLS] In subscriber certificates, at least three SCTs from two different CTLog operators SHALL be included in the "usable" status.

id-etsi-ext-valassured-ST-certs

(39) In short-term certificates, that cannot be revoked, `id-etsi-ext-valassured-ST-certs` SHALL be set. In short-term certificates, that can be revoked, `id-etsi-ext-valassured-ST-certs` SHOULD NOT be set. In subscriber certificates, that are not short-term certificates, `id-etsi-ext-valassured-ST-certs` SHALL NOT be set.

7.1.3 Algorithm object identifiers

Algorithms used for signing certificates SHALL comply with the requirements from [SOGIS].

CA certificates, that are based on an RSA key, SHALL use one of the following signature algorithms to sign the certificates they issue:

- `sha256WithRSAEncryption (1.2.840.113549.1.1.11)`, the Hex-coded value of the `AlgorithmIdentifier` SHALL be: `300d06092a864886f70d01010b0500`
- `sha384WithRSAEncryption (1.2.840.113549.1.1.12)`, the Hex-coded value of the `AlgorithmIdentifier` SHALL be: `300d06092a864886f70d01010c0500`
- `sha512WithRSAEncryption (1.2.840.113549.1.1.13)`, the Hex-coded value of the `AlgorithmIdentifier` SHALL be: `300d06092a864886f70d01010d0500`
- `rsassa-pss (OID 1.2.840.113549.1.1.10)`
    - MGF-1 with SHA-256, and a salt length of 32 bytes, the Hex-coded value of the `AlgorithmIdentifier` SHALL be: `304106092a864886f70d01010a3034a00f300d060960864801650304020105000a11c301a06092a864886f70d010108300d060960864801650304020105000a203020120`
    - MGF-1 with SHA-384, and a salt length of 48 bytes, the Hex-coded value of the `AlgorithmIdentifier` SHALL be: `304106092a864886f70d01010a3034a00f300d060960864801650304020205000a11c301a06092a864886f70d010108300d060960864801650304020205000a203020130`
    - MGF-1 with SHA-512, and a salt length of 64 bytes, the Hex-coded value of the `AlgorithmIdentifier` SHALL be: `304106092a864886f70d01010a3034a00f300d060960864801650304020305000a11c301a06092a864886f70d010108300d060960864801650304020305000a203020140`

CA certificates based on a P256 ECDSA key SHALL use `ecdsa-with-SHA256 (1.2.840.10045.4.3.2)` to sign the certificates they issue. The Hex-coded value of the `AlgorithmIdentifier` SHALL be: `300a06082a8648ce3d040302`

CA certificates based on a P384 ECDSA key SHALL use `ecdsa-with-SHA384 (1.2.840.10045.4.3.3)` to sign the certificates they issue. The Hex-coded value of the `AlgorithmIdentifier` SHALL be: `300a06082a8648ce3d040303`

For certificates based on RSA keys, `rsaEncryption (1.2.840.113549.1.1.1)` SHALL be set with `NULL` parameter in the `subjectPublicKeyInfo`. The hex-encoded value of the `AlgorithmIdentifier` SHALL be: `300d06092a864886f70d01010500`.

For certificates based on ECDSA keys, `ecPublicKey (1.2.840.10045.2.1)` SHALL be set without `NULL` parameter and depending on the used curve of one of the following OIDs of the `subjectPublicKeyInfo`:

- P256: `prime256v1 (1.2.840.10045.3.1.7)`, the Hex-coded value of the `AlgorithmIdentifier` SHALL be: `301306072a8648ce3d020106082a8648ce3d030107`
- P384: `secp384r1 (1.3.132.0.34)`, the Hex-coded value of the `AlgorithmIdentifier` SHALL be: `301006072a8648ce3d020106052b81040022`

Algorithms and parameters used SHALL be listed in the CPSs.

7.1.4 Name forms

General regulations:

- The `issuerDN` of a certificate SHALL correspond to the `subjectDN` of the issuing certificate "byte-by-byte".
- In CA certificates, all attributes SHALL NOT be set more than once.
- In subscriber certificates, the following attributes of the `subjectDN` SHALL NOT be set more than once:
  - `commonName`
  - `organizationIdentifier`
  - `organizationName`
  - `countryName`
- `subjectDN` attributes SHALL NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

The following table provides an overview of mandatory and optional `subjectDN` attributes for CA, subscriber and OCSP Signer certificates[9].

The following conventions apply:

- **M** (mandatory): this attribute SHALL be set.
  (M) this attribute SHALL be set only under certain circumstances.
- **O** (optional): this attribute MAY be set.
- **S** (should): this attribute SHOULD be set.
- **SN** (should not): this attribute SHOULD NOT be set.
- **N** (not allowed): this attribute SHALL NOT be set.
- **(#)** Reference to the description of the contents to be set following the table.

[9] CRL Signer certificates are not listed due to CRLs being currently directly issued by the corresponding CA.

Table 3 - Name forms

Subject-DN attribute (OID)	Root CA	Sub CA	Subscriber	OCSP-Signer
commonName (2.5.4.3)	M (01)(02)	M (01)	M, [TLS] O (03)(04)	M
serialNumber (2.5.4.5)	N	N	(M) (05)(06)	N
givenName (2.5.4.42)	N	N	(M) (07)(08)	N
surname (2.5.4.4)	N	N	(M) (09)(10)	N
pseudonym (2.5.4.65)	N	N	(M) (11)	N
streetAddress (2.5.4.9)	N	N	O (12)(13)	N
localityName (2.5.4.7)	N	N	(M) (14)(15)	N
stateOrProvinceName (2.5.4.8)	N	N	(M) (16)(17)	N
postalCode (2.5.4.17)	N	N	(M) (18)(19)	N
businessCategory (2.5.4.15)	N	N	(M) (20)	N
organizationalUnitName (2.5.4.11)	N	N	O, [TLS] N	N
organizationIdentifier (2.5.4.97)	N, [QCP] O	(S) (21)(22)	(M) (23)(24)	N
jurisdictionOfIncorporation-LocalityName (1.3.6.1.4.1.311.60.2.1.1)	N	N	(M) (25)	N
jurisdictionOfIncorporation-StateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2)	N	N	(M) (26)	N
jurisdictionOfIncorporation-CountryName (1.3.6.1.4.1.311.60.2.1.3)	N	N	(M) (27)	N
organizationName (2.5.4.10)	M (28)	M (28)	(M) (29)(30)(31)	M
countryName (2.5.4.6)	M	M	M, [TLS] (M) (32)(33)(34)	M
Other attributes	N	N	O, [TLS] N	N

The contents are described below if there are requirements that go beyond the standards.

commonName

(01) In CA certificates, the commonName SHALL contain a name that is unique across all certificates generated by the issuing CA. The commonName SHALL include a common name (i.e., not necessarily the full registered name) of the TSP and SHALL be chosen in a language common to the TSP's market.

(02) In Root CA certificates the commonName SHALL NOT be reused, i.e., in subsequent certificates another commonName SHALL be assigned.

(03) [TLS] In subscriber certificates, the `commonName` MAY be set. If set, it SHALL contain exactly one entry that is also contained in the `subjectAltName`. Regarding the encoding of the commonName applies:
- IPv4 addresses SHALL be encoded according to [RFC3986],
- IPv6 addresses SHALL be encoded according to [RFC5952#4],
- FQDN and wildcard domain names SHALL be a character-by-character copy of the corresponding `dNSName` entry from the `subjectAltName` (see chapter 7.1.2).

(04) [EVCP] In subscriber certificates, the `commonName` MAY be set. If set, it SHALL contain exactly one domain name that the subject owns or has under its control and that is associated with the subject's server. The server may be owned or operated by the subject or a third party (e.g. hosting service provider). Wildcard certificates SHALL NOT be issued, with the exception of "onion" certificates[10].

`serialNumber`

(05) [ETSI] In subscriber certificates the `serialNumber` SHALL be set if `countryName`, `commonName` as well as `givenName` and `surname` or `pseudonym` are not sufficient to ensure the uniqueness of the name. `serialNumber` has no defined semantics beyond ensuring the uniqueness of the `subjectDN`.

(06) [EVCP] In subscriber certificates, the `serialNumber` SHALL contain the legally assigned number (incorporation number or similar number) of the organization. If no such number has been assigned, the date of incorporation SHALL be set in a common date format. For Government Entities and Non-Commercial Organizations that cannot provide a registration number or date of incorporation, an appropriate description SHALL be included to indicate that the organization is a Government Entity or a Non-Commercial Organization.

`givenName`

(07) [IVCP] In subscriber certificates the `givenName` MAY be set. If the `givenName` is set, it SHALL contain the name of the subject together with the `surname`.

(08) [ETSI] In subscriber certificates for natural persons either `surname` and `givenName` or `pseudonym` SHALL be set. In subscriber certificates for organizations these fields SHALL NOT be set.

`surName`

(09) [IVCP] In subscriber certificates the `surname` MAY be set. If `surname` is set, it SHALL contain the name of the subject together with the `givenName`.

[10] See Appendix F of CABF EV Guidelines

(10) [ETSI] In subscriber certificates for natural persons either `surname` and `givenName` or the `pseudonym` SHALL be set. In subscriber certificates for organizations these fields SHALL NOT be set.

pseudonym

(11) [ETSI] In subscriber certificates for natural persons the `pseudonym` SHALL be set if `surname` and `givenName` are not set, otherwise `pseudonym` SHALL NOT be set. If the `pseudonym` is set, `countryName` SHOULD be set with the value "DE" (country of CA's location). For certificates for natural persons in association with an organization, the country of the organization's location MAY alternatively be set as the `countryName`.

streetAddress

(12) [TLS] In subscriber certificates, the `streetAddress` MAY be set if `surname` and `givenName` or `organizationName` are set, otherwise `streetAddress` SHALL NOT be set.

(13) [EVCP] If `streetAddress` is set, it SHALL contain the physical address of the subject's place of business.

localityName

(14) [TLS] In subscriber certificates the `localityName` SHALL be set if `surname` and `givenName` or `organizationName` are set and `stateOrProvinceName` is not set. It MAY be set if `stateOrProvinceName` and `surname` and `givenName` or `organizationName` are set. It SHALL NOT be set if `surname` and `givenName` or `organizationName` are not set.
Note: If the attribute `countryName` contains the code "XX", the attribute `localityName` MAY contain the city and / or the state or province of the subject.

(15) [EVCP] If `localityName` is set, it SHALL contain the physical address of the subject's place of business.

stateOrProvinceName

(16) [TLS] In subscriber certificates, the `stateOrProvinceName` SHALL be set if `surname` and `givenName` or `organizationName` are set and `localityName` is not set. `stateOrProvinceName` MAY be set if `localityName`, `surname` and `givenName` or `organizationName` are set. It SHALL NOT be set if `surname` and `givenName` or `organizationName` are not set.

(17) [EVCP] If `stateOrProvinceName` is set, it SHALL contain the physical address of the subject's place of business.

postalCode

(18) [TLS] In subscriber certificates, the `postalCode` MAY be set if `surname` and `givenName` or `organizationName` are set. Otherwise, it SHALL NOT be set.

(19) [EVCP] If `postalCode` is set, it SHALL contain the physical address of the subject's place of business.

businessCategory

(20) [EVCP] In subscriber certificates, the `businessCategory` attribute SHALL be set with the applicable organization type (see Section 1.3.3)

organizationIdentifier

(21) [ETSI] In Sub CA certificates the `organizationIdentifier` SHOULD be set and contain a registration number of the certificate owner according to the following scheme:
- three characters for the registration scheme (VAT or NTR) or two characters of a country-specific registration scheme followed by a colon
- two characters for the country code[11]
- a hyphen ("-")
- reference assigned according to the identified registration scheme

(22) [TLS] In Sub CA certificates, the `organizationIdentifier` SHALL NOT be set.

(23) [EVCP] In subscriber certificates the `organizationIdentifier` MAY be set. If set, it SHALL include a reference to the registration of the organization as follows:
- three characters for the identifier of the registration scheme (VAT, NTR or PSD)
- two characters for the country code[11]
- a hyphen ("-")
- reference assigned according to the identified registration scheme

(24) [ETSI] In subscriber certificates for organizations, the `organizationIdentifier` SHALL be set and SHALL include a reference to the registration of the organization as follows:
- three characters for the registration scheme (VAT or NTR) or two characters of a country-specific registration scheme followed by a colon
- two characters for the country code[11]
- a hyphen ("-")
- reference assigned according to the identified registration scheme

[11] ISO 3166 country codes, in case of NTR also two characters for country and two characters for state or province, separated by a "+"

jurisdictionOfIncorporationLocalityName

(25) [EVCP] In subscriber certificates, the `jurisdictionOfIncorporationLocalityName` SHALL be set if the registration entity acts at the local level. If the registration authority acts on national or state level, `jurisdictionOfIncorporationStateOrProvinceName` SHALL NOT be set.

jurisdictionOfIncorporationStateOrProvinceName

(26) [EVCP] In subscriber certificates, the `jurisdictionOfIncorporationStateOrProvinceName` SHALL be set if the registration entity acts at the state or local level. If the registration authority acts on the national level, `jurisdictionOfIncorporationStateOrProvinceName` SHALL NOT be set.

jurisdictionOfIncorporationCountryName

(27) [EVCP] In subscriber certificates the `jurisdictionOfIncorporationCountryName` SHALL be set[11].

organizationName

(28) [TLS] In Root or Sub CA certificates, the `organizationName` SHALL be set and it SHALL contain the full registered name of the TSP.

(29) [TLS] In subscriber certificates, the `organizationName` MAY be set. If set, it SHALL contain the validated name of the subject. This may be set in slightly modified form (e.g. common abbreviations or usages), provided that this is traceable.

(30) [EVCP] In subscriber certificates, the `organizationName` SHALL be set and SHALL contain the full legal name of the organization. Common and unambiguous abbreviations MAY be used or, in order not to exceed the maximum length of 64 characters, non-critical name components MAY also be omitted, provided the name is still unambiguously recognizable. If this is not possible, the requested certificate SHALL NOT be issued. An alias MAY be included at the beginning of the field if the full legal name is added thereafter.

(31) [ETSI] In subscriber certificates for organizations, the `organizationName` SHALL be set and it SHALL contain the full legal name of the subject.

countryName

For the encoding of the `countryName` for countries that are not represented by a two-character country code, refer to ISO 3166-1.

(32) [ETSI] Regarding the values to be set for `countryName` in subscriber certificates in association with the `pseudonym`, see (08) above.

(33) [TLS] In subscriber certificates the `countryName` SHALL be set if `surname` and `givenName` or `organizationName` are set, otherwise it MAY be set.

(34) If the attribute is set, it SHALL contain the physical address of the subject's place of business.

7.1.5 Name constraints

`nameConstraints` SHALL NOT be set in Root CA and subscriber certificates, but MAY only be set in Sub CA certificates.

[TLS] [SMIME] In Sub CA certificates, `nameConstraints` SHALL be set if the Sub CA certificates are to be technically constrained. In this case, the `extendedKeyUsage` SHALL also be set with `id-kp-serverAuth` or `id-kp-emailProtection`. If the `extendedKeyUsage` is set with `id-kp-serverAuth`, the `nameConstraints` SHALL contain constraints for `dNSName`, `iPAddress`, and/or `directoryName`. If the `extendedKeyUsage` is set with `id-kp- emailProtection`, the `nameConstraints` must contain constraints for `rfc822Name` with at least one allowed name.

7.1.6 `certificatePolicies` object identifier

See Section 7.1.2.

7.1.7 Usage of `policyConstraints` extension

No stipulation.

[ETSI] In subscriber certificates, `policyConstraints` SHALL NOT be set.

7.1.8 `policyQualifiers` syntax and semantics

The `policyQualifiers` SHALL be set conforming to [RFC5280] with the contents defined in Section 7.1.2.

7.1.9 Processing semantics for `certificatePolicies`

`certificatePolicies` SHALL NOT be marked as critical, so it is up to the decision of the certificate users to evaluate this extension.

7.2 CRL profile

All revocation lists SHALL comply with the requirements of [RFC5280] and be signed by the respective CA itself.

The algorithms listed in Section 7.1.3 SHALL be used for signing the revocation lists.

7.2.1 Version number(s)

All revocation lists SHALL be issued in X.509 version 2 format.

7.2.2 CRL and CRL entry extensions

All revocation lists SHALL contain at least the `authorityKeyIdentifier` and `cRLNumber` CRL extensions.

CARLs SHALL contain the CRL entry extension `reasonCode` (not marked as critical).

If expired certificates are not removed from the revocation list, the revocation list SHALL contain the `expiredCertsOnCRL` extension. If expired certificates are removed from the revocation list, the revocation list SHALL NOT contain `expiredCertsOnCRL`.

[TLS] CRLs SHALL contain the CRL entry extension `reasonCode` (not marked as critical), if any of the following revocation reasons exist (see also Section 4.9.1.2, and [MOZRP#6.1.1]):

- `keyCompromise`
- `privilegeWithdrawn`
- `cessationOfOperation`
- `affiliationChanged`
- `superseded`

If the revocation reason does not match any of the above-mentioned revocation reasons, the `reasonCode` SHALL NOT be set.

All extensions SHALL NOT be marked as critical.

7.3 OCSP Profile

All OCSP responses SHALL meet the requirements of [RFC6960] and SHALL be signed either by the CA itself or by an OCSP Signer whose certificate has been issued by the CA.

If the OCSP responses are signed by a dedicated OCSP Signer, then according to [RFC6960], one of the following options SHALL be chosen for the OCSP Signer certificate:

- The OCSP Signer can be trusted for the lifetime of the OCSP Signer certificate. In this case, `id-pkix-ocsp-nocheck` SHALL be set in the OCSP Signer certificate and contain the value `NULL`. In this case, `cRLDistributionPoints` and `authorityInfoAccess` SHOULD NOT be set in the OCSP Signer certificate and the OCSP Signer certificate SHOULD have a short validity period and be renewed periodically due to the lack of ability to check its status.
- A checking capability of the OCSP Signer certificate in `cRLDistributionPoints` and/or `authorityInfoAccess` is set.
- No method for checking the status of the OCSP Signer is specified, leaving it up to the verifier to decide whether and how to check the status of the OCSP Signer certificate.

[TLS] [SMIME] If the OCSP responses are signed by a delegated OCSP Signer, the first of the variants above SHALL be selected for the OCSP Signer certificate.

The algorithms listed in Section 7.1.3 SHALL be used for signing the OCSP responses.

[TLS] OCSP responses for revoked certificates SHALL contain the revocation reason in the `revocationReason` attribute within the `revokedInfo` (not in the extensions, see Section 7.3.2). The specifications made in Section 7.2.2 apply with regard to the revocation reasons.

7.3.1 Version number(s)

OCSP in version 1 according to [RFC6960] SHALL be used.

7.3.2 OCSP extensions

No stipulation.

[TLS] The `reasonCode` extension according to [RFC5280#5.3.1] SHALL NOT be set in OCSP responses (see also Section 7.3).

[QCP] The `archiveCutOff` extension SHOULD be set in the response with the time of the validity start of the referenced CA certificate.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

8.1.1 Internal audits

No stipulation.

[TLS] Compliance with the requirements of this CP and the applicable CPS, as well as their quality of service, SHALL be monitored through appropriate internal audits during the period in which subscriber certificates are issued. These internal audits SHALL be conducted at least quarterly and SHALL include random sampling of at least three percent of the subscriber certificates (resp. six percent in the case of EV certificates) issued since the last internal audit.

Furthermore, certificates issued by delegated third parties or containing information verified by delegated third parties SHALL be audited at least quarterly, unless the delegated third party is audited itself according to Section 8.1.2.

In addition, the practices and procedures of all delegated third parties SHALL be reviewed at least annually for compliance with the requirements of this CP and the applicable CPS.

8.1.2 External Audits

No stipulation.

[TLS] [SMIME] Trust Services SHALL be audited in a continuous sequence of audit periods from the generation of a CA key pair to its destruction and withdrawal of trust ("cradle-to-grave") according to an audit scheme listed in Section 8.4 ("period-of-time audits"), whereby a period SHALL NOT exceed the duration of one year

[3145] Trust Services SHALL be audited annually according to Section 8.4.

[QCP] Trust Services SHALL be audited by a Conformity Assessment Body at least every 24 months.

8.1.3 Audits of subcontractors and delegated third parties

No stipulation.

[TLS] It SHALL be verified that delegated third parties meet the requirements for document retention and event logging as specified in Section 5.4.1.

[3145] Subcontractors or delegated third parties SHALL be audited in the applicable areas to the same extent in accordance with the requirements of [3145] as the operation of the TSP itself. This requirement SHALL be contractually agreed with the subcontractors or delegated third parties.

8.2 Identity/qualifications of assessor

Internal auditors performing the internal audits according to Section 8.1.1 and the audits of subcontractors and delegated third parties according to Section 8.1.3 SHALL have sufficient experience as auditors and expertise in PKI technologies and processes.

External auditors performing audits in accordance with Section 8.1.2 SHALL be qualified auditors who have the following qualifications and skills, i.e., they SHALL

- be independent from the subject of the audit,
- be able to conduct audits that addresses the criteria specified in eligible audit schemes according to Section 8.4,
- employ individuals who have proficiency in examining PKI technologies, information security tools and techniques, information technology and security auditing and the third-party attestation function,
- be bound by law, government regulations, or professional code of ethics.

[TLS][SMIME] External auditors SHALL maintain a professional liability errors and omissions insurance with coverage of at least one million dollars.

For auditing according to the ETSI standards, the evaluation body SHALL also be accredited by “DAkkS” (German Accreditation Body) according to ISO 17065 using the requirements defined in ETSI EN 319 403 and SHALL be a member of the „Accredited Conformity Assessment Bodies‘ Council“ (ACAB’c).

[QCP] The Trust Services SHALL be audited by Conformity Assessment Bodies meeting the requirements of ETSI EN 319 403.

[3145] Audits SHALL be performed by ISO 27001 auditors.

8.3 Assessor's relationship to assessed entity

External auditors performing the audits according to Section 8.1.2 SHALL be independent of the audited entity and item.

For internal auditors, the separation of roles according to Section 5.2.4 SHALL be observed.

8.4 Topics covered by assessment

No stipulation.

[TLS] [SMIME] The Trust Services SHALL be audited according to ETSI EN 319 411-1 or ETSI 319 411-2 in the then current version.

[TLS] Applicable policies are

- IVCP,
- DVCP,
- OVCP,
- QNCP-w.

[SMIME] Applicable policies are

- LCP,
- NCP or
- NCP+.

[EVCP] Applicable Policies are

- EVCP or
- QEVCP-w

The audits SHALL include all Root CAs and non-restricted Sub CAs as well as cross-certificates. The audit documentation SHALL document all audited PKI hierarchies.

[QCP] The Trust Services SHALL be audited according to ETSI EN 319 411-2 in the then current version.

Applicable policies are

- QCP-n,
- QCP-l,
- QCP-n-qscd,
- QCP-l-qscd,
- QEVCP-w or
- QNCP-w.

Furthermore, a conformity assessment according to [eIDAS] SHALL be performed

[3145] The audit process SHALL include the ISMS and the requirements of [TR3145].

8.5 Actions taken as a result of deficiency

Deficiencies SHALL be corrected within the timelines set by the internal or external auditors.

[TLS] [SMIME] Deficiencies that violate the [BR], [EVCG], [MSRP], [MOZRP], [GCRP] or [APLRP] SHALL be reported to the affected Root Store operators. Provided that faulty certificates are complained, the revocation reasons and timelines according to Section 4.9.1 SHALL be taken into account.

8.6 Communication of results

No stipulation.

[TLS] [SMIME] The links to the audit attestations of all technically unrestricted CAs issued and published by the external auditors SHALL be published in the "Common CA Database" (CCADB).

These attestations SHOULD be published within three months after the end of the audit. In case of a delay of more than three months, a letter of explanation signed by the external auditor SHALL be provided.

When preparing the audit attestations, the external auditors SHALL consider the requirements on form and content from [CCADB#5.1] ("Audit Statement Content", see https://www.ccadb.org/policy).

[QCP] Conformity Assessment Reports of the audits SHALL be submitted in accordance with Section 8.1.2 to the appropriate supervisory body within three days of receipt.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

[QCP] Status information SHALL be provided free of charge.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

The TSPs SHALL have the financial stability and resources necessary to operate in compliance with this CP, including a planned termination in accordance with Section 5.8. In addition, the TSPs SHALL, to the extent possible under applicable insolvency laws, have arrangements in place to cover the costs of meeting the minimum requirements of Section 5.8 in the event of insolvency.

9.2.1 Insurance coverage

TSPs SHALL have adequate liability insurance in accordance with applicable law if they do not have sufficient financial resources to cover any liability claims arising from intentional or negligent acts.

[EVCP] The TSPs SHALL have a liability insurance policy with respect to its Trust Services and obligations under this CP as follows:

- a general liability insurance with coverage of at least $2 million
- a professional liability insurance policy with coverage of at least $5 million, which covers claims for damages arising out of
  - an act, error or omission
  - an unintentional breach of contract
  - an act of neglect in the issuance or operation of EV certificates
  - a violation of third-party proprietary rights (excluding copyright and trademark violations)
  - a violation of privacy
  - a violation of advertising.

This insurance SHALL be with a company rated no less than "A" in the current edition of "Best's Insurance Guide".

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

Confidential business information SHALL be protected according to its classification.

9.4 Privacy of personal information

9.4.1 Privacy plan

The requirements of the German "Bundesdatenschutzgesetz" [BDSG] SHALL be complied with and data, that is not relevant or appropriate for the provision of the service SHALL NOT be collected.

The privacy plans SHALL describe how the provisions of the [BDSG] with regard to the data collected in the registration process are implemented. Appropriate technical and organizational measures SHALL be taken to maintain integrity and confidentiality during transmission and storage and to protect the data against unauthorized or unlawful processing or accidental loss or destruction or damage.

9.4.2 Information treated as private

No stipulation.

9.4.3 Information not deemed private

No stipulation.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

No stipulation.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The TSPs SHALL be reliable and operate their Trust Services in a trustworthy and legal manner compliant with this CP and their CPSs.

The TSPs SHALL retain overall responsibility for compliance with this CP and their CPSs even if they outsource activities to subcontractors or third parties e.g., providers of Trust Service Components or external RAs. To this end, the tasks of the third parties and the associated procedures, responsibilities and liability conditions SHALL be defined and they SHALL be contractually obliged to implement all the required measures. Third party obligations SHALL be described in the CPS.

If Trust Service Components provided by a Trust Service Component Provider are used, it SHALL be ensured that

- the use of the component's interface complies with the requirements specified by the Trust Service Component Provider,
- the security and functionality required by the Trust Service Component comply with the relevant requirements of this CP and the relevant CPSs.

When independent third-party data sources are used to validate data ("QIIS", see Section 3.2.2), they SHALL be evaluated with respect to their reliability, accuracy, and resistance to alteration or falsification. The following SHALL be considered:

- Age of the information provided
- Frequency of updates to the information source
- Data provider and the purpose of the data collection
- Availability of the data
- Integrity of the data (i.e., the relative difficulty of falsifying or altering it)

Databases maintained by the TSP or its affiliates themselves SHALL NOT be considered reliable data sources if the primary purpose of the databases is to collect information to meet validation requirements.

[3145] If third parties provide services to a TSP as part of the identification and registration process, a "high" security level for the third parties SHALL be ensured and the reliability of the third party as well as the trustworthiness of the personnel used by the third party SHALL be required. For this purpose, a signed agreement SHALL be concluded with the third party, which in addition also includes the aspects listed in the previous Section.

Trust Services SHALL NOT be discriminatory and SHOULD be made available to all applicants,

- whose activities fall within the scope of activities specified by the services and
- who agree to comply with their obligations set forth in the respective terms and conditions.

Trust Services SHALL be made accessible to people with disabilities as far as possible. Applicable accessibility standards from ETSI EN 301 549 SHOULD be taken into account.

Third parties SHALL be given the possibility to validate and test all offered certificate types.

[TLS] Telekom Security as the operator of the Root CAs is responsible for

- the services and warranties of the TSP,
- the TSP's compliance with this CP,
- all liabilities and indemnification obligations of the TSP according to [BR].

For each certificate issued, it SHALL be guaranteed to both the subscribers and the Root Store operators, with whom Telekom Security has an agreement to include the Root CA certificates in the Root Stores, as well as to all relying parties that

- the subscriber has the right to use the domain names or IP addresses listed in the certificate (in the `subjectDN` and/or `subjectAltName`)
- if applicable, the applicant was authorized to apply for the certificate on behalf of the subscriber,
- the TSP was authorized by the subscribers to issue the certificates,
- the accuracy of all content included in the certificate was validated,
- the subscriber has been identified according to Section 3.2,
- if the subscriber is not affiliated with the TSP, the TSP has entered into a legally valid and enforceable contract with the subscriber that meets all relevant requirements,
- if the subscriber is affiliated with the TSP, a representative of the subscriber has acknowledged the Terms of Use,
- the TSP operates status services in accordance with Section 4.10 at least until the expiration date of the certificates and makes status information available to the public on a 24-hour basis
- the TSP revokes a certificate if one of the reasons for revocation listed in the CPS applies,
- she complies with the requirements of this CP and the respective CPSs during the entire validity period of a certificate

The processes and measures required to comply with the aforementioned certificate guarantees SHALL be described in the CPSs.

An appropriate communication channel to all subscribers SHALL exist to inform them about changes if needed.

The agreements with subscribers including the Terms of Use (see Section 9.6.3) SHALL be legally enforceable. Acceptance of the agreement MAY be electronic, if legally enforceable. A separate agreement for each certificate MAY be accepted as well as an agreement that applies to multiple certificates.

[EVCP] For each EV certificate issued, it SHALL be ensured that

- the subscriber exists as a legally valid organization, verified with an incorporation or registration agency in the subscriber's incorporation or registration jurisdiction,
- the name of the subscriber at the time of issuance of the certificate is the same as the name in the official registration documents,
- all reasonable steps are taken to verify that
  - the subscriber has the right to use all domain names listed in the certificate at the time of issuance of the certificate,
  - the subscriber has authorized the issuance of the Certificate,
  - all other information in the certificate was correct at the time the certificate was issued,
- a legally valid and enforceable agreement with a subscriber, that is not affiliated, is concluded, which takes into account all requirements from [EVCG].

[QCP] If the private keys of the subscribers are managed by the TSP during the validity period of the corresponding certificates, this SHOULD be described in the CPSs. In addition, this information MAY also be included in the subscriber certificate.

9.6.2 RA representations and warranties

The representations and warranties of RAs SHALL be defined and described in the CPS, taking into account at least

- application processing according to Section 4,
- organizational measures according to Section 5.2,
- personnel measures according to Section 5.3,
- archiving of documents according to Section 5.5 and
- technical measures according to Section 6.5.

9.6.3 Subscriber representations and warranties

The Terms of Use for subscriber certificates SHALL be defined and the subscribers SHALL have confirmed their acceptance before the certificates are issued. These Terms of Use SHALL consider at least the following obligations of subscribers:

a) an obligation to provide accurate and complete information,
b) an obligation to take all reasonable measures to ensure confidentiality and control over private keys and activation data,
c) an obligation to use the key pair only in accordance with any restrictions communicated to the subscriber,
d) a prohibition on the unauthorized use of the private subscriber keys,
e) an obligation to revoke or have a certificate revoked without delay if there is a reason for revocation according to Section 4.9.1.2.
f) an obligation to immediately and permanently cease using the private key, except for key decryption (if applicable), after revocation of the subscriber certificate,
g) an obligation to immediately and permanently cease using the private key, except for key decryption (if applicable), once the compromise of the issuing Sub CA has become known,
h) if a subscriber generates its keys itself: An obligation to generate the keys using suitable algorithms and key lengths according to Section 6.1.5,
i) in the case where the subscriber is a natural person and generates its keys itself and these are used for a "signed content commitment" (see Section 7.1.2 (06) regarding KeyUsage "nonRepudiation"): a commitment that the private key is kept under the sole control of the end entity,
j) in the case where the subscriber is a legal person and generates its own keys and uses them for a "signed content commitment" (see Section 7.1.2 (06) regarding KeyUsage „nonRepudiation“): a commitment that the private key is kept under the sole control of the end entity,

k) [NCP+] a commitment to use the private key for cryptographic functions only within secure cryptographic modules,
l) [NCP+] in the case that the keys are generated under the control of the subscriber: a commitment to generate the keys within the secure cryptographic module,

m) [TLS] an obligation to verify the content of the certificate for accuracy,
n) [TLS] an obligation to install the certificate only on servers that can be accessed under the names listed in the certificate attribute `subjectAltName`,
o) [TLS] an obligation to use the certificate only in accordance with all applicable laws and with the concluded agreement and the terms of use,
p) [TLS] an obligation to respond to the TSP's instructions within a specified period of time in the event of compromise of a key or certificate misuse,
q) [TLS] an obligation to accept that the TSP is entitled to revoke a certificate immediately if there is a reason for revocation in accordance with Section 4.9.1.2,

r) [3145] an obligation to notify the TSP of any change in the registration data and to confirm that the registration data is still valid at the latest after the expiry of the period specified in rr)
s) [3145] if the subscriber generates the keys itself: an obligation to generate and retain the keys in accordance with the specifications (cf. Sections 6.1.5 and 6.1.6),
t) [3145] if the TSP generates and hands over the keys of the subscriber on a token: an obligation to report a compromise of the activation data in the course of token handover, which leads to a revocation of the certificate,
u) [3145] an obligation to verify the subscriber certificate as well as the issuing Sub CA certificate,

x) [QCP-n-qscd] an obligation to keep the key under its sole control,
y) [QCP-l-qscd] an obligation to keep the key under the control of the subject of the certificate,
z) [QCP-n-qscd] an obligation to use the key only for generating electronic signatures,
aa) [QCP-l-qscd] an obligation to use the key only for the generation of electronic seals.

In addition, the Terms of Use SHALL contain information on the following aspects:

bb) if applicable, the applicable policy according to ETSI EN 319 411-1 resp. -2,
cc) an information what is considered as acceptance of the certificate,
dd) the period for which the records are kept (see Section 5.5.2),
ee) the requirements for relying parties according to Section 9.6.4,
ff) whether, and if so in what way, the requirements of this CP will be supplemented or further restricted,
gg) any restrictions on the use of the services provided,
hh) the limitations of liability of the TSP,
ii) the applicable law,
jj) the procedures for complaints and dispute resolution,
kk) frequency and applicable audit schemes of the audits of the TSP according to Sections 8.1 and 8.4,
ll) contact information of the TSP,
mm) statements on the availability of the services provided,
nn) the revocation reasons to be chosen in the event of revocation by the subscriber,

oo)	[3145] the way in which the subscribers can transmit the registration data,
pp)	[3145] regulations on the acceptance of new versions of the Terms of Use by the subscribers in accordance with the applicable laws,
qq)	[3145] a definition of the various roles of the subscribers, the various possible subjects of a certificate and other significant roles in the certificate management processes (see Section 1.3.3)
rr)	[3145] a time limit after which subscribers must confirm, that the registration data is still valid,
ss)	[3145] further requirements for subscribers depending on the required security level (e.g., virus protection, firewalls as well as security updates of operating systems, adequate protection of keys and activation data, use of secure cryptographic modules in case of high security level),
tt)	[3145] if the subscriber generates the keys itself: the requirements for the hardware and software used to generate the keys,
uu)	[3145] if the TSP generates subscriber keys: the process of handing over the keys,
vv)	[3145] if the TSP generates and hands over subscriber keys on token: the process of handing over the token,
ww)	[3145] the requirements for certificate renewal with or without key change and for issuing a replacement certificate,
xx)	[3145] The periods and circumstances under which modification of certificate data is permitted or required,
yy)	[3145] information about the process of termination according to Section 5.8,
zz)	information about the periods of the regular updates of the status services.

aaa)	[VS-NfD] Classification of key material according to [SÜG] and [VSA].

In case the subscriber is not the subject of the certificate and the subject of the certificate is not a device

1) the above-mentioned obligations c), d), e), f), g), i) j) and k) SHALL apply to the subject of the certificate and in case the subject of the certificate is a person, the person SHALL be informed about it,
2) the agreement with the subscriber SHALL consist of two parts,
   a) the first part SHALL be signed by the subscriber and SHALL consider the following aspects:
      i) consent to the obligations of the subscriber,
      ii) consent to the use of a secure cryptographic module, if required,
      iii) consent to the processing of the collected data and, if applicable, the transfer of this data to third parties contracted by the TSP, including a transfer of the data in case of termination of the service,
      iv) conditions for publication of the certificate at the request of the subscriber with the consent of the subject of the certificate,
      v) confirmation of correctness of all data to be included in the certificate,
      vi) obligations applicable to the subject of the certificate (informative).
   b) The second part SHALL be signed by the subject of the certificate and SHALL consider the following aspects:
      i) consent to the obligations of the subject of the certificate (see Section 1)),
      ii) consent to the use of a secure cryptographic module, if required,
      iii) consent to the processing of the collected data and, if applicable, the transfer of such data to third parties contracted by the TSP, including a transfer of the data in the event of termination of the service.

The Terms of Use MAY be provided in the form of a PDS according to [ETS411-1#Annex A].

9.6.4 Relying party representations and warranties

The following recommendations for relying parties SHALL be included in the Terms of Use (see also Section 9.6.3) and/or the PDS.

Relying parties SHOULD

- check the validity of the certificates via the offered status services according to Section 4.9.10 and 4.10,
- consider the restrictions on the use of the certificates set out in the terms of use or in the certificate,
- take all further precautions arising for third parties from agreements or other regulations.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

The liability of the TSP MAY be limited in accordance with applicable law. The limitations of liability SHALL be described in the CPSs as well as in the Terms of Use, see also Section 9.6.3 para. hh).

[EVCP] The liability to subscribers or relying parties for legally recognized and provable claims SHALL NOT be limited to a monetary amount of less than two thousand U.S. dollars per subscriber or relying party per subscriber certificate.

[QCP] The TSP SHALL be liable under Article 13 of EU Regulation 910/2014 ("eIDAS") for any damage caused intentionally or negligently to a natural or legal person.

9.9 Indemnities

No stipulation.

9.10 Term and termination of this CP or a CPS

9.10.1 Term

This CP and all CPSs based on it have a maximum validity period of one year, see also Section 9.12.

9.10.2 Termination

No stipulation.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments to this CP or a CPS

9.12.1 Procedure for amendment

This CP SHALL be reviewed by the Trust Center's PKI Compliance Management as needed, e.g., due to changed requirements or relevant changes in operations, but at least once per year. The PKI Compliance Management SHALL therefore regularly review, at appropriate intervals, the underlying requirements of the documents referenced in Annex B for new versions and monitor activity in relevant forums.

Changes to this CP as well as the annual review SHALL be listed in the revision history of this document. This applies even if no substantive changes are made at the annual review.

New versions of this CP SHALL be approved according to Section 1.5.4 and shall be assigned a new ascending version number.

Similarly, the CPSs SHALL be reviewed by the Trusted Services due to changed requirements or relevant changes in operation, but at least once per year. Regarding the change history, approval procedure and versioning, the above applies.

If changes are made to the CPS that affect the Terms of Use, the Terms of Use SHALL be amended and provided in a new version.

9.12.2 Notification mechanism and period

New versions of this CP SHALL be published according to the specifications of Section 2.2. All affected Trusted Services SHALL be informed at the latest when a new version is published.

New versions of a CPS or the Terms of Use SHALL be published according to the specifications of Section 2.2. At the latest with the release of a new version, all affected Trust Service staff SHALL be informed.

The subscribers and, if applicable, relying parties SHALL be informed about new versions of the Terms of Use if they contain new or changed conditions that also affect the use of already issued certificates or keys. When announcing the changes, reference MAY be made to the changed documents in the repository with regard to the details.

[3145] Acceptance of new Terms of Use, which contain new or modified conditions that also affect the use of already issued certificates or keys, SHALL be obtained from the subscriber. Regarding the regulations for the acceptance of new Terms of Use besides the application processes, see Section 9.6.3 pp).

[QCP] New versions of a CPS SHALL be communicated to the supervisory authorities.

9.12.3 Circumstances under which OID must be changed

If there are changes to this CP or to a CPS that affect the applicability of the respective document, the document SHOULD be given a new OID.

9.13 Dispute resolution provisions

Policies and procedures for resolving complaints and disputes received from subscribers or relying parties regarding the Trust Services SHALL be established and described in the CPSs and Terms of Use .

9.14 Governing law

German law SHALL be set as the applicable law in the CPSs.

9.15 Compliance with applicable law

The TSP SHALL ensure that they comply with applicable law and provide evidence of how they comply with applicable legal requirements as needed.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

[TLS] In the case of a conflict between [BR] and a law, any conflicting requirement MAY be modified to the extent necessary to make the requirement valid and legal. This applies only to operations or certificate issuances subject to this law. In such a case, a detailed reference to the law requiring modification of those requirements under this section SHALL be given in the CPS, as well as the specific modification of those requirements made by the TSP. Before issuing a certificate under the modified requirements, the CA/Browser Forum SHALL be informed of the relevant passages of the modified Section (see [BR#9.16.3]).

Modifications made SHALL be ceased as soon as the law relied upon for that modification is no longer in effect or the requirements of the [BR] have been modified to make it possible to comply with them and the law at the same time. An appropriate change in practice, a change in the respective CPSs, and notification to the CA/Browser Forum SHALL be made within 90 days.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.

APPENDIX

Appendix A: Abbreviations

Table 4 - Abbreviations

Abbreviation	Meaning
AATL	Adobe Approved Trust List
ADN	Authorization Domain Name
ARL	Authority Revocation List (see CARL)
ASN.1	Abstract Syntax Notation One
BR	Baseline Requirements
CA	Certification Authority
CAA	Certification Authority Authorization
CAB Forum	CA/Browser Forum
CARL	Certification Authority Revocation List
CCADB	Common CA Database
ccTLD	Country Code Top-Level Domain
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DAkkS	„Deutsche Akkreditierungsstelle“ (German Accreditation Body)
DBA	Doing Business As
DNS	Domain Name System
DVCP	Domain Validation Certificate Policy
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
eIDAS	Electronic IDentification, Authentication and trust Services
EKU	Extended Key Usage
ETSI	European Telecommunications Standards Institute
EVCP	Extended Validation Certificate Policy
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
gTLD	Generic Top-Level Domain
HSM	Hardware Security Module
ICANN	Internet Corporation for Assigned Names and Numbers
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IPS	Intrusion-Prevention-System
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITU	International Telecommunications Union
IVCP	Individual Validation Certificate Policy

LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
MGF	Mask Generation Function
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVCP	Organizational Validation Certificate Policy
PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PSS	Probabilistic Signature Scheme
QCP	Qualified Certificate Policy
QCP-l	Policy for EU qualified certificate issued to a legal person
QCP-l-qscd	Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD
QCP-n	Policy for EU qualified certificate issued to a natural person
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD
QCP-w	Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person (deprecated)
QEVCP-w	Policy for EU qualified website certificate issued to a legal person and linking the website to that person based on the EVCG (formerly QCP-w)
QNCP-w	Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person based on the BRG
QSCD	Qualified electronic Signature/Seal Creation Device
QTSP	Qualified TSP
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest-Shamir-Adleman (public-key cryptosystem, described by Ron Rivest, Adi Shamir and Leonard Adleman)
RSASSA	RSA Signature Scheme with Appendix
RSASSA-PSS	Improved Probabilistic RSA Signature Scheme
SCT	Signed Certificate Timestamp
SHA	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extensions
SOG-IS	Senior Officials Group Information Systems Security
SSL	Secure Socket Layer
SÜG	Sicherheitsüberprüfungsgesetz
TLS	Transport Layer Security
TSP	Trust Service Provider
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VDG	Vertrauensdienstegesetz
VDV	Vertrauensdiensteverordnung
VSA	Verschlusssachenanweisung
VS-NfD	„Verschlusssache - Nur für den Dienstgebrauch“ (German Federal secrecy instruction)

Appendix B: References

Table 5 - References

Reference	Referenced Document
[ADTL]	Adobe Approved Trust-List Tech. Requirements
[APRP]	Apple Root Certificate Program
[APCT]	Apple's Certificate Transparency policy
[BR]	CAB-Forum Baseline Requirements
[CCADB]	CCADB Policy
[eIDAS]	eIDAS (Regulation (EU) No. 910/2014 of the European Parliament and of the Council)
[ETS401]	ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETS411-1]	ETSI EN 319-411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETS411-2]	ETSI EN 319-411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETS412-1]	ETSI EN 319-412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[ETS412-2]	ETSI EN 319-412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[ETS412-3]	ETSI EN 319-412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[ETS412-4]	ETSI EN 319-412-4: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
[ETS412-5]	ETSI EN 319-412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[ETS312]	ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[ETS431-1]	ETSI TS 119 431-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
[ETS461]	ETSI TS 119 461: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
[RFC5753]	RFC 5753 Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)
[RFC3279]	RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC3647]	RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[RFC5280]	RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC6960]	RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
[RFC6962]	RFC 6962 Certificate Transparency

[RFC4055]	RFC 4055 Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC5756]	RFC 5756 Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters
[RFC4491]	RFC 4491 Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile
[RFC5480]	RFC 5480 Elliptic Curve Cryptography Subject Public Key Information, March 2009
[RFC5758]	RFC 5758 Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA, January 2010
[RFC8692]	RFC 8692 Internet X.509 Public Key Infrastructure: Additional Algorithm Identifiers for RSASSA-PSS and ECDSA Using SHAKEs, December 2019
[RFC8813]	RFC 8813 Clarifications for Elliptic Curve Cryptography Subject Public Key Information
[RFC5019]	RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments
[RFC8823]	RFC 8823 Extensions to Automatic Certificate Management Environment for End-User S/MIME Certificates
[EVCG]	CAB-Forum Extended Validation Certificate Guidelines
[GCTP]	Google chrome Certicate Transparency Policy
[GCRP]	Chromium Root Certificate Policy
[GGS]	Google G-Suite SMIME Certificate Profile
[GCTL]	Google Certificate Transparency Log Policy
[MSRP]	Microsoft Trusted Root Program incl. - Security Incident Response Requirements - Audit Requirements -Testing Instruction - New CA application
[MOZRP]	Mozilla Root Store Policy
[MOZCA]	Mozilla CA/Application Process
[NCSSR]	CAB-Forum Network Security Guidelines
[SÜG]	„Sicherheitsüberprüfungsgesetz“ (German Law)
[TR3145]	Technical Guideline TR-03145-1, Secure CA operation, Part 1, German Federal Office for Information Security
[TR3145VS]	Technical Guideline TR-03145-VS-NfD, Secure CA operation, VS-NfD, German Federal Office for Information Security
[VDG]	„Vertrauensdienstegesetz“ (German Law)
[VDV]	„Vertrauensdiensteverordnung“ (German Law)
[VSA]	„Verschlusssachenanweisung des Bundes“ (German Federal secrecy instruction)
[X500]	ITU-T X.500 Serie / ISO/IEC 9594 Serie Information technology - Open systems interconnection - The Directory

Appendix C: Definitions

Note: At this point, it is omitted from listing again known definitions of internationally established terms in the PKI environment; in this respect, reference is made to the definitions of the ETSI specifications and RFCs listed in Appendix B. In the following, terms are defined that are used specifically for certain certificate types, and some terms used in this document whose usage may differ between the German and English languages are clarified.

Table 6 - Definitions

Term	Definition
Advanced electronic seal	Electronic seal according to [eIDAS#Art.36]
Advanced electronic signature	Electronic signature according to [eIDAS#Art.26]
Certification Authority Authorization (CAA)	[TLS] DNS resource record that allows the owner of a DNS domain name to specify the TSPs that are authorized to issue certificates for that domain
High-Risk Certificate Request	[TLS] Certificate applications the TSP flags for additional review based on internal criteria. These may include: ▪ mixed character domain names ▪ names that are at higher risk for phishing or other fraudulent use, ▪ names included in previously rejected certificate requests or revoked certificates, ▪ names listed on the Miller Smiles phishing list or the Google Safe Browsing list; or ▪ names that a TSP identifies based on their own risk mitigation criteria.
Leaf Certificate	[TLS] A TLS certificate that was previously published as a pre-certificate
Non-Reserved LDH-Label	[TLS] Component of a domain name that does not have a '-' in the third and fourth positions
P-Label	[TLS] Component of a domain name that has a '-' in the third and fourth positions ("XN label") and is followed from the fifth position by a valid output of the punycode algorithm according to [RFC3492# 6.3]
Pre-Certificate	[TLS] Certificate according to [RFC6962] for public logging of a yet-to-be-issued TLS certificate. The pre-certificate is generated from the yet-to-be-issued certificate plus the special critical extension `Certificate Transparency precertificate poison extension (OID 1.3.6.1.4.1.11129.2.4.3)`. Pre-Certificates are not considered certificates according to [RFC5280] and cannot be validated by standard X.509v3 clients. The (real) TLS certificate generated later from the Pre-certificate is called a *Leaf Certificate*.

Pseudonym	Fictitious identity that a person assumes for a specific purpose and that is different from his or her original or true identity. NOTE: A pseudonymous identity, unlike an anonymous identity, can be linked to the person's true identity. The true identity is known to the TSP
Short-term certificate	Certificate whose validity period is shorter than the maximum processing time for a revocation request specified in the CPS
Technically constraint CA	[TLS] A Sub CA where a combination of values in the extendedKeyUsage and nameConstraints extensions is used to limit the scope within which this Sub CA is allowed to issue subscriber or additional Sub CA certificates
Token	Hardware module that generates and/or handles cryptographic keys in a secure manner
Verified method of communication	[EVCP] The use of a telephone number, fax number, email address, or postal address that has been verified by a TSP as a reliable way of communicating with the *Applicant* in accordance with [EVCG#11.5]
Verschlusssache - Nur für den Dienstgebrauch	[3145] A classification of German government information to be protected
Wildcard Certificate	[TLS] A certificate with a *Wildcard Domain Name*
Wildcard Domain Name	[TLS] A domain name consisting of a single asterisk followed by a single dot ("*.") followed by a FQDN.