Deutsche Telekom Security GmbH
Trust Center Certificate Policy

Public

Version: 01.00

Valid from: 15.03.2021

Status: RELEASE

Last Review: 15.03.2021

IMPRINT

Table 1: Imprint

Information	Expression
Publisher	Telekom Security Trust Center & ID-Solutions Untere Industriestraße 20, 57250 Netphen, Deutschland
File name	Telekom Security CP EN v01.00_RELEASE.docx
Valid from	15.03.2021
Title	Trust Center Certificate Policy
Version	01.00
Last review	15.03.2021
Status	RELEASE
Author	Telekom Security
Reviewed by	Telekom Security
Released by	--
Involved organizational unit	Telekom Security Trust Center & ID-Solutions
Contact	Telekom Security Leiter Trust Center Betrieb
Brief description	Overarching Certificate Policy

HISTORY

Table 2: Change history

Version	Date	Editor	Changes / Comment
00.10	08.03.21	Telekom Security	Initial English version, based on the German version 00.17.
00.11	11.03.21	Telekom Security	Final Draft
00.18	15.03.21	Telekom Security	Review
00.90	17.03.21	Telekom Security	Formal QS
01.00	18.03.21	Telekom Security	Release

TABLE OF CONTENTS

LIST OF TABLES

1 INTRODUCTION

1.1 Overview

As a trust service provider (TSP), Deutsche Telekom Security GmbH (hereinafter referred to as Telekom Security) operates various root certification authorities (Root-CAs) and subordinate certification authorities (Sub CAs) in its trust center for issuing certificates, both for customers and employees of the Deutsche Telekom AG.

This document is the Certificate Policy (CP) of the Telekom Security Trust Center. This CP applies to all certificates that are issued by

- Telekom Security below its public and qualified Root CAs,
- Telekom Security below its internal Root CAs that commit to this CP,
- the Sub CAs of the „Deutsches Forschungsnetz" (DFN) below Telekom Security's public Root CAs, and
- Telekom Security below the Root CAs of the Federal Office for Information Security (BSI) in accordance with the requirements of BSI technical guideline TR-03145 [TR3145].

The document describes, structured in accordance with RFC 3647, the requirements that must be implemented by the TSPs of the Root and Sub CAs in the scope of this CP.

The following semantics apply:

- Requirements that are not specifically marked apply in general for all certificate types.
- Requirements that begin with the specification of one or more certificate types in square brackets (such as the last paragraph of this section) apply only to the certificate types concerned. The following certificate types are distinguished in this document:
  - [SSL] identifies all TLS authentication certificates issued under the Telekom Security public Root CAs integrated in the trusted root stores of the browser manufacturers, in accordance with the current version of the "CA/Browser Forum Baseline Requirements" [BR], published at http://www.cabforum.org. This marking also applies in principle to TLS certificates issued in accordance with [EVCP], [OVCP], [DVCP], [IVCP] or [QCP-w].
  - [SMIME] identifies all S/MIME certificates for e-mail security that are issued under the Telekom Security public Root CAs integrated in the trusted root stores of Microsoft [MSRP], Mozilla [MOZRP], Google [GGLRP] 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 the [TR3145] and also meet the requirements for "VS-NfD" (classified information, "Verschlusssache, nur für den Dienstgebrauch") in accordance with the extension of the [TR3145] for VS-NfD [TR3145NfD].

- [Non-QCP] identifies all non-qualified certificates issued in accordance with ETSI EN 319 411-1 [ETS4111]. In detail, these are:
  - [LCP] Certificates issued according to the Lightweight Certificate Policy.
  - [NCP] or [NCP+] certificates issued according to the Normalized Certificate Policy or Extended Normalized Certificate Policy, respectively.
  - [EVCP] Certificates issued according to the Extended Validation Certificate Policy.
  - [OVCP] Certificates issued in accordance with the Organizational Validation Certificate Policy.
  - [DVCP] Certificates issued according to the Domain Validation Certificate Policy.
  - [IVCP] Certificates issued in accordance with the Individual Validation Certificate Policy.
- [QCP] identifies all qualified certificates issued in accordance with ETSI EN 319 411-2 [ETS4112]. In detail, these are:
  - [QCP-n] qualified certificates for natural persons
  - [QCP-l] qualified certificates for legal persons
  - [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
  - [QCP-w] for website authentication (TLS-Server)

The options or obligations to implement the requirements are described by the keywords according to RFC 2119:

- 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.

The TSP SHALL describe the implementation of and compliance with the requirements of this CP and the referenced documents in the current versions in their Certification Practice Statements (CPS). In case of conflict between this CP, the CPS of the TSP and the referenced documents, the regulations from the referenced documents shall take precedence.

[EVCP] The TSP SHALL explicitly refer in their CPS to compliance with the latest version of the [BR] and the [EVCG] including the indication of the link to the documents (http://www.cabforum.org) as well as the EVCP policy according to ETSI EN 319 411-1.

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)}

The binding information on version, validity date and status are listed on the cover sheet.

1.3 PKI participants

1.3.1 Certification Authorities (CA)

1.3.1.1 Root Certification Authorities (Root CA)

The root certification authorities are the highest level of a PKI hierarchy. They issue only their own Root CA certificates and the certificates of the certification authorities directly subordinate to them. In addition, they may issue CRL or OCSP signer certificates for the status services they operate.

Telekom Security operates several of its own public and internal Root CAs and also issues its own cross certificates, but it does not issue cross certificates to Root or Sub CAs of other TSPs.

The following terms are used in this document:

- Following [ETS4111], the term "Root Trust Service Provider" (Root TSP) is used to refer to Telekom Security as the operator of the Root CAs.
- The term "Root CA" is used to refer to the technology used in operation.
- The term "Root CA certificate" is used to describe a specific CA certificate from a root certification authority.

1.3.1.2 (Subordinate) Certification Authorities (Sub CA)

The certification authorities issue either end entity certificates or CA certificates of further Sub CAs and thus form the second to penultimate hierarchy level of a PKI. In addition, they may issue CRL or OCSP signer certificates for the status services they operate.

Telekom Security operates several public and internal Sub CAs, all of which issue end entity certificates and CRL or OCSP signer certificates only and no certificates for other Sub CAs.

The scope of this document also includes the certification authorities of the “DFN-Verein” (“Verein zur Förderung eines Deutschen Forschungsnetzes e. V”., hereinafter referred to as DFN). Telekom Security issues Sub CA certificates to the DFN below its public Root CA certificates. These Sub CA certificates issued by Telekom Security are used by DFN to issue further subordinate Sub CA certificates, which in turn issue the end entity certificates. The Sub CAs of the two hierarchy levels also issue CRL or OCSP signer certificates as required.

The following terms are used in this document:

- The term "Trust Service Provider" (TSP) is used to refer to Telekom Security or DFN as the operator of the Sub CAs.

- The term "Sub CA" is used to describe the technology used in operation.
- The term "Sub CA certificate" refers to a specific CA certificate of a TSP.

The TSPs are exclusively legal entities, i.e. no natural person acts as an issuer of certificates.

Where a distinction between the Telekom Security and DFN TSPs is necessary in the description of the requirements in this document, the requirements are identified by a mark in square brackets in analogy to the distinction between the certificate types (see above):

- [TSEC-CA] refers to the certificates issued by Telekom Security.
- [DFN-CA] refers to the certificates issued by the DFN.

1.3.2 Registration Authorities (RA)

The registration authorities carry out the identification and authentication of end subscribers as part of the application for issuance, renewal or revocation of certificates. They can either be a part of the TSP or act as an external registration authority on its behalf.

The requirements for TSPs set out in this document also apply to external RAs, where applicable. When using external RAs, TSPs SHALL describe in their CPS the structures, relevant processes, rights and obligations of the external RAs and close appropriate agreements with them.

[EVCP] No external RAs are currently used.

1.3.3 Subscribers

Subscribers are natural or legal persons who apply for and hold the subscriber certificates and thus also have responsibility for the keys.

The subject of an end entity certificate can be the end entity itself as a natural or legal person or it can be a group, function, IT process or technical device for which the subscriber is responsible.

The TSP SHALL describe in their CPS the end entities to be considered in the scope of the CPS and the possible objects of the end entities certificates

1.3.4 Relying parties

Relying parties are persons or IT processes that trust the certificates and use them

- for the verification of digital signatures,
- for the verification of authentications or
- for encryption.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The use of Root CA certificates SHALL be limited to the following:

- Signature of Sub CA certificates,
- Signature of OCSP or CRL signer certificates,
- Signature of revocation lists.

The use of Sub CA certificates SHALL be limited to the following:

- Signature of Sub CA certificates,
- Signature of end entity certificates,
- Signature of OCSP or CRL signer certificates,
- Signature of revocation lists,
- signature of OCSP statements.

The use of the end entity certificates SHALL be restricted to the use cases according to the keyUsage attribute and, if set, the extendedKeyUsage extension. The TSP SHALL describe in the CPS the appropriate use of the Sub CA and end entity certificates.

1.4.2 Prohibited certificate uses

Certificates SHALL NOT be used for use cases other than those listed in section 1.4.1. In particular, Root CA certificates SHALL NOT be used for issuing end entity certificates.

1.5 Policy administration

1.5.1 Organization administering the document

This document is administered by:

Deutsche Telekom Security GmbH

Trust Center – Root Programm

Untere Industriestraße 20

57250 Netphen

Germany

1.5.2 Contact person

The contact person for this CP is the Trust Center Root Programm, which can be contacted as follows:

Phone: +49 (0) 1805 268 204

Note on the costs incurred:

Landline Phone 0.14 EUR/minute, mobile networks max. 0.42 EUR/minute

WWW: http://www.telesec.de/

E-Mail: FMB_Trust_Center_Rootprogram@t-systems.com

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 Root Programm, for contacts see section 1.5.2.

1.5.4 CPS approval procedures

This CP has been approved by the Trust Center management and remains valid as long as it is not revoked or replaced by a new version.

This CP SHALL be subject to a review by the Root Programm when required, e.g. due to changed requirements or relevant changes in operation, but at least once a year. The root program SHALL therefore regularly review the underlying requirements (e.g. those of CABF, ETSI or BSI) for new versions at appropriate intervals. Changes to this CP as well as the annual review SHALL be listed in the change history of this document. This applies even if no substantive changes are made at the annual review. Each new version SHALL be approved by Trust Center management, assigned a new ascending version number, and published as specified in section 2.2. All affected TSPs SHALL be informed at the latest with the release of a new version.

The CPSs based on this CP SHALL be reviewed analogously. The revision and release processes as well as the releasing entity SHALL be described in the respective CPS. In addition, the Root Programm, for determining conformance of the revised CPS to this CP, SHALL be involved in the release process. After release of a new version of a CPS, all affected employees of the TSP and, if available, of the external RAs SHALL be informed.

The TSP SHALL close agreements with the Root TSP to adhere to the most current version of this CP.

1.6 Definitions and acronyms

1.6.1 Definitions

Table 3: Definitions

Term	Explanation
Affiliate	For example, a company, partnership, joint venture, corporation, (capital) company, association, foundation, or other organization (legal person) that supervises, is supervised by, or is controlled together with another organization (legal person), facility, department, governmental unit, or unit that is directly subordinate to a governmental authority.

Term	Explanation
Applicant	The natural or legal person who applies for a certificate (or requests its renewal). Once the certificate has been issued, the applicant is referred to as the subscriber. In the case of certificates issued for devices, the applicant is the organization that controls or operates the device listed on the certificate, even if the device sends the actual certification application.
Applicant's representative	If different from the applicant, a natural person or payer, an employee of the applicant, or an authorized representative who has the express authority to represent the applicant: (i) who signs, submits, or approves an application for a certificate in the name of the applicant and/or (ii) signs and submits a subscriber agreement in the name of the applicant and/or (iii) acknowledges and agrees to the certificate's terms of use in the name of the applicant if the applicant is an affiliated company (affiliate) of the certification authority (CA).
Application for a certificate with increased risk	An application for which the CA provides an additional check with regards to internal criteria and databases that the CA runs. This can concern names that are subject to a high risk about phishing or other fraudulent use, names that are contained in previously rejected certificate applications or revoked certificates, names that are on the MillerSmiles phishing list, or the Google Safe Browsing list or names that the CA identifies based on its own risk-minimization criteria.
Application software provider	A provider of Internet browser software or other application software on the relying side that displays or uses certificates and contains root certificates.
Authentication	Checking an identity based on claimed characteristics.
Authority revocation list (ARL)	List showing digital certificates that have been revoked by certification authorities (except Root CA). Before a digital certificate of a certification authority is used, the ARL should be used to check whether the certificate may still be used.
Authorization document	The documentation that proves an applicant is authorized to apply for one or more certificates for a certain natural person, group of persons or functions, legal person, or device. This may also be a document from the certification authority regarding communication with the person or organization in question.
Bulk	Function of a CA with which the sub-registration authority can generate soft PSEs in bulk.
Central registration model	Following successful registration, the sub-registration authority requests the certificate on the sub-registration authority website (using a web form or in bulk) and directly receives this certificate or the key material for the end entity (except in the case of a registration authority certificate).
Central repository	An online database that contains public PKI documents (e.g., certificate policy, certificate practice statement, CA certificates), as well as additional information, either in the form of a CRL or an OCSP response.
Certificate	An electronic document that uses a digital signature to bind a public key to an identity (e.g., person, device).
Certificate administration process	Processes, practices, and procedures relating to the use of keys, software, and hardware that the certification authority (CA) uses to check certificate data, issue certificates, maintain a central data repository, and revoke certificates.
Certificate application	A request made in electronic or written form that contains data regarding an applicant.
Certificate data	Certificate applications and associated data (obtained from the applicant or elsewhere) that is in the possession of the certification authority (CA), is subject to monitoring by the CA or that the CA has access to.
Certificate Management Protocol (CMP)	The Certificate Management Protocol is a protocol developed by the IETF to manage X.509 certificates within a public key infrastructure (PKI).
Certificate policy (CP)	Defines the guidelines for generating and managing certificates of a certain type. A set of rules that specifies the options for using a named certificate in a certain community (parties involved in PKIs) and/or a PKI implementation with common security requirements.

Term	Explanation
Certificate problem report	Complaints due to suspicion that the key is at risk, certificate misuse, or with regard to other types of fraudulent behavior, risk, misuse, or incorrect behavior in connection with certificates.
Certificate revocation list (CRL)	A regularly updated, time-stamped list of revoked certificates that is generated and signed digitally by the issuing certification authority (CA). The authority revocation list (ARL) is a special certificate revocation list (CRL), as it contains only Sub CA certificates.
Certificate signing request (CSR) [TC]	A certificate request that is created electronically by a device (e.g., server) and signed using the private key, which contains the public key and the certificate data in coded form. The syntax is described by the standard PKCS#11.
Certification authority (CA)	An organization that is responsible for generating, issuing, revoking and managing certificates. This term is used for both root certification authorities (Root CA) and subordinate certification authorities (Sub CA).
Certification practice statement (CPS)	Explanations for operating a certification authority. In particular, the CPS implements the provisions and policies of the CP of a certification authority. One of several documents that provide general and specific framework conditions. This contains, in particular, a description of the procedure the certification authority (CA) follows for issuing, managing, revoking, and renewing certificates.
Change Advisory Board	A board within Telekom Security that decides on PKI functions.
Chip card	Plastic card with an integrated computer chip. Telephone cards are an example of these. If the computer chip is able to perform calculations, it is also called a smartcard. Smartcards can also be used for cryptographic applications.
Compromise	A private key is compromised if it is made known to unauthorized persons or can be used by them. A compromise could occur through a criminal attack, for example.
Country	Either a member of the United Nations or a geographical region that at least two member states of the UNO recognize as a sovereign state.
Cryptography	Science dealing with the encryption of data and related issues (such as digital signatures).
Delegated third party	A natural or legal person who is not identical to the certification authority (CA) but is authorized by this authority to support the certificate management process by performing tasks to fulfill one or more requirements. This may be an external registration authority or an internal enterprise registration authority.
Device	Component such as a router, server, gateway, or application that supports certificate-based functions but cannot request certificates itself or can do so only to a limited extent. Frequently, certificates are requested via an authorized person (e.g., administrator) and installed on the component.
Device certificate	X.509 V3 certificate that contains either a host name, an IP address, or an e-mail address in the commonName field (CN) of the subscriber's distinguishedName (subject) and/or in at least one subjectAltName extension.
Digital signature	A checksum created with a special mathematical procedure. Guarantees the authenticity of the signatory and the integrity of the data.
Directory service	Data repository for calling up certificates and certificate validation information (revocation list).
Distinguished name	Format with which distinguished names can be specified in accordance with the X.500 standard. A digital certificate must contain a DN.
Domain authorization document	The documentation that the domain name registrar, a registered domain owner (domain name registrant), or the person or organization that is listed as the registered domain owner in WHOIS (including all private, anonymous, or proxy registration services) provides and that proves the applicant's authorization to request a certificate for a particular domain name space. This may also be a

Term	Explanation
	document from the certification authority regarding communication with the person or organization in question.
Domain name	The name that is given to a node in the Domain Name System (DNS).
Dual key certificate	Variant in which separate key pairs are used for encryption and signing. This means the user has two corresponding certificates.
End entity	Also see Subscriber. The term end entity is largely used in the X.509 environment.
End-entity certificate	A certificate that does not use the "certification authority" basic constraint and therefore cannot sign certificates itself.
ETSI certification	Check and confirmation for certification authorities by an independent expert to ensure that the PKI is operated in accordance with the "ETSI TS 102 042" ETSI criteria. The aim of ETSI audits is to strengthen demand-side trust in electronic business transactions.
External registration authority	An employee (staff member) or representative of a company that is not affiliated with the certification authority (CA) (non-affiliate) that approves certificates for third parties. These roles (trusted roles) are performed, for example, by the tenant's master and sub-registration authority or authorized representative.
Fully qualified domain name (FQDN)	Correct and complete domain name, i.e., a chain of all labels for a path in the domain name space (for further information see RFC 2181).
Hardware security module (HSM)	Hardware to generate and store private keys securely.
Hash value	In this context, a fixed length cryptographic checksum (the correct name is cryptographic hash value). It should be as unlikely as possible to calculate the entry from the hash value or to find several possible inputs for the same hash value (hash value is used as a synonym for fingerprint). In most cases a hash value is signed instead of a complete digital document.
Identification	The process of providing the identity of a subject or object (e.g., user, device) to a system. The identification is part of the validation.
Interface	An interface is part of a system that is used for communication (input and output).
Internal registration authority	An employee (staff member) or representative of a CA who checks the "domain" specified by the PKI tenant and provides it for the certificate application. This role (trusted role) is performed, for example, by the Trust Center operator.
Internal server name	A server name (which may or may not contain a registered domain name) that cannot be dissolved with the public Domain Name System (DNS).
Issuer distinguished name (issuer DN)	Format with which distinguished names can be specified in accordance with the X.500 and LDAP standards. The issuer DN describes the CA issuing the certificate in a unique way.
Issuing certification authority (CA)	The certification authority (CA) that issued a specific certificate. This could be a root certification authority (Root CA) or a subordinate certification authority (Sub CA).
Key backup	Mechanism for backing up keys. In order to be able to restore encrypted e-mails in the event of key loss, we recommend backing up the key material of the encryption key. Key backup is also used as a synonym for key archiving.
Key compromise	A private key is considered to be compromised if its value is shared with an unauthorized person, an unauthorized person has access to it, or there is a practical method that an unauthorized person could use to find out its value.

Term	Explanation
Key owner	A natural person authorized by the delegated third party who is responsible for the proper use (distribution, use and, if necessary, revocation) of the key pair and certificate that was issued for a group of persons or functions, legal person, or device.
Key pair	The private key and its corresponding public key.
Key recovery	Mechanism for recovering keys. This can be necessary if users lose their key (such as through a damaged file).
Latency period	Period of time between an action and the occurrence of a delayed reaction (delay period). With latency periods, the action occurs unnoticed and is only discovered through the reaction.
LDAP server	Server that saves information that can be called up via LDAP.
Legal person	A company, group, partnership, sole trader, trust, government authority, or legal entity with legal standing within the legal system of a country.
Lightweight Directory Access Protocol (LDAP)	Protocol for querying directories. This has displaced the significantly more complicated Directory Access Protocol (DAP) in many areas. LDAP offers more options than HTTP and FTP (such as setting up a context that can be maintained using several queries). LDAP is used in particular to query digital certificates and revocation lists within public key infrastructures.
Local registration model	The user requests the certificate via the user website or by sending an e-mail request, or the device uses its SCEP interface to request the certificate. This request is processed by the sub-registrar (approval, rejection, or postponement (resubmission)).
Mail security	Security functions such as digital signature and encryption that support standard mail applications.
Management system for information security (ISMS)	The management system for information security (ISMS) represents a set of procedures and rules within a company that serve to define, manage, monitor, maintain, and continually improve information security over the long term. The term is used in the ISO/IEC 27002 standard; ISO/IEC 27001 defines an ISMS.
Master domain	Independent administrative area that has a distinguished name and is set up exclusively for a delegated third party. The delegated third party can approve and manage certificates within the tenant. The tenant is managed using the master registration authority certificate. Further information is available under: Tenant.
Master registration authority	Natural person (trusted role) who manages the master domain.
Multitenancy	In information technology (IT), multitenancy refers to the property of software or a server to map multiple, fully separated tenants on one installation. The respective tenants (e.g., legal units or companies) are unable to view the data, user administration, or similar of the other parties/tenants.
Object identifier (OID)	A unique, alphanumeric, or numeric identifier that is registered for a specific object or object class of the International Standards Organization (ISO) under the appropriate standard.
OCSP responder	An online server that is subordinate to the certification authority (CA) and is connected to its central repository to process certificate applications. Also see Online Certificate Status Protocol (OCSP).
Online Certificate Status Protocol (OCSP) [BR]	A protocol for online certificate validation with the help of which the application software on the relying side can determine the status of an identified certificate. Also see OCSP responder.
Period of validity	The period from the issue date (not before) until the expiry date (not after).
Permitted Internet domains	A domain name that consists of the top-level domain and further sub-domains and is added to the tenant's PKI configuration (master domain) as a "permitted Internet domain" following a successful check by the internal registration authority.

Term	Explanation
Permitted public data source	An authentication document or a data source (e.g., identity database, commercial register) that is used to check subject identity data, that is generally recognized by commercial companies and authorities (public administration) as reliable and that a third party created for a different purpose other than the issuing of certificates by the applicant.
Person authorized to revoke	A person who is authorized by the subscriber or key owner to revoke a certificate for a group of persons or functions, legal person, or device. Authorization is via the certificate revocation password.
Personal Identification Number (PIN)	Secret code used at cash machines, for example.
Personal security environment (PSE)	All security-relevant information such as the private key is saved in the personal security environment. The PSE can be available as an encrypted file or on a smartcard and is protected by a password or a PIN.
Policy	Guidelines or explanations that determine the security level for creating and using certificates. There is a difference between certificate policy (CP) and certification practice statement (CPS).
Power of attorney	Power of attorney is understood to be a power of representation founded on a legal transaction. The power of attorney is established through unilateral declarations of intent that the principal must communicate to the agent of the power of attorney.
Private key	They key from a key pair that the key owner keeps secret and uses to create digital signatures and/or decrypt electronic data and files that were encrypted using the corresponding public key.
Public device certificate	A device certificate that a Sub CA issues in the CA hierarchy below a root certificate.
Public key	The key from a key pair that the owner of the corresponding private key is permitted to make publicly available and that the relying side uses to verify digital signatures that were created using the owner's private key and/or to encrypt messages that can only be decrypted using the owner's corresponding private key.
Public key infrastructure	Hardware, software, persons, procedures, rules, guidelines, and obligations that enable certificates and keys to be generated, issued, managed, and used reliably based on the public key cryptography.
Public Key Infrastructure X.509 (PKIX)	IETF standard that standardizes all relevant parts of a PKI.
Public Key Service (PKS)	Service of the Trust Center for issuing and administrating certificates that comply with the German Digital Signature Act.
Qualified auditor	A natural or legal person who meets the specified criteria.
Registered domain name	A domain name that is registered with a domain name registration authority (registrar).
Registration authority (RA)	A legal person who is responsible for identifying and authenticating certificate subjects. However, this is not a CA and therefore does not sign or issue certificates. An RA can provide support when requesting or denying a certificate or in both cases. When "RA" is used as an adjective to describe a role or function, this does not necessarily refer to an independent authority. It can, however, be part of the CA.
Registration authority of a	An employee (staff member) or representative of an organization who is not affiliated with the certification authority (CA) (non-affiliate) that approves certificates for third parties. These roles (trusted roles) can be performed, for

Term	Explanation
company (enterprise RA)	example, by the tenant's master and sub-registration authority or authorized representative.
Registration model	A distinction is made between the central registration model (see there) and the local registration model (see there).
Relying parties	A natural or legal person who relies on a valid certificate. A provider of software is not a relying party if the software this provider sells merely contains information on a certificate.
Revocation authority	An employee (staff member) or representative of an organization who performs certificate revocations.
Rivest Shamir Adleman (RSA)	Procedure for encryption, for digital signature and for the secure transmission of keys that is named after the three cryptographers Rivest, Shamir, and Adleman.
Root CA	See Root certification authority.
Root certification authority (Root CA)	The highest-level certification authority whose root certificate is distributed by application software providers and who issues the subordinate CA certificates (sub-certificates).
Root certification authority certificate (root certificate)	The self-signed certificate that the root certification authority (Root CA) issues for self-identification. In addition, this certificate helps with the validation of issued sub-certificates.
Secure Multipurpose Internet Mail Extension (S/MIME)	Secure Multipurpose Internet Mail Extension. Extension of the MIME e-mail format, which describes additions for cryptographic services that guarantee the authenticity, integrity, and confidentiality of messages.
Secure Socket Layer (SSL)	Crypto protocol for ensuring end-to-end connections on the Internet. This has now been superseded by the newer TLS process. Can be used instead of the more complex IPSec in many cases.
Service desk	The service desk is an organizational unit within a company that serves as the tenant or delegated third party's central contact point for all service and support requests and that conveys these within the company in accordance with the agreed business processes.
Simple Certificate Enrollment Protocol (SCEP)	Simple Certificate Enrollment Protocol. Protocol for ordering and loading certificates in IPSec devices.
Simple Object Access Protocol (SOAP)	Simple Object Access Protocol: SOAP provides a simple mechanism for exchanging structured information between applications in a decentralized, distributed environment.
Single key certificate	Variant in which the same key pair is used for encryption and signing. This means the user has one certificate.
Smartcard	A special plastic card with an integrated computer chip that can also be used for cryptographic applications.
Software PSE (soft PSE)	An encrypted file for saving the certificate and the corresponding private and public keys.
Sub-domain	Hierarchically subordinated sub-section of the master domain that is managed by a sub-registration authority.
Subject	The natural person, device, system, unit, or legal person that is named as the subject in a certificate. The subject is either the subscriber or a device that is under the subscriber's control or is operated by this person.
Subject Alternative Name	Additional fields in a certificate. The fields can be used to enter additional names of the subscriber and are a standard extension of the X509 standard.
Subject distinguished name (subjectDN)	Format with which distinguished names can be specified in accordance with the X.500 and LDAP standards. The subjectDN uniquely specifies a person or device.

Term	Explanation
Subject identity data	Data that identifies the subject of the certificate. Subject identity data does not contain a domain name that is listed in the subjectAltName extension or the subject commonName field.
Subordinate certification authority (Sub CA)	A certification authority whose certificate is signed by a root certification authority (Root CA) or another subordinate certification authority (Sub CA).
Sub-registration authority	Natural person (trusted role) who manages the sub-domain.
Subscriber agreement	An agreement between the certification authority (CA) and the applicant/subscriber that specifies the rights and obligations of the parties.
Suspension	In relation to the PKI, suspension means a provisional or temporary revocation. The certificate initially appears in the certificate revocation list, but can be re-activated by the sub-registration authority.
Tenant	The tenant is a separate, logically self-contained unit with its own legal, organization, and data management within the system. The tenant thus structures the use of the system. The master domains are known as tenants. Within the master domains, there are further subdivisions in the form of areas of responsibility (also known as sub-domains).
Terms of use	Provisions regarding safekeeping and permitted usage of an issued certificate in accordance with the specified requirements if the applicant/subscriber is an affiliated company of the certification authority (CA), for example.
Transport layer security (TLS)	Crypto protocol for ensuring end-to-end connections on the Internet.
Triple key certificate	Variant in which separate key pairs are used for encryption and signing and Microsoft smartcard logon. This means the user has three corresponding certificates.
Trusted certificate	A certificate that is trusted due to the fact that its corresponding root certificate represents a trust anchor in widely distributed application software.
Unregistered domain name	A domain name that is not a registered domain name.
Valid certificate	A certificate that passes the validation procedure described in RFC 5280.
Validation	Evidence of the reproducibility of a result from a described procedure under defined conditions. The more precisely a procedure is described and the fewer unknown influencing factors there are, the more certain it is that corresponding results will be produced. A description of the goal and method is required for a validation. In this context, valid means that the method leads to the result in a repeatable manner. In the context of a PKI, there is a validation process in the following places: notification and verification of an identity (e.g., natural person, device) against the certificate application. Algorithm to check a certificate for its validity period, issuing certification authorities, and certificate status (valid, revoked).
Validation specialist	Someone who performs the data validation tasks in accordance with the requirements in question. In the context of the Trust Centers these are the following role owners: Trust Center operator, master registrar, sub-registrar
WHOIS	Information that is (a) directly retrieved from the Domain Name Registrar or registry operator via RFC 3912 protocol, (b) the Registry Data Access Protocol (RFC 7482), or (c) an HTTPS website.
Wildcard certificate	A certificate that has an asterisk (*) in the left-most position of a fully qualified domain name of the subject contained in the certificate.

Term	Explanation
X.509	Standard, whose most important element is a format for digital certificates. Certificates of version X.509v3 are supported in all common public key infrastructures.

1.6.2 Abbreviations

Table 4: Abbreviations

Abbreviation	Definition
ARL	Authority Revocation List
BR	Baseline Requirements
DK	Dual Key
CA	Certification Authority
CMP	Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement
CN	Common Name
CRL	Certificate Revocation List
DN	Distinguished Name
EDV	Electronic Data Processing
eIDAS	Electronic Identification and Signature
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
FQDN	Fully Qualified Domain Name
GRP	Identifies a group, function, or role certificate
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IPS	Intrusion-Prevention-System
IPSec	Internet Protocol Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
IV	Individual Validation
LB	Service Description
LDAP	Lightweight Directory Access Protocol
n.a.	not available
NCP	"Normalized" Certificate Policy
NIC	Network information center
OCSP	Online Certificate Status Protocol
OID	Object Identifier
opt.	optional
OV	Organization Validated
OVCP	"Organizational Validation" Certificate Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PN	Stands for pseudonym
PSE	Personal Security Environment
PTC	Publicly trusted certificate
RA	Registration Authority
RFC	Request for Comments
SCEP	Simple Certificate Enrollment Protocol
SK	Single Key

Abbreviation	Definition
SLA	Service Level Agreement
RSA	Rivest Shamir Adleman
S/MIME	Secure Multipurpose Internet Mail Extension
SigG	German Digital Signature Act (*Signaturgesetz*)
SigV	German Digital Signature Regulation (*Signaturverordnung*)
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
TK	Triple Key
UPN	User Principal Name
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
XML	Extensible Markup Language

1.6.3 References

Table 5: References

Shortcut	Reference
[BDSG]	Datenschutzgesetz, Bundesgesetzblatt I 2003 S.66 (Data Protection Act, Federal Law Gazette I 2003 p.66)
[CAB-BR]	Version of the “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” document published by CA/Browser Forum at http://www.cabforum.org/ valid at the time
[EU-RL]	Directive of the European Parliament and of the Council on a Community framework for electronic signatures, 1999/93/EC, EU, 1999
[Moz-2-7]	Mozilla Root Store Policy, Version 2.7, Stand 01.01.2020, https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy
[PKCS]	RSA Security Inc., RSA Laboratories "Public Key Cryptography Standards," http://www.rsasecurity.com/rsalabs
[PKIX]	RFCs and specifications by the Public Key Infrastructure (X.509) IETF working group.
[RFC3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003
[RFC5280]	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008
[RFC6960]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.
[RFC6962]	Certificate Transparency. B. Laurie, A. Langley, E. Kasper. June 2013.
[SigG]	Law on general conditions for digital signatures and for the amendment of additional provisions (Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung von weiteren Vorschriften), Federal Law Gazette (Bundesgesetzblatt) I 2001, p. 876
[SigV]	Digital signature regulation (Verordnung zur elektronischen Signatur), BGBl (German Civil Code). I p. 3074, November 21, 2001
[X.509]	Information technology - Open Systems Interconnection - The Directory:authentication framework, Version 3, ITU, 1997

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Respositories

TSPs SHALL describe in their CPS who maintains which directories containing information about the certificates they issue.

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, the TSP SHALL publish

- the terms of use in a generally understandable language,
- the CPS in the structure according to RFC 3647,
- the Root, Cross and Sub CA certificates, and
- the status information according to sections 4.9 and 4.10 for all unexpired certificates issued by them

via suitable online services around the clock. The relevant terms of use and CPS SHALL be easily identifiable to the certificates.

The TSP SHALL list in their CPS the complete CA hierarchies, i.e. all Root and Sub CA certificates that are in the scope of the CPS.

In addition, the TSP MAY publish the end entity certificates with the end entity's consent.

[SSL] The TSP operating technically non-restricted Sub CAs SHALL (also) publish their CPS and the audit certificates in English. The CPS translated into English SHALL have the same version number as the original CPS in German language. The translated version SHALL NOT differ significantly from the original version, but it does not have to be authoritative in all disputes.

The TSP SHALL publish all issued certificates, including at least all Sub CA certificates and, if applicable, the Root CA (optional) from its chain, in at least one "Certificate Transparency Log" (CTLog). In addition, the TSP MAY also publish "pre-certificates" (see section 4.3.1) in one or more CTLogs.

[SSL] [SMIME] The Root TSP SHALL publish the required information on the Root- and Sub CA certificates in the "Common CA Database" (CCADB) in accordance with the CCADB policy (see https://www.ccadb.org) and keep it up to date; see also section 4.9.3 regarding revoked Sub CA certificates.

The TSP SHALL publish their CPS on their own official website.

[QCP] The TSP SHALL, in addition to the CPS, also publish a PKI Disclosure Statement (PDS) in the structure according to Annex A of [ETS4111].

[3145] The TSPs SHALL ensure that new Sub CA certificates or information about them are delivered to end entities in an authentic form. The TSP SHALL (also) publish the fingerprints of their Sub CA certificates via a different channel than the Sub CA certificate.

[EVCP] The TSP SHALL provide test web pages secured with appropriate TLS server certificates, from the TSP, chained up to a public Root CA. Web pages SHALL be provided with one valid, one expired, and one revoked certificate.

2.3 Time or frequency of publication

The TSP SHALL describe in their CPS the timing or frequencies of the publications listed in section 2.2.

2.4 Access controls on repositories

The directories SHALL be available on the Internet without access restriction and SHALL be restricted to read-only and protected against unauthorized manipulation as well as data loss.

[3145] [VSNfD] The end entities SHALL be able to decide for themselves whether their end entity certificates are to be published on the Internet or, if applicable, only in internal customer-specific directories. The revocation lists as well as Root and Sub CA certificates SHALL in any case be provided in a directory on the Internet.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

If a certificate is issued to a natural person in association with a legal person, then the certificate attributes identifying the organization SHALL reflect the legal entity and the subject identifier in the certificate SHOULD be the natural person.

See section 7.1.2 and 7.1.4.

3.1.1 Types of names

See section 7.1.2 and 7.1.4.

3.1.2 Need for names to be meaningful

See section 7.1.2 and 7.1.4.

3.1.3 Anonymity or pseudonymity of subscribers

See section 7.1.2 and 7.1.4.

3.1.4 Rules for interpreting various name forms

See section 7.1.2 and 7.1.4.

3.1.5 Uniqueness of names

Over the lifetime of a CA, an already used Subject Distinguished Name SHOULD NOT be assigned to another subject.

[SSL] The Subject Distinguished Name in domain-validated certificates is excepted from this if an applicant has proven his legal right of ownership.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

The TSP SHALL verify the identity of the applicant as well as the subject and verify that the certificate applications are accurate, authorized and complete according to the available evidence.

The TSP SHALL request a physical address or other contact information from the applicant.

The TSP SHALL use either direct evidence or attestations from appropriate and authorized sources to verify the identity and, if applicable, other attributes of the subjects. Evidence MAY be submitted in hard copy or electronically. The TSP SHALL verify the authenticity of the evidence provided for alterations and forgeries. All information used for the verification of the identity and further attributes of the subject SHALL be documented.

The TSP SHALL require only the evidence necessary to verify identity.

Verification of identity SHALL take place in an appropriate time frame of registration.

[EVCP] The TSP SHALL publish online in an appropriate and easily accessible manner sufficient information, such as name, jurisdiction, and website, to uniquely identify the authorized sources used to validate identities and shall describe in their CPS in section 3.2 where this information is published. In addition, TSPs SHALL publish the authorized values on the fields listed below that will be included in end entity certificates issued based on information from this source:

- jurisdictionLocalityName (OID 1.3.6.1.4.1.311.60.2.1.1)
- jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)
- jursidictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)

[SMIME] The TSP SHALL use reasonable and secure methods 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. Validation of the domain portion of the email address SHALL NOT be delegated by the TSP to a third party. The TSP MAY rely on validations performed for an Authorization Domain Name (as defined in the Baseline Requirements) as valid for subdomains from that Authorization Domain Name. The verification methods used SHALL be described by the TSP in their CPS.

[VS-NfD] The TSP SHALL additionally verify the applicant's security approval with respect to the use of the PKI.

3.2.1 Method to prove possession of private key

If the key pair is not generated by the TSP, the certificate request verification process SHALL cover ownership or control of the private key.

[3145] If the key is generated by the subscriber, at least the public key and the subject attributes SHALL be signed with the private key. The TSP SHALL verify the signature.

3.2.2 Authentication of organization identity

[SSL] If the subject is an organization, the TSP SHALL use a reliable method of communication to verify the authorization of the representative to submit a certificate request on behalf of the organization.

The TSP MAY verify the authenticity of the certificate application directly with the representative or through an authoritative source within the applicant's organization.

The TSP SHALL establish a process that allows the applicant to specify individuals who may submit certificate approvals. If appropriate individuals are designated by the applicant, the TSP SHALL reject all certificate applications from non-specified individuals. Upon written request by the applicant, the TSP SHALL provide the applicant with a list of authorized certificate applicant individuals.

[NCP] Evidence of the identity of a legal subject and, if applicable, other attributes SHALL be verified against a duly authorized applicant either directly, in the physical presence of an authorized representative of the legal entity, or indirectly, using means that provide assurance comparable to physical presence.

If the subject is a legal person or an organizational entity identified in association with a legal person, then the following SHALL be verified:

- Full name of the organizational entity/legal person based on national or otherwise applicable identification practices.
- If applicable, the association of the legal person to the organizational entity identified in association with this legal person, which is entered in the Organization attribute in the certificate.

If the subject is a device or system operated on behalf of a legal person or an organizational entity identified in association with a legal person, then the following SHALL additionally be verified:

- Identifier of the device or system

[SSL] If the identity of an organization, address of an organization, a company name, or a brand name are to be included in a certificate, then they SHALL be verified against documents provided by or through communication with at least one of the following entities:

- Government agency in the jurisdiction of incorporation, existence or recognition of the legal person (identity, address, company name, brand name).
- Third party database that is regularly updated and considered a reliable source of data (identity, address, company name, brand name)
- On-site visit by the TSP or an authorized representative (identity, address)
- Certification letter (identity, address, company name, brand name)
- Utility bill, bank statement, credit card statement, state-issued tax receipts, or other forms of identification that the TSP identifies as acceptable (address, firm name, brand name)
- Communication with a government agency for the administration of firm or brand names (firm name, brand name)

If the countryName attribute is to be set, the country associated with the subject SHALL be verified based on the following information:

- IP address range assignment by country for the IP address of the web page as specified by the DNS record for that web page or the IP address of the applicant
- ccTLD of the requested domain name
- Information from the domain name registrar
- Using one of the methods listed in the previous section

For IP address verification, a process SHOULD be implemented to detect the use of proxy servers.

Before using a data source as a reliable data source, the source SHALL be evaluated for reliability, accuracy, and resistance to change or falsification. The following points SHALL be considered:

- Age of the information provided
- Frequency of updates of the information source
- Data provider and the purpose of data collection
- Data availability
- Data integrity

Databases maintained by the CA, its owner, or its affiliates are not considered a reliable data source if the primary purpose of the database is to collect information to meet validation requirements.

[QCP-w] The applicant's connection to the specified domain name SHALL be additionally verified.

3.2.2.1 [SSL] Authentication of domain identities

Each fully qualified domain name (FQDN) to be listed in a certificate SHALL be validated by the TSP as follows:

- If the FQDN does not contain "onion" as the rightmost entry, the TSP SHALL validate the FQDN using one of the methods described in the Baseline Requirements [CAB/BR] section 3.2.2.4 or EV Guidelines [EVCG] section 11.7.
- If the FQDN contains "onion" as the rightmost entry, the TSP SHALL validate the FQDN according to Appendix C of the Baseline Requirements [CAB/BR] or Appendix F of the EV Guidelines [EVCG].

The validation of control over an IP address SHALL be performed according to section 3.2.2.5 of the Baseline Requirements [CAB/BR].

Validations performed MAY be valid for issuance of multiple certificates over time. A validation SHALL have been initiated within 825 days prior to certificate issuance.

Furthermore, the requirements from section 3.2.2.6 and 3.2.2.8 of the Baseline Requirements [CAB/BR] or the further requirements from section 11 of the EV Guidelines [EVCG] SHALL be considered. The TSP SHALL list in their CPS the used methods.

3.2.3 Authentication of individual identity

[NCP] Evidence of the identity of a natural subject and, if applicable, other attributes SHALL be verified against the natural person either directly, in the physical presence of the person or a duly authorized applicant, or indirectly, using means that provide assurance comparable to physical presence.

If the subject is a natural person, then the following SHALL be verified:

- Full name of the person (surname, given name)
- Date and place of birth, references to nationally recognized identification documents or other attributes that can be used for unique identification

If the subject is a natural person identified in association with a legal person, then the following SHALL additionally be verified:

- Full name and legal status of the associated legal person
- Relevant registration information of the associated legal person
- Affiliation of the natural person to the legal entity
- Confirmation of the legal person and natural person that the attributes of the subject also identify the organization

If the subject is a device or system operated by a natural person, then the following SHALL be verified:

- Identifier of the device or system
- Nationally recognized identity number or other attributes that can be used for unique identification of the natural person

[SSL] The TSP SHALL verify the name, address and authenticity of the certificate request.

At a minimum, a legible copy of a valid, government-issued photo identification showing the face of the applicant in a recognizable manner SHALL be used to verify the name. The copy SHALL be examined for signs of alteration and forgery.

A form of identification that the TSP deems trustworthy SHALL be used for address verification. The government photo identification used for name verification may be used.

A reliable method of communication SHALL be used to verify the authenticity of the certificate request (cf. Baseline Requirements Reliable Method of Communication).

[QCP-w] The applicant's connection to the specified domain name SHALL be additionally verified.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

If the applicant is not the subject, then the full name and authorization of the applicant to act on behalf of the subject SHALL be verified.

To avoid conflicts of interest, the TSP and the applicant SHALL be different entities. The only exception is the organization that performs RA tasks and issues a certificate to itself or to individuals identified in connection with that organization. The exception SHALL be described in the TSP's policies.

3.2.6 Criteria for interoperation

No stipulation.

[SSL] The TSP SHALL publish all cross-certificates that have indicated the TSP's CAs as subjects, provided that the TSP has initiated or accepted these cross-certifications.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The TSP SHALL check the existence and validity of the certificate to be renewed and the validity of the information verifying the identity and attributes of the subject according to section 3.2.

Existing evidence MAY be reused for the validation of identity, taking into account the applicable legal situation and the remaining validity of the evidence.

[SSL] Verification of information used for certificate renewal SHALL NOT be older than 825. If the verification is older than 825 days, the information SHALL be checked for validity and accuracy.

[EVCP] The TSP SHALL perform all authentication and verification tasks according to the EV Guidelines [EVCG] to ensure that the certificate request is authorized and the information is still accurate and valid.

If an applicant already has a valid EV certificate from the TSP at the time of application, the TSP MAY rely on prior authentication and verification according to section 11.14.1 of the EV Guidelines [EVCG].

For the re-issuance of EV certificates, the verification of the information specified in section 11.14.3 of the EV Guidelines [EVCG] SHALL NOT be older than 13 months. The period of 13 months starts with the receipt of the information.

For the issuance of replacement certificates, the TSP MAY use already verified certificate requests, as long as the certificate to be replaced has not been revoked due to fraud or other illegal actions and the expiration date of the replacement certificate and the Subject Information remain identical.

3.3.2 Identification and authentication for re-key after revocation

No stipulation.

3.4 Identification and authentication for revocation request

TSPs SHALL specify in their CPS the methods for identification and authentication of revocation requests.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

The Root CA and the TSP SHALL define in their CPS who may apply for which certificates, describing the possible roles (e.g., applicant, subject of the certificate, natural persons, legal persons).

[SSL] The TSP SHALL maintain an internal database containing all certificate requests and certificates that have been rejected or revoked due to suspicion of fraudulent use. Further applications from end entities listed in this database SHALL be checked for suspected fraudulent use and rejected if necessary.

[EVCP] The issuance of certificates SHALL be restricted to the following organizational forms (for definitions see section 1.6.1):

- Business entities,
- Government entities,
- Private organizations and
- Non-commercial entities.

[3145] Suspended end entities MAY NOT submit certificate applications.

The TSP SHALL check their database to see if the end entity has been registered before. If this is the case, all further certificates SHALL be assigned to this registration, so that in case of suspension of the end entity, all certificates of this end entity can be suspended or revoked simultaneously according to the terms of use.

4.1.2 Enrollment process and responsibilities

4.1.2.1 Applying for a Root-CA certificate

The Root TSP SHALL describe the application processes and responsibilities in its CPS.

4.1.2.2 Applying for a Sub CA certificate

Before issuing a Sub CA certificate, the Root TSP SHALL have obtained

- a certificate application form provided by the Root CA and completed and signed by the requesting TSP,
- an electronic certificate request ("Certificate Signing Request", CSR) in the format specified by the Root CA, and
- any other documents required by the Root TSP (e.g., commercial agreements).

In addition, the Root TSP SHALL assure that the requesting TSP owns or has control over the private key associated with the public key submitted for certification.

The applying TSP SHALL confirm the acceptance of the terms of use (see section 9.6.1) and the correctness of the information provided in the certificate application form.

The certificate application form MAY be submitted in electronic form. In this case, however, it must be provided with at least an advanced electronic signature or an advanced electronic seal.

4.1.2.3 Applying for an end entity certificate

The TSP SHALL clearly describe the application process including the interfaces to be used for the end entities.

If the applicant is not the subject of the certificate and the subject of the certificate is a natural or legal person, the certificate application SHALL consist of two parts:

- The first part SHALL be signed by the applicant and include at least the following points:
  - the confirmation of knowledge and acceptance of the terms of use,
  - the consent to the duties of the applicant,
  - consent to the use of an appropriate cryptographic module (HSM or QSCD), if required by the TSP,
  - consent to the recording of the data recorded within application and processing as well as in the issuance and delivery and, if applicable, later revocation of a certificate by the TSP,
  - information whether the applicant wishes the certificate to be published and whether it is accepted by the subject of the certificate,
  - confirmation that the data to be included in the certificate is correct,
  - the obligations of the subject of the certificate.
- The second part SHALL be signed by the subject of the certificate and include at least the following points:
  - the confirmation of knowledge and acceptance of the terms of use,
  - the consent to the duties of the subject,
  - consent to the use of an appropriate cryptographic module (HSM or QSCD), if required by the TSP,
  - consent to the recording of the data recorded within application and processing as well as in the issuance and delivery and, if applicable, later revocation of a certificate by the TSP.

  Note on certificates for legal persons: If the applicant is the official representative of the subject of the certificate, or the subject is the official representative of the applicant, the two parts of the application MAY be signed together.

If the applicant is also the subject of the certificate or the subject of the certificate is a device, the certificate application form MAY consist of either one or two parts with the above contents.

Certificate applications MAY be submitted in electronic form unless otherwise specified by the TSP.

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

[SSL] End entities SHALL submit both a formal certificate request with the above information and an electronic certificate request (e.g., in PKCS#10 format) to the TSP to request a certificate.

The TSP MAY, taking into account the validity periods of identifications, accept a certificate application form in which multiple certificates of an applicant are requested, provided that a separate valid electronic certificate request is submitted for each certificate.

[EVCP] The first part of the application (see above) SHALL include confirmation of the applicant's authorization to apply for a certificate on behalf of the organization.

The following roles (for definitions see section 1.6.1) SHALL be implemented for the applicants:

- certificate requester,
- certificate approver,
- contract signer as well as
- if applicable, representative of the applicant (in case the applicant is associated with the TSP).

The applicant MAY assign one person to more than one of the listed roles and may fill the roles with more than one person.

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

4.2 Certificate application processing

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

The TSP MAY outsource the processing of certificate applications or parts thereof to External RAs. In this case, the TSP SHALL ensure that the process as a whole meets the requirements of this CP. Accordingly, the TSP SHALL identify and authenticate the External RAs and SHALL ensure that the information exchanged between External RA and TSP is securely shared.

4.2.1 Performing identification and authentication functions

The TSP SHALL perform identification and authentication according to section 3.2 and describe in their CPS the processes and specifications for performing identification and authentication including verification of all data requested by the applicant for inclusion in the certificate.

[SSL] If certificate applications are verified by external customer RAs, the TSP SHALL

- before including an FQDN in a certificate, ensure that it originates from the customer's permitted name range,
- before including another name (not an FQDN) in a certificate, ensure that the name corresponds either to the customer himself or to one of the customer's contractual partners, or that the TSP's customer represents him.

The TSP SHALL impose these requirements on customer RAs as a contractual requirement and verify compliance with them.

[SSL] The TSP SHALL implement and describe in the CPS, where applicable, additional required validations for "high risk certificates".

4.2.2 Approval or rejection of certificate applications

Approval or rejection of certificate applications SHALL be made by RAs of the TSP or External RAs approved by the TSP.

If an end entity requests a certificate for a key that was not generated by the TSP, the TSP SHALL verify that the end entity has possession of or control over the private key.

[SSL] If a key is submitted in an application that does not meet the requirements of section 6.1.5 and 6.1.6 or it is a "Debian weak key" or the key was previously generated by a Sub CA, the TSP SHALL reject the application.

If a certificate request does not contain all the required information, the TSP SHALL request the missing information from the applicant or, after the TSP has obtained it through another reliable means, the TSP SHALL have it confirmed by the applicant.

TSPs SHALL describe in section 4.2 of their CPS the treatment of CAA records for FQDNs compliant with the [BR] and list the issuer domain names accepted by the TSP.

[3145] If a key is submitted in an application that does not meet the requirements of section 6.1.5 and 6.1.6, the TSP SHALL reject the application.

If the use of cryptographic tokens is required, the TSP SHALL ensure via technical measures that the supplied public key is correctly mapped to the token and the registration data.

[QCP-l-qscd] [QCP-n-qscd] The TSP SHALL ensure that the public key presented is from a key pair generated in a QSCD.

[EVCP] If not all required information is included in a certificate request, the TSP SHALL have the missing information confirmed by the certificate approver or contract signer and not by the certificate requester (for roles see section 4.1.2.3).

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The TSP SHALL ensure integrity and authenticity when issuing the certificates and take appropriate measures (technical, organizational or personnel) to protect against falsification of the data before issuing the certificates. The process of issuing the certificates SHALL be securely linked to the associated registration and, if applicable, to the public key provided by the applicant.

When an end entity delivers the public key to be included in the certificate, the TSP SHALL make sure that the end entity is in possession of or has control over the private key. This can be done, for example, by handing over a key by means of a signed PKCS#10 request whose signature the TSP verifies before issuing the certificate.

If the TSPs generate the keys for the end entities, they SHALL ensure the confidentiality of the keys in the generation process.

[SSL] The end entity certificates SHALL be published as "pre-certificates" in a sufficiently large number of CT log servers (Certificate Transparency according to RFC 6962) before issuance. The time-stamped confirmations returned in this process SHALL be included in the certificates as an extension with the OID 1.3.6.1.4.1.11129.2.4.2.

[3145] The TSP SHOULD check that no certificates with the same attributes but different keys exist before issuing certificates. In this case, no further certificate with these attributes SHOULD be generated.

If the use of cryptographic tokens is required, the TSP SHALL

- ensure that the correct public key of the selected token is included in the certificate and that the certificate is stored on the token,
- ensure that the personalized token is sent to the correct recipient,
- design the shipment/handover of the token 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.

The TSP SHALL describe the procedures for issuing the tokens in the terms of use and the CPS.

If the TSP generate the keys for the end entity certificates, the TSP SHALL

- ensure that the keys are delivered to the correct recipient,
- ensure that the confidentiality of the keys is guaranteed during delivery,
- ensure that keys are deleted at the TSP after delivery to the correct recipient, unless the TSP provides key backup for end entities.

The TSP SHALL describe the procedures for handing over the keys in the terms of use and the CPS.

[VS-NfD] In addition to the requirements for [3145] above, the specifications from [VSA] for the protection of the keys according to their classification SHALL be considered.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The TSP SHALL, if applicable, deliver the issued end entity certificates to the end entities, i.e., the Applicant and/or the Subject of the Certificate, or notify them of the issuance of the same.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

The TSP SHALL publish end entity certificates accessible to everyone, provided that the end-entities (applicant or, if applicable, the subject of the certificate) have agreed to the publication, otherwise they SHALL NOT publish the end entity certifcates.

The TSP SHALL describe the processes of publication in their CPS, see also section 2.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

TSPs SHALL describe in their CPS the permitted and non-permitted uses of the end entity certificates.

4.5.2 Relying party public key and certificate usage

No stipulation.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

The TSP SHALL define the circumstances under which a renewal is allowed. 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.

[3145] The TSP SHALL describe in their CPS as well as in the terms of use in which period and under which circumstances a renewal is allowed.

Revoked certificates SHALL NOT be renewed.

Certificates SHALL NOT be renewed if they have been revoked due to a security incident.

4.6.2 Who may request renewal

See section 4.1.1.

4.6.3 Processing certificate renewal requests

If the terms of use have changed from the terms of use in effect at the time the predecessor certificate was applied for, the TSP SHALL obtain acceptance of these new terms of use from the subscriber before issuing a new certificate.

The TSP SHALL verify the validity of the expiring certificate and the subject's original submitted identification data and attributes prior to renewal. Applications SHALL be complete, accurate, current, and authorized.

When certificates are renewed, the same validity periods SHALL be applied as for initial issuance, unless otherwise specified in the TSP CPS (see section 6.3.2.3).

[SSL] The TSP MAY use existing documents and data for validation, provided they are not older than 825 days.

[EVCP] The TSP SHALL set the same expiration date and subjectDN in a renewed end entity certificate as in the original certificate.

[3145] The TSP SHALL describe in their CPS the necessary processes in case the integrity of the original data is no longer given.

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 TSP SHALL specify the circumstances under which re-keying is permitted.

[3145] TSPs SHALL describe in their CPS as well as in the terms of use during which period and under which circumstances re-keying is allowed. Re-keying SHALL NOT be allowed for revoked certificates.

Re-keying SHALL NOT be allowed for certificates that have been revoked due to a security incident.

4.7.2 Who may request certification of a new public key

See section 4.1.1.

4.7.3 Processing certificate re-keying requests

If the terms of use have changed from the terms of use in effect at the time the predecessor certificate was applied for, the TSP SHALL obtain acceptance of these new terms of use from the subscriber before issuing a new certificate.

The TSP SHALL verify the validity of the expiring certificate and the subject's original submitted identification data and attributes prior to re-keying. Applications SHALL be complete, accurate, current, and authorized.

In the case of re-keying, the same validity periods SHALL be applied as for initial issuance, unless otherwise specified in the TSP CPS (see section 6.3.2.3).

[SSL] The TSP MAY use existing documents and data for validation, provided they are not older than 825 days.

[3145] TSPs SHALL describe in their CPS the processes required in the event that the integrity of the original data is no longer maintained. The TSP SHALL enforce the generation of new keys and verify that they meet the requirements specified in sections 6.1.5 and 6.1.6.

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 TSP SHALL require subscribers to notify the TSP of the change of registered data in the validity period of the certificates issued based on the registered data and SHALL inform the end entities 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 terms of use have changed from the terms of use in effect at the time the predecessor certificate was applied for, the TSP SHALL obtain acceptance of these new terms of use from the subscriber before issuing a new certificate.

TSPs SHALL verify the validity of the expiring certificate and any unmodified subject identification data and attributes originally submitted before modifying certificate data. The data SHALL be complete, accurate, current, and authorized.

[3145] TSPs SHALL describe in their CPS the processes required in the event that the integrity of the original data is no longer maintained.

The TSP SHALL enforce the generation of new keys and verify that they meet the requirements specified in sections 6.1.5 and 6.1.6.

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

Due to the criticality of certificate revocation or suspension, the TSP and all end entities involved are obligated to know the revocation reasons and deadlines to be observed as well as the processes. These SHALL therefore be described in the CPS of the TSP.

In addition, end entities in particular SHALL be informed about the revocation reasons as well as the available interfaces for requesting revocation, e.g. in the general terms and conditions, terms of use, PDS etc.

4.9.1 Circumstances for revocation

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 an organization not associated with the Sub CA, 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 TSP is not operating 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 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.

In addition, the Root TSP or the TSP MAY specify other revocation reasons in their CPS.

4.9.1.2 Reasons for revoking an end entity certificate

End entity certificates must be revoked for various reasons. Since different revocation deadlines are defined depending on the revocation reasons, the revocation reasons are listed below sorted by the deadlines.

In addition, a TSP MAY define further revocation reasons in its CPS.

4.9.1.2.1 Short-term revocation within 24 hours

An end entity certificate SHALL be revoked within 24 hours if

- a written revocation request, even without giving reasons, has been made by the subscriber,
- 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 has been compromised or disclosed to an unauthorized person or an organization not associated with the subject.

[SSL] In addition, an end entity certificate SHALL be revoked if it is determined that the validation of domain authorization or control over an FQDN or IP address in the certificate cannot be trusted.

[S/MIME] In addition, an end entity certificate SHALL also be revoked if it is determined that the e-mail address included in the certificate may no longer legally be used.

[QCP] In addition, an end entity certificate SHALL be revoked if it is determined that the private key of the end entity certificate has been lost.

4.9.1.2.2 Medium-term revocation within five days

An end entity certificate SHOULD be revoked within 24 hours and SHALL be revoked within five days at the latest if

- it is determined that the certificate was not issued in accordance with the CPS of the Sub CA,
- if the private key no longer meets the requirements of section 6.1.5 and 6.1.6, or methods have become known that compromise the private key or allow the private key to be calculated from the public key, or that there is unambiguous evidence that the method used to generate the private key was insufficient.
- it is determined that the certificate has been misused,
- the end entity is found to have violated one or more material agreements or terms of use,
- it is determined that the information in the certificate is not correct or there have been significant changes to it.

[SSL] In addition, an end entity certificate SHALL be revoked if

- the TSP's right to issue certificates has expired or has been revoked or terminated in accordance with the Baseline Requirements of the CA/Browser Forum and no arrangements have been made for continuing the revocation services,
- it is determined that the use of an FQDN or IP address in the certificate is no longer permitted by law,
- it is determined that a wildcard certificate was used to authenticate a fraudulently misleading sub-FQDN.

4.9.1.2.3 Revocation in a reasonable, unspecified period of time

An end entity certificate SHALL be revoked if

- the TSP ceases operation and no arrangements have been made for continuing the revocation services,
- security incidents, integrity problems or malfunctions require it.

[3145] In addition, an end entity certificate SHALL be revoked if

- an admissible justification is provided by a third party,
- the end entity is suspended.

The aforementioned revocation reasons usually require further checks or coordination, so that no time periods can be specified for this in advance. In these cases, revocation SHALL take place within a reasonable period of time and as fast as possible.

4.9.2 Who can request revocation

The revocation of a Sub CA SHALL always be requested by an authorized representative of the TSP. If one of the revocation reasons listed in section 4.9.1.1 is identified by or reported to the Root TSP, a revocation SHALL also be initiated by the Root TSP. The further organizational and procedural requirements SHALL be described in the CPS of the Root TSP.

[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 Root TSP and SHALL be described in the CPS of the TSP.

The revocation of an end entity certificate SHALL always be requested by the end entity itself or the responsible RA. If one of the reasons for revocation listed in section 4.9.1.2 is identified by the TSP or reported by a third party and can be comprehended by the TSP, a revocation SHALL be initiated by the TSP. The further organizational and procedural requirements SHALL be described in the CPS of the TSP.

[SSL] [SMIME] In addition, the revocation of an end entity certificate SHALL be initiated by the TSP if a representative of the relevant trusted root programs reports one of the revocation reasons listed in section 4.9.1.2.

[3145] In addition, the revocation of an end entity certificate SHALL be initiated by the TSP if the end entity is suspended.

[VS-NfD] In addition, the revocation of an end user certificate SHALL be initiated by the TSP upon a justified request by the security officer.

4.9.3 Procedure for revocation request

For the 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 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 reviewed by the responsible TSP and that are not classified as a legitimate revocation reason.

The authorized applicants SHALL be informed about the provided interfaces and their use.

[SSL] [SMIME] The interfaces for reporting problems, such as suspected key compromise, certificate misuse, or other types of fraud or inappropriate behavior related to certificates, SHALL be listed on the TSP web pages and in the relevant CPS (in the contact information in section 1.5.2 according to RFC3647).

Both the revocation applicant and the subject of the revoked certificate SHALL be informed about the revocation, if possible.

Revoked certificates SHALL NOT be unrevoked again.

[SSL] [SMIME] After revocation of a Sub CA certificate, the TSP SHALL update the CCADB. 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.

The processes for revoking Root and Sub CAs certificates SHALL be described in the Telekom Security Root-CPS.

The processes for revoking end entity certificates SHALL be described in the CPS of the TSP.

[SSL] The TSP SHALL be able to respond 24/7 to high priority problem reports and forward a report to law enforcement if needed and / or revoke the certificates affected by the problem.

[3145] The processes for suspending end entities SHALL be described in the TSP's CPS.

[VS-Nfd] The processes for revoking end entity certificates including the specified deadlines SHALL be released by the security officer.

4.9.4 Revocation request grace period

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

4.9.5 Time within which CA must process the revocation request

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.

End entity 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 by a subscriber. In this case, the TSP MAY, if this procedure is described in the CPS, set the desired date for revocation of the certificate listed in the revocation request as the date of receipt of the authorized revocation request.

For revocations that are not based on authorized revocation requests but result from problem reports, the deadlines listed in section 4.9.1 apply.

[SSL] Within 24 hours of receipt of a problem report, the facts and circumstances SHALL be investigated by the affected TSP and initial feedback on the findings available until then SHALL be provided to the end entity and the reporting person. Subsequently, the results of the analysis SHALL be discussed with the end entity and the reporting person and a decision SHALL be made as to whether a revocation is required. If revocation is required, the timing of revocation SHALL be determined, taking into account the requirements of section 4.9.1 and considering the following aspects:

- the nature of the alleged problem (scope, context, severity, magnitude, risk of harm)
- the effects of revocation (direct and collateral effects on end entities and relying parties)
- the number of problem messages for a certificate or end entity
- the entity that set the message as well as
- the relevant legislation

In addition to the listed deadlines, a TSP MAY specify shorter deadlines in its CPS for certain revocation reasons.

4.9.6 Revocation checking requirement for relying parties

Relying parties SHALL use the certificate status services offered by the TSP according to section 4.10 to check the status of certificates.

4.9.7 CRL issuance frequency

Revocation lists that provide information about revoked Sub CAs SHALL be updated within 24 hours after revocation of a Sub CA certificate and regularly at least every 12 months. This requirement applies to the CA Revocation Lists (CARL) issued by the Root CAs as well as by the Sub CAs issuing further Sub CA certificates (hierarchies with multiple Sub CA levels).

Revocation lists that provide information about revoked end entity certificates (Certificate Revocation Lists (CRL)) SHALL be updated regularly at least every 24 hours.

[SSL] [3145] Revocation lists that provide information about revoked end entity certificates SHALL also be issued and published following the revocation of an end entity certificate in addition to the regular issuance.

4.9.8 Maximum latency for CRLs

Newly issued revocation lists SHALL be published within one hour after their generation.

4.9.9 On-line revocation/status checking availability

The Root TSP MAY offer online status information for the Sub CA certificates via OCSP.

The Sub CAs SHALL offer online status information for the end entity certificates via OCSP.

4.9.10 On-line revocation checking requirements

If relying parties check the status of certificates via OCSP, they SHALL use RFC6960-compliant OCSP client components, i.e. they SHALL be able to process OCSP responses of the type "id-pkix-ocsp-basic response" as well as the signature algorithm "sha256WithRSAEncryption" and verify that

- the certificate referenced in the response matches the certificate in the request,
- the signature of the response is valid,
- the identity of the OCSP signer matches the intended recipient of the request,
- the OCSP signer is authorized to provide status information about the requested certificate at the time of signing,
- the time of creation of the status information ("thisUpdate") is sufficiently current and,
- if specified, the time for the scheduled update of the status information ("nextUpdate"), is in the future.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

The specifications made in section 4.9.1 apply.

4.9.13 Circumstances for suspension

Root CA and Sub CA certificates SHALL NOT be suspended.

End entity certificates MAY be suspended, there are no specific requirements in this regard. If suspension is offered by a Sub CA, the TSP SHALL specify the circumstances for suspension in the relevant CPS.

[SSL] End entity certificates SHALL NOT be suspended.

[3145] In addition to the revocation or suspension of end entity certificates, end entities SHALL also be suspended under certain circumstances. The specifications and processes SHALL be described in the CPS of the TSP.

4.9.14 Who can request suspension

If suspension is offered by a Sub CA, the eligible applicants for suspension SHALL be defined in the CPS of the TSP.

[SSL] Not applicable.

[3145] Eligible applicants for suspension of end entities SHALL be described in the TSP's CPS

4.9.15 Procedure for suspension request

If suspension is offered by a Sub CA, the procedures for suspension SHALL be defined in the CPS of the TSP.

[SSL] Not applicable.

[3145] The processes for suspending end entities SHALL be described in the TSP's CPS.

4.9.16 Limits on suspension period

If suspension is offered by a Sub CA, the time periods and deadlines for suspension SHALL be specified in the TSP's CPS.

[SSL] Not applicable.

[3145] The time periods and deadlines for suspension of end entities SHALL be described in the CPS of the TSP.

4.10 Certificate status services

Authentic and integer certificate status services SHALL be provided at least over the validity period of all issued certificates.

Revocation lists or OCSP information or both SHALL be provided for the Sub CA certificates.

Revocation lists and OCSP information SHALL be provided for the subscriber certificates.

[QCP] In addition or in deviation, the following specifications apply to the certificate status services for qualified certificates:

- Certificate status services SHALL be provided beyond certificate validity.
- Revocation lists MAY be provided. If revocation lists are provided, they SHALL be provided at least until all certificates in the scope of the revocation list have expired or are revoked. If revocation lists are provided beyond the certificate validity period, the provisioning time SHALL be described in the TSP's CPS and the integrity of the revocation list SHALL be ensured for the duration of provisioning.

4.10.1 Operational characteristics

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

If revocation list 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.

4.10.1.1 Operational characteristics for the provision of the OCSP responder

The OCSP responders SHALL work conform to RFC6960. Concretizing to RFC6960, requests for certificates with unknown certificate serial numbers SHALL NOT be answered with the status "good" but SHALL be answered with either the error message "unauthorized" or the status "unknown" or "revoked".

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

- For preproduced OCSP responses, such requests SHALL be answered with the error message "unauthorized", since the OCSP responder does not have a preproduced response to the requests and also cannot be produced ad hoc.
- For ad hoc generated OCSP responses such requests SHOULD be answered with the status "unknown", because the OCSP responder does not have a status for the requested serial number, but a valid OCSP response can be produced ad hoc. For ad hoc generated OCSP responses such requests MAY also be answered with the status "revoked", but then the extension "Extended Revoked Definition" according to RFC6960 #4.4.8 SHALL be set.

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 end entity certificates SHALL have a validity of at least 8 hours but no more than 10 days. After a revocation of an end entity certificate, updated information SHALL be available in the OCSP responder within 60 minutes.

[QCP] A validity end (nextUpdate) MAY be set, the specification is not mandatory.

The OCSP responses created once to OCSP requests MAY be kept in the OCSP responder and reused within their validity for further requests as long as the status of the requested certificate has not changed.

[SSL] The following conditions apply to the reuse of existing OCSP responses that are still valid:

- If OCSP responses have a validity of less than 16 hours, they SHALL NOT be reused after half of their validity has expired.

- If OCSP responses have a validity of 16 hours or more, they SHALL NOT be reused more than 4 days after they are issued and more than 8 hours before their validity expires.

4.10.1.2 Operational characteristics for the provision of revocation lists

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

Revocation lists that provide information about revoked Sub CA certificates SHALL NOT exceed a validity of 12 months.

Revocation lists that provide information about revoked end entity certificates SHALL NOT exceed a validity of 10 days.

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

Revoked certificates MAY in principle be removed from the revocation list after their expiry date, but they SHALL still be in the next regular revocation list after their expiry date, according to section 4.10.1.2.

[QCP] If revocation lists are provided, expired certificates SHALL NOT be removed from the revocation list, according to section 4.10.2.

4.10.2 Service availability

The certificate status services SHALL be available 7x24h. In case of a fault, the greatest possible efforts SHALL be made to eliminate the fault within the agreed fault clearance periods.

Sufficient capacity SHALL be provided so that the response time does not exceed 10 seconds under normal operating conditions.

[EVCP] Sufficient capacity SHALL be provided so that the response time does not exceed 3 seconds under normal operating conditions.

[3145] [NCP] The TSP SHALL list in their CPS the maximum downtime of the systems.

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 a TSP offers a key escrow,

- encryption keys MAY be deposited,
- authentication keys and signature keys SHALL NOT be stored in a form that allows decryption of these keys without control of the owner,
- the TSP SHALL ensure that all copies of the private keys are kept under the same security level as the original and are only handed over to authorized recipients,
- there SHALL NOT be created more copies of the private keys than are required to ensure continuity,
- 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 TSP SHALL define the approach to managing information security in an information security policy approved by management and SHALL have an appropriate information security management system (ISMS, e.g., based on ISO 27001) that, among other things,

- manages the development, implementation and maintenance of security concepts including regular risk analyses for the services of the TSP,
- 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 services of the TSP.

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

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)
- Network security and firewall management
- Integrity assurance of systems (including configuration management) and trusted code used
- Malware detection and prevention
- 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 of the TSP.

5.1 Physical controls

The TSP SHALL implement physical controls to prevent loss, theft, damage, or compromise of assets, media, and information.

5.1.1 Site location and construction

TSPs SHALL operate their systems in appropriate locations in secure premises with adequate physical protection and consider potential natural disasters (e.g., floods) as well as disaster recovery when selecting locations.

If premises are shared with other non-TSP organizations, the non-TSP 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 operate 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.

[VS-NfD] The instructions for the protection of VSIT rooms according to § 29 VSA [VSIT] SHALL be taken into account 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 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

The TSP SHALL establish secure disposal processes to prevent unauthorized use or access to information. 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 TSP: has the overall responsibility for the services of the TSP
- Security Officer: plans and monitors the implementation of security controls
- Registration staff: reviews and processes applications for certificate-issuance, -suspension, -revocation or -renewal
- Administrator: configures and maintains the IT structure including networks, databases and servers
- CA Operator: generates Root- and CA-keys and -certificates and technically sets up the access rights for the Registration staff (in the case of multi-level RA concepts, the top instance of the RA).
- Internal Auditor: checks for example log data, databases and paper-based documentation of the TSP on a regular basis as well as in case of discrepancies

[SSL] In addition to the roles listed above, the TSP SHALL establish the role of the Validation Specialist.

The TSP SHALL describe the relevant roles of the TSP incl. an overview of the assigned activities in the CPS.

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 by the TSP and corresponding agreements shall be made with the third parties to ensure that all regulations specified by the TSP are also complied with by the third parties.

5.2.2 Number of persons required per task

At least one representative SHALL be appointed for all roles listed in section 5.2.1.

Security-relevant or -critical activities, such as generation, backup and recovery of Root CA or 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.

[EVCP] Certificate applications for end entity certificates SHALL be validated and released using the dual control principle. The TSP SHALL implement auditable security controls to ensure the dual control principle.

The TSP SHALL describe the security-relevant and -critical activities for which a dual control principle (or more) is required in their CPS.

5.2.3 Identification and authentication for each role

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

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 management of the TSP and from the individual to whom the role is to be delegated.

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

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 of the TSP entrusted with generating and revoking certificates SHALL be independent of other organizations in their decisions to establish, provide, maintain, and suspend 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 duties that could affect trust in the services provided by the TSP. This applies to all employees in trusted roles as well as senior managers and executives.

The TSP SHALL document this structure that ensures impartiality of operation.

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.

[EVCP] Identification of persons to be entrusted with a trusted role SHALL be done face-to-face and by presenting an official identification document.

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 by the TSP and corresponding agreements SHALL be made with the third parties 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

The following roles SHALL be separated:

- Management of the TSP
- IT security officer and/or internal auditor
- RA
- Administrator and/or CA-Operator

In addition, the persons in the above roles SHALL NOT also be applicants for end entity certificates, except for applications for the TSP's own certificates and certificates for the TSP's employees. The exceptions SHALL be described by the TSP in its CPS.

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 services provided by the TSP,
- familiarity with security procedures for personnel with security responsibilities, and
- experience with information security and risk assessment sufficient to perform management functions.

The TSP SHALL verify a person's identity and trustworthiness before hiring them.

TSP employees SHALL have sufficient expert knowledge and qualifications to perform their job 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 activities.

5.3.2 Background check procedures

No stipulation.

[EVCP] The TSP SHALL ensure that a person who is to be assigned to a trusted role has successfully completed a background check that includes checking of

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

[3145] [VS-NfD] The TSP SHALL ensure 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

No stipulation (see section 5.3.1).

[SSL] The TSP SHALL train or have trained all staff involved in validating certificate applications 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/or CPS, and the [BR].

The TSP SHALL maintain evidence of this training and document that each employee involved in validation has the required know-how before taking on the activities.

In addition, the TSP SHALL require all validation specialists to pass an examination provided by the TSP on the information verification requirements outlined in the [BR].

5.3.4 Retraining frequency and requirements

The TSP SHOULD provide regular training (at least annually) to their staff on current threats and security practices.

The TSP SHALL ensure, through appropriate regular training, 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

TSP personnel SHALL be accountable for their actions. Appropriate sanctions SHALL be imposed on individuals who violate 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.

[SSL] The TSP SHALL verify that third party personnel involved in the issuance of certificates meet the training and qualification requirements specified in section 5.3.3 and the document retention and event logging requirements specified in section 5.4.1.

[3145] The TSP SHALL clearly define to involved third parties their responsibilities and relevant practices and make appropriate arrangements to ensure that these are implemented by the third parties.

5.3.8 Documentation supplied to personnel

Role owners SHALL be provided with role descriptions that, in addition to the responsibilities and duties resulting from the role, at least specify the required

- (minimum) authorizations,
- segregation of duties,
- dual control principles,
- background checks and
- training and awareness measures.

Where required, these role descriptions SHALL distinguish between general roles and TSP-specific roles.

5.4 Audit logging procedures

5.4.1 Types of events recorded

5.4.1.1 Activities of persons

The TSP SHALL record the following activities of TSP staff and external RAs:

- all activities related to the processing of requests for issuance, renewal and revocation of certificates,
- all activities related to the lifecycle of Root and Sub CA certificates and keys, including at least key generation, storage, backup, recovery, archiving and destruction, generation and revocation of the Root and Sub CA certificates, and the lifecycle of the HSM.

[SSL] In addition to the listing above, the TSP SHALL record the following activities:

- validations according to the [BR],
- telephone conversations (date, time, telephone number, conversation partners, results), if these took place within the scope of the validation activities.

[QCP-n-qscd] [QCP-l-qscd] In addition to the listing above, the TSP SHALL record all events related to the creation of QSCDs.

5.4.1.2 Technical system events

The TSP SHALL log the following technical events including the precise time, the identity of the trigger (if applicable), and the description of the event:

- all significant certificate and key management events,
- all security events on the 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 PKI system access attempts.

Note: The time used to record the above events must be synchronized at least once a day (UTC).

[SSL] The TSP SHOULD log OCSP requests for unassigned serial numbers.

In addition, the TSP SHALL log all (physical) entries and exits to the security zones. The log entries SHALL contain at least the date and time of the entry, a reference to the person or system that generated the entry, and a description of the event.

5.4.2 Frequency of processing log

The events listed in section 5.4.1 SHALL be logged continuously.

The records of the activities listed in section 5.4.1.1 SHALL be evaluated in case of need, e.g. in case of problem reports, in legal proceedings or upon request of internal and external auditors).

The records for the events listed in section 5.4.1.2 SHALL be evaluated as follows:

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

5.4.3 Retention period for audit log

The records of the activities listed in section 5.4.1.1 SHALL be retained by the TSP for a reasonable period of time, taking into account privacy requirements, both to ensure the continuity of the TSP's services and, if applicable, due to legal requirements. The TSP SHALL describe the retention periods in its CPS, see also section 5.5.2.

This retention obligation also applies beyond the termination of a service or the TSP. The termination plan SHALL therefore specify which information is transferred and how this information can be accessed, see also section 5.8.

5.4.4 Protection of audit log

Records of the activities listed in section 5.4.1.1 SHALL be kept confidential, integrity-secured, and protected in such a way that they cannot be easily destroyed or deleted. The TSP SHALL describe in their CPS how the protection of these records is ensured.

[SSL] [SMIME] The TSP SHALL monitor the record retention (e.g., in internal audits).

[3145] The TSP SHALL store the technical system events according to section 5.4.1.2 in a separate tamper-proof system, i.e. not only in the system where the events are logged.

5.4.5 Audit log backup procedures

The TSP SHALL establish safeguarding procedures necessary to achieve the protection objectives listed in section 5.4.4 over the retention periods listed in section 5.4.3.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

[3145] The log files SHOULD not only be stored on the systems used for managing the certificates. They SHOULD also be exported over a secured connection to systems intended for log file storage. Its database SHALL be designed in such a way that entries can only be added, but not deleted. The size of the database 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

[3145] The TSP SHALL archive the records in such a way that they are able to unambiguously assign all issued certificates to a registered subscriber. In addition, tracking SHALL be possible to prevent fraudulent or manipulated certificates from being generated.

5.5.1 Types of records archived

At a minimum, the TSP SHALL archive the following data:

- all registration information, including
  - documents submitted by the applicant in the context of the application for an issue, revocation or renewal,
  - if applicable, the identification data of identification documents,
  - the location of copies of applications (including required attachments) and identification documents,
  - specific requests in the application, (such as consent to publish the certificate),
  - if available, the method of validation of identification documents,
  - the identity of the RA (incl. the RA employee) who reviewed, approved or rejected the application.
- all significant events related to the life cycle of the certificates (application, verification, release, rejection, issuance, acceptance, revocation, renewal, modification)
- all published CP or CPS,
- certification documents and audit reports,
- if necessary, other information required to ensure the continuity of services,
- if applicable, other information issued and received by the TSP that may be needed as evidence in legal proceedings.

The TSP MAY archive additional data, taking into account the relevant privacy aspects, and SHALL describe in their CPS and terms of use which data are archived.

5.5.2 Retention period for archive

TSPs SHALL archive the data related to a certificate for at least 7 years after the expiration of the certificate's validity and SHALL describe the retention period (if applicable per certificate type) in their CPS as well as in the terms of use.

5.5.3 Protection of archive

The information listed in section 5.5.1 SHALL be kept confidential and integrity-secured and protected in such a way that it cannot be easily destroyed or deleted. The TSP SHALL describe in its CPS how the protection of the archived information is ensured.

[EVCP] The TSP SHALL monitor the archiving of the information (e.g., in internal audits).

5.5.4 Archive backup procedures

The TSP SHALL establish backup procedures necessary to achieve the protection objectives listed in section 5.5.3 over the periods of time listed in section 5.5.2.

5.5.5 Requirements for time-stamping of records

All significant certificate lifecycle events listed in section 5.5.1 SHALL be archived with date and time information.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

The archived data listed in section 5.5.1 as well as the records of the activities listed in section 5.4.1.1 SHALL be reviewed and, if necessary, handed over as evidence in case of need (e.g. in case of problem reports or in legal proceedings) and SHALL be made available to internal and external auditors upon request

5.6 Key changeover

Prior to the expiration of a CA certificate, the TSP SHALL, if they wish to continue their services, apply for a new CA certificate in good time in accordance with the current versions of this CP and the CPS of the TSP. In doing so, the TSP SHOULD choose a sufficiently long period between the publication of the new CA certificate and the taking out of service of the expiring CA certificate so that there is no interruption in service for the end subscribers.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The TSP SHALL describe the procedures for notification and handling incidents and compromises and for recovery from outages or disasters in their 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 TSP data needed to resume CA operations after a disaster at secure, preferably remotely located sites,
  - distance from the primary site to sites that can be used to restore 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 competent authorities or other relevant stakeholders,
  - security breaches that adversely affect natural or legal persons to the affected persons (without delay),
  - privacy incidents to the competent authorities or other relevant stakeholders (within 24 hours),
- decision-making options for dealing with vulnerabilities found (mitigation or justified acceptance),
- critical vulnerability remediation targets (within 48 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,
- planning documents for securing the operations site during a disaster and recovery at that site or at another site.
- 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 TSP SHALL disclose emergency documentation to auditors upon request.

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

The TSP SHALL establish procedures for notifying incidents and ensure that they are known and used by employees.

[SSL] [SMIME] The TSP SHALL immediately report violations of the Mozilla Root Store Policy to Mozilla in the form of an incident report ("Bugzilla") and SHOULD stop issuing the affected certificate types until the cause of the violation is resolved.

The TSP SHALL respond in a timely manner to incidents reported by individuals and alarms reported by systems (see section 6.6.2) to minimize potential damage. Potentially security-critical incidents SHALL be investigated immediately by personnel in trusted roles

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

See section 5.7.1.

5.7.3 Entity private key compromise procedures

The TSP SHALL define compromise, suspected compromise, and loss of a CA private key as an emergency in their emergency documentation and describe the resulting activities.

In the event of a CA key compromise, the TSP SHALL revoke (have revoked) the CA certificate and inform all affected parties (end entities as well as all others with whom the TSP has agreements). In addition, the TSP SHALL make the information available to relying third parties and indicate that the certificates and status information issued by the affected CA can no longer be trusted.

[QCP] The TSP SHALL describe in the CPS how the status information on end entity certificates is provided in case of compromise of a CA key.

[3145] In the event of a suspected compromise of a CA key, the TSP SHALL NOT use the affected key until final clarification.

5.7.4 Business continuity capabilities after a disaster

See section 5.7.1.

5.8 CA or RA termination

The TSP SHALL describe in the CPS the precautions taken to terminate services, at a minimum these include

- the information to be provided to all affected parties,
- the handling of status information of unexpired certificates, and,
- if possible, the delegation of duties to others.

[QCP] The TSP SHALL describe in the CPS how status information will be provided after the TSP's services are terminated.

The TSP SHALL maintain a current termination plan.

Potential disruption to end entities and relying parties SHALL be minimized in case of terminating the services of the TSP, in particular, the revocation and status services SHALL be continued (by other entities).

[3145] Instead of continuation of services by another entity, the TSP MAY terminate operation of all services, provided secure termination of all services can be guaranteed.

Before terminating a service, the TSP SHALL

- inform all affected parties (end entities, responsible supervisory authorities, if applicable, TSPs to which cross-certificates have been issued, as well as other affected parties with whom the TSP has contracts,
- provide relaying parties with the information about the termination,
- terminate the agreements with external RAs,
- require a reliable entity to retain all information necessary to demonstrate operation of the TSP for a reasonable period of time, as agreed upon with end entities and others, if applicable. This shall include, at a minimum:
    - Registration information,
    - certificate status information,
    - event log archives,
- destroy the private CA keys or take them out of service in such a way that they cannot be reused,
- revoke the CA certificates,
- if applicable, revoke any cross certificates.

TSPs SHALL either continue to provide their CA certificate themselves for a reasonable period of time after termination or engage another entity to do so.

In addition, when a service is terminated, the TSP SHOULD make arrangements, if possible, to transfer the provision of services to its existing customers to another TSP.

[3145] The TSP SHALL delete all keys, certificates and customer data.

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 technical and organizational requirements for generating the various keys are listed below.

6.1.1.1 Root CA key pair generation

Root CA key pairs SHALL be generated in a crypto module according to section 6.2.1 in the secure environment of the Trust Center.

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 NOT occur prior to application by a Trust Center Root Program staff member and approval by the Trust Center management or a representative, and SHALL be performed by at least two trusted Root TSP staff members different from the above. The following requirements apply:

- Each of the two employees SHALL have knowledge only of a part of the activation data required for key generation and SHALL NOT have knowledge of the complete activation data.
- The two employees SHALL act in different roles.

Both an internal and a qualified external auditor (see section 8.2) SHALL monitor the key ceremony and confirm its correct performance in the protocol.

In addition, the external auditor (see section 8.2) SHALL confirm in his report the compliance with all requirements as well as the preservation of the integrity and confidentiality of the keys.

6.1.1.2 Sub CA key pair generation

Sub CA key pairs SHALL be generated in a crypto module according to section 6.2.1 in the secure environment of the operator of the Sub CA that wants to use these keys.

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 trusted employees of the TSP. Each of the two employees SHALL have knowledge of only a part of the activation data required for key generation and SHALL NOT have knowledge of the complete activation data.

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

[TSEC-CA] The key ceremony SHALL be supervised by the product owner or a representative as well as an independent auditor. This SHALL be an experienced internal auditor of the Sub CA. If possible, a qualified external auditor (as defined in section 8.2) SHOULD be involved or the key ceremony should be video recorded for later review. The auditor's report SHALL confirm compliance with all requirements and the preservation of the integrity and confidentiality of the keys.

[DFN-CA] The key ceremony for keys for which Sub CA certificates of a Telekom Root CA are to be applied for SHALL be monitored by a qualified external auditor (according to section 8.2). The auditor's report SHALL confirm compliance with all requirements and the preservation of the integrity and confidentiality of the keys.

6.1.1.3 RA key pair generation

The TSP SHALL generate RA key pairs 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 subscriber keys are generated by the subscribers, the TSP must inform the subscribers about the permitted algorithms and key lengths to be used.

If subscriber keys are generated by the TSP, the TSP SHALL generate the keys in a secure manner and maintain them until certificate generation, ensuring integrity and confidentiality. The keys SHALL be considered suitable for the entire lifetime and intended uses at the time of generation.

[SSL] Subscriber keys that can be used to authenticate servers (i.e. if the certificates for these keys are to contain the extendedKeyUsage "id-kp-serverAuth" or "anyExtendedKeyUsage") SHALL NOT be generated by the TSP.

[QCP] Subscriber key pairs SHALL be generated by a QSCD.

[3145] TSP that generate subscriber keys for cryptographic token as a storage medium of the keys

- SHOULD have the keys generated by the token itself,
- SHALL delete keys generated outside the token immediately after they are stored in the token, unless the TSP provides a backup of the subscriber keys.

6.1.2 Private key delivery to subscriber

TSP that generate end entity keys SHALL take into account the following requirements:

- The keys SHALL be handed over to the end-user in such a way that the preservation of confidentiality and integrity is ensured and unauthorized use is impossible.
- After the keys have been handed over to the end user, all copies of the keys SHALL be deleted from the TSP's systems, unless the keys are to be deposited with the TSP on behalf of the end entity (see section 6.2.3).
- If the keys are handed over to the end entities by means of personalized secure cryptographic devices (e.g. smartcard), the handover of the devices and the associated activation data SHALL be done separately from each other.

[LCP] [NCP] TSPs that generate the keys of the end entities SHALL hand them over to the registered entity in a secure way, unless they manage the keys themselves on behalf of the end entity.

[NCP+] TSPs generating the keys of end entities SHALL ensure that they are provided on a secure cryptographic device (e.g., smart card) in a secure manner. The devices SHALL be delivered in a secure manner to the registered entity, unless the TSP manages the keys itself on behalf of the end entity. In the latter case, the TSP SHALL ensure that it has the keys under its sole control.

[QCP-n-qscd] [QCP-l-qscd] TSPs managing QSCD from end entities SHALL ensure that they can be used under the sole control of the end entity.

6.1.3 Public key delivery to certificate issuer

No stipulation.

[SSL] The TSP SHOULD specify in its CPS or in a document referenced in the CPS the format and methods of accepted electronic certificate requests.

6.1.4 CA public key delivery to relying parties

TSPs SHALL make their Root and Sub CA certificates generally available in an integrity and authenticity form. For Root CA certificates, additional validation mechanisms SHALL be provided, such as a check of the hash value of the certificate against a trusted source.

6.1.5 Key sizes

The TSP SHALL generate keys according to the requirements listed below and SHALL NOT accept keys generated by Sub CAs or end entities that do not meet these requirements. If the key lengths used are no longer sufficient for the intended use due to new knowledge or requirements, the TSP SHALL inform their Sub CAs and / or end entities and relying parties and set a schedule to revoke the certificates and migrate to sufficiently long keys.

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

- RSA: The 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

[SSL] [SMIME] RSA keys SHALL have a minimum length of 2048 bits, and 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] The requirements from [TR2102-1] apply.

6.1.6 Public key parameters generation and quality checking

No stipulation.

[SSL] The following requirements for the keys SHALL be implemented by the TSPs for the keys they generate themselves or checked for the keys submitted to them:

- 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 number and has no factors smaller than 752.
- ECC: The TSP SHOULD validate the keys 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)

6.1.7.1 Root CA

The use of the private key of a Root CA SHALL be restricted to the purposes listed in the corresponding Root CA certificate in the keyUsage attribute (see section 7.1.2).

[SSL] The private keys corresponding to the Root CA certificates SHALL NOT be used to sign certificates except for signing

- the Root CA certificate itself,
- Sub CA and cross certificates,

- infrastructure certificates, e.g. for administrative roles or operating devices,
- OCSP signer certificates.

6.1.7.2 Sub CA

The use of the private key of a Sub CA SHALL be restricted to issuing certificates and/or signing status information. In doing so, the intended uses listed in the corresponding Sub CA certificate in the keyUsage attribute (see section 7.1.2) SHALL be taken into account.

[SSL] [SMIME] The use of the private key of a Sub CA for signing end entity certificates SHALL be restricted to the signing of certificates that correspond to the purposes listed in the corresponding Sub CA certificate in the extendedKeyUsage attribute (see section 7.1.2).

6.1.7.3 Subscriber

The use of an end entity's private key SHALL be restricted to the uses listed in the corresponding end entity certificate in the keyUsage and/or extendedKeyUsage attributes (see section 7.1.2).

The TSP SHALL list in the CPS as well as the terms of use the permitted usages.

[QCP-n-qcsd] If a TSP manages the QSCD of an end entity, the use of the private key SHALL be limited to the generation of electronic signatures.

[QCP-l-qcsd] If a TSP manages the QSCD of an end entity, the use of the private key SHALL be limited to the generation of electronic seals.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

To protect the private keys of all levels of the hierarchy, the TSP SHALL take sufficient security measures or, in the case of end entity keys, that the TSP does not manage, require sufficient security measures.

The requirements for generating the keys and, if necessary, for transferring the private keys generated by the TSP to the end entities are described in section 6.1. The following sections specify the requirements for the use, storage, backup, archiving, take out of service and, if necessary, destruction of the keys used in cryptographic modules (HSM, smartcards, other tokens).

End entity keys that are not used in cryptographic modules are not discussed further here. The measures and requirements for this SHALL be described by the TSP in their CPS and, if applicable, terms of use.

6.2.1 Cryptographic module standards and controls

The Root and Sub CA as well as RA keys SHALL be generated in cryptographic modules that are either evaluated to CC EAL 4 or higher, or to a comparable standard, or certified to FIPS 1402-2 Level 3.

The TSP SHALL ensure that the cryptographic modules are not tampered with during storage and transport.

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

All cryptographic modules SHALL be operated according to the specifications of the certification documentation or in a comparable configuration with the same security level.

[QCP-n-qscd] [QCP-l-qscd] The QSCD SHALL be certified. The TSP SHALL monitor the certification status of the QSCD until the expiration of the validity of the end entity certificates and take appropriate measures if the certification status changes before the expiration of the end entity certificates.

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

No stipulation.

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

6.2.3 Private key escrow

No stipulation.

6.2.4 Private key backup

The private keys of the Root and Sub CAs 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.

The backup as well as the restore, if applicable, 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). In addition, it SHALL be ensured that access to the backups requires at least two trusted employees of the TSP.

[3145] TSPs that backup keys on behalf of end entities SHALL

- store the end user keys encrypted,
- use individual secrets generated by the Sub CA itself to encrypt the end entity keys in each case,
- also encrypt the individual secrets used for encryption and securely store them separately from the end entity keys, ensuring their integrity and confidentiality,

- securely identify end entities in the event of a back-up request (along the lines of identification at the time of application, (see section 4.2.1),
- handover the backup to the end entity in the same way as the original keys (see section 6.1.2)

[VS-NfD] TSPs that backup keys on behalf of end entities,

- SHALL, in addition to the above guidance on [3145], have the recovery actions and policies approved by the security officer; and
- MAY NOT secure other than the encryption keys of the end subscribers.

6.2.5 Private key archival

No stipulation.

[SSL] Parties other than the TSP operating a Sub CA SHALL NOT archive the Sub CA's private keys without the TSP's permission. Likewise, parties other than the end entity itself SHALL NOT archive the end entity's private keys without the end entity's permission.

6.2.6 Private key transfer into or from a cryptographic module

If Root or Sub CA keys are stored outside a cryptographic module according to section 6.2.1, they SHALL be stored in such a way that a security level comparable to the storage inside a cryptographic module is ensured. The 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).

[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 above requirements.

6.2.7 Private key storage on cryptographic module

The private keys of the Root and Sub CAs SHALL be generated, stored and used in cryptographic modules according to sections 6.1.1, 6.2.1 and 6.2.2.

[NCP+] The private keys of end entities SHALL be stored and used in secure cryptographic modules.

[QCP-n-qscd] [QCP-l-qscd] The private keys of the end entities SHALL be generated, stored and used in certified QSCD according to section 6.2.1.

6.2.8 Method of activating private key

TSPs generating and handing over keys for end entities SHALL ensure that the activation by end entities is done in a secure manner. TSPs SHALL describe the required measures and requirements in their CPS and, if applicable, in the terms of use.

6.2.9 Method of deactivating private key

TSPs that generate keys for end entities and hand them over by means of cryptographic modules (e.g., smart cards) SHALL ensure that their deactivation and, if necessary, reactivation by the end entities is done in a secure manner. TSPs SHALL describe the required measures and requirements in their CPS and, if applicable, in the terms of use.

6.2.10 Method of destroying private key

The private keys of a Root or Sub CA SHALL be destroyed at the end of the life cycle of the corresponding Root or Sub CA certificate, i.e., upon expiration, revocation or taking out of service of the Sub CA certificate, or termination of service. The destruction of the keys SHALL be performed in a key ceremony and shall take into account all copies of the keys. 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 at the end of their life or due to a defect, all private keys stored in the module SHALL be destroyed. The destruction does not affect the copies of the private keys, if the keys are still to be used in other or new cryptographic modules.

[VS-NfD] In case a TSP is not able to provide sufficient evidence for the destruction of the private key of a Sub CA, the corresponding Sub CA certificate SHALL be revoked.

6.2.11 Cryptographic Module Rating

The TSP SHALL evaluate cryptographic modules for usability and compliance with all requirements prior to purchasing.

6.3 Other aspects of key pair management

6.3.1 Public key archival

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

The keys of all hierarchy levels SHALL only be used as long as they, together with the algorithms used for certificate signing, can be regarded as sufficiently secure in accordance with sections 6.1.5 and 6.1.6.

6.3.2.1 Root CA

No stipulations for the certificate validity period of the Root CAs.

The private key of a Root CA SHALL NOT be used after the end of the life cycle of the corresponding Root CA certificate, i.e. with the expiry of the validity period or the taking out of service of the certificate or the termination of the service.

To ensure uninterrupted operation, the Root TSP SHALL issue a follow-up certificate in due time before the expiration of a Root CA certificate or the end of the usability of the keys.

6.3.2.2 Sub CA

The validity period of a Sub CA certificate SHALL not exceed the validity period of the issuing Root CA certificate ("shell model").

[SMIME] The validity period of a Sub CA certificate SHOULD NOT be greater than 10 years and SHALL NOT be greater than 20 years.

The private key of a Sub CA SHALL NOT be used after the end of the life cycle of the corresponding Root CA certificate, i.e. with the expiry of the validity period or the taking out of service of the certificate or the termination of the service.

To ensure uninterrupted operation, the TSP SHALL issue a follow-up certificate in due time before the expiration of a Sub CA certificate or the end of the usability of the keys.

[3145] In addition, the use of the private key of a Sub CA SHALL be prevented, e.g. by deactivation, if this is

- only to be used at a defined point in time (e.g. taking a new Sub CA certificate into operation planned for the future),
- not to be used for a certain period of time due to a special use case.

6.3.2.3 Subscriber

The validity period of an end entity certificate SHALL not exceed the validity period of the issuing Sub CA certificate ("shell model").

[QCP] The chain model applies differently for qualified certificates, i.e. the end entity certificates MAY be valid longer than the validity end date of the issuing Sub CA certificate.

[SSL] End entity certificates SHOULD NOT be valid for more than 397 days and SHALL NOT be valid for more than 398 days.

[SMIME] End entity certificates SHALL NOT be valid for more than 27 months.

6.4 Activation data

6.4.1 Activation data generation and installation

TSPs that issue end entity certificates on cryptographic modules (e.g., smartcards) that are provided with individual activation data (e.g., PINs) SHALL generate and set the activation data in the cryptographic modules in a secure manner.

6.4.2 Activation data protection

The activation data generated by the TSP (see section 6.4.1) SHALL be protected from generation to handover to the end entity in such a way that their integrity and confidentiality are ensured.

6.4.3 Other aspects of activation data

The activation data generated by the TSP (see section 6.4.1) SHALL be given to the subscriber in such a way that it is time-shifted and via a different communication channel to the cryptographic module itself.

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.

The TSP SHALL protect the systems required for certificate management and status and directory services according to the potential for damage.

The TSP SHALL manage the accounts of the trusted roles (see section 5.2.1) required to operate the critical systems 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. The TSP SHALL manage these accounts in such a way that they are changed or deleted within a reasonable time.

The TSP SHALL implement multi-factor authentication for the accounts that can directly initiate the issue of certificates.

The systems SHALL technically support the required separation of trusted roles (see section 5.2.4).

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

[SMIME] The TSP SHALL implement multi-factor authentication for all accounts

- of internal and external RAs,
- through which technical controls are set to restrict pre-approved domains or email addresses.

[SSL] [SMIME] The TSP SHALL

- review the accounts of those authorized to access the system at least every three months and deactivate accounts that are no longer needed,
- implement multi-factor authentication on all systems that support multi-factor authentication,
- change the authentication keys and passwords of the privileged accounts of the CA systems when a person's authorization for administrative access to the systems changes or is revoked,
- for trusted roles, ensure that they log in to the systems with personal accounts for traceability,
- if technically possible, for trusted roles that log in to the systems using username and password, implement the measures listed below:
  - 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,
- require individuals in trusted roles to log out of their account or lock their workstation when they are no longer in the role,
- either configure workstations to automatically lock out after a specified period of user inactivity, or configure relevant applications to automatically log out of the account after a specified period of user inactivity,
- disable access to CA systems 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,
- ensure multi-factor authentication or multi-person authentication for administrative access to critical systems,
- ensure multi-factor authentication for all accounts of trusted roles on CA systems accessible from outside the secure environments,
- allow remote access to critical systems only 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.

The TSP SHALL use trusted systems that ensure the technical security and reliability of the processes supported by the systems.

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

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

The TSP SHALL use separate systems for the production environment and the test/development environment.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

TSPs SHALL perform security requirements analysis during the design and requirements specification phase of a system development project to ensure that system security is addressed from the very beginning.

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 of the TSP.

The TSP SHALL ensure 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 TSP SHALL monitor the systems for the following activities and implement appropriate alarming capabilities.:

- Security relevant system events, these include:
  - successful and unsuccessful attempts to access the certificate systems,
  - activities performed on the certificate and security systems,
  - starting and shutting down the logging functions,
- availability and use of the required services.

[SSL] [SMIME] In addition to the above events, 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, and
- entries and exits into and out of certificate management system operations rooms.

The TSP SHOULD consider the sensitivity of any information collected or analyzed when monitoring.

The TSP SHALL continuously monitor the configuration of the systems for changes that have not been made based on an authorized change, and alarm as appropriate.

[NCP] TSPs SHALL monitor system capacity needs and forecast future capacity needs to ensure adequate processing and storage capacity is available.

The TSP SHOULD test the backups 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.

6.6.3 Life cycle security controls

The TSP SHALL implement appropriate security controls for the management of all cryptographic keys and cryptographic devices throughout their lifecycle.

6.7 Network security controls

The TSP SHALL protect their internal networks and systems from unauthorized access and attacks, e.g., by firewalls. The TSP SHALL configure their network components (e.g. firewalls, routers) in such a way that all not required protocols and accesses are deactivated.

[SSL] [SMIME] The TSP SHALL implement intrusion detection (IDS) and intrusion prevention systems (IPS) that they have under their own control or have delegated to trusted third-party roles.

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

The TSP SHALL segment their systems into networks or zones based on a risk assessment considering the functional, logical, and physical (including location) relationship between trusted systems and services.

[VS-NfD] The TSP SHALL use [ISI LANA] as a guide in network separation.

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 operated offline or separate from all other networks. The TSP SHALL implement and configure security procedures that protect the systems and communications between systems within secure zones.

The TSP SHALL separate the networks for administration of the systems 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.

The TSP SHALL review the rules above 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 to the TSP's systems is required, the external network connections SHALL be redundant.

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

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

[SSL] [SMIME] The TSP SHALL perform or have performed the above-mentioned vulnerability tests´

- within one week upon request of the CA/Browser Forum,
- in case of significant changes to the infrastructure or applications, and
- at least every three months.

The TSP SHALL perform or have performed the above-mentioned penetration tests at least annually.

The TSP SHALL, within 96 hours of the discovery of a critical vulnerability

- remediate this vulnerability, or
- if remediation of the vulnerability is not possible within 96 hours, prepare a mitigation plan for the vulnerability, including prioritization based on the affected systems; or
- Document 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

[3145] The TSP SHALL perform or have performed the above-mentioned penetration tests on a regular basis within a period of time determined by the TSP

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 by the TSP.

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The following sections describe the requirements for the certificate profiles. In addition, the following requirements apply:

- Certificate profiles SHALL comply with RFC5280 and ITU-T X.509 recommendations (https://www.itu.int/rec/T-REC-X.509/) and be described in the TSP's CPS.
- Certificate serial numbers SHALL be generated using a cryptographically secure random number generator. They SHALL be greater than zero (positive integer) and SHALL NOT exceed a maximum length of 160 bits. Each serial number SHALL NOT be used more than once per issuer.
- Please refer to section 6.3.2 regarding the validity periods of the certificates.
- Pre-certificates according to RFC 6962 ("Certificate Transparency") are not considered valid certificates in the sense of RFC 5280.
- The certificate profiles shown apply to all certificates issued from the start of validity of this CP. Certificates already issued with profiles in accordance with older requirements retain their validity unless explicit reference is made to their invalidity (legacy).

[SSL] [SMIME] The serial numbers SHALL have at least 64 bit.

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 Root CA, Sub CA, end entity and OCSP Signer certificates[1]. Extensions that are not listed there SHALL NOT be used. 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.
- ***(nn)*** Reference to the description of the parameters or contents to be set following the table. References in the "Extension according to RFC5280" column mean that the listed specifications apply to all certificate types.

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

Table 6 - Certificate extensions

Extension according to RFC5280 (OID)	Root CA certifi-cate	Sub CA certificate	End entity certificate	OCSP-Signer
AuthorityKeyIdentifier (2.5.29.35)	O (01)	M (01)	M (01)	M (01)
SubjectKeyIdentifier (2.5.29.14)	M (02) (03)	M (02) (03)	S	S
KeyUsage c (2.5.29.15)	M (04)	M (04)	M, [SSL] O (05) (06)	M
CertificatePolicies (2.5.29.32)	SN	O, [SSL] [EVCP] M (07) (08)	M (07) (09) (10)	O (07)
subjectAltName (2.5.29.17)	O (11)	O (11)	O, [SSL] M (11) (12)	O (11)
BasicConstraints (2.5.29.19)	M (13) c	M (13) c	O (14) (c)	O (c)
NameConstraints c (2.5.29.30)	N	(M) (15)	N	N
ExtendedKeyUsage (2.5.29.37)	N	SN, [SSL] [SMIME] M (16) (17)	(M) (18) (19)	M (20)
cRLDistributionPoints (2.5.29.31)	(M) (21)	(M) (22)	(M) (23)	O[2]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	(M) (24)	(M) (24) (25)	M (26) (27)	O[2]
qcStatements (1.3.6.1.5.5.7.1.3)	N	N	N, [QCP] M (28)	N
IssuerAlternativeName (2.5.29.18)	SN	SN	O	SN
SubjectDirectoryAttributes (2.5.29.9)	SN	SN	O	N
No-Check (1.3.6.1.5.5.7.48.1.5)	N	N	N	(M)[2]
cabfOrganizationIdentifier (2.23.140.3.1)	N	N	N, [EVCP] (M) (29)	N

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

AuthorityKeyIdentifier

(01) The "keyIdentifier " according to RFC5280 #4.2.1.1 SHALL be set.

[SSL] The attributes "authorityCertIssuer" and "authorityCertSerialNumber" SHALL NOT be set.

SubjectKeyIdentifier

(02) The "keyIdentifier " according to RFC5280 #4.2.1.1 SHALL be set.

(03) In a Root or Sub CA certificate, the subjectKeyIdentifier SHALL match the AuthorityKeyIdentifier in the certificates issued by that CA.

[2] See section 7.3.

KeyUsage

(04) In a Root or Sub CA certificate, the bits for keyCertSign or cRLSign SHALL be set. The bit for digitalSignature SHALL be set if OCSP responses are also to be signed with this certificate, otherwise it SHOULD NOT be set.

(05) In end entity certificates, the bits for keyCertSign and cRLSign SHALL NOT be set. If the extension "ExtendedKeyUsage" is set, the bits of the KeyUsage SHALL be set consistently to the parameters of the ExtendedKeyUsage according to RFC5280, section 4.2.1.12.

(06) [LCP] [NCP] [NCP+] [QCP] In end entity certificates for natural or legal persons (not SSL server certificates) one of the following variants of the KeyUsage SHALL be set:

a) nonRepudiation
b) nonRepudiation and digitialSignature
c) digitialSignature
d) digitialSignature and [keyEncipherment oder keyAgreement]
e) keyEncipherment or keyAgreement
f) nonrepudiation and digitialSignature 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

(07) In principle, only OIDs SHOULD be used. If the sole use of OIDs is insufficient, the qualifiers "cPSuri" or "userNotice" MAY be set additionally. An OID SHALL NOT be set multiple times in the "certificatePolicies" extension.

(08) [SSL] [TSEC-CA] Sub CA certificates MAY contain an OID that confirms compliance with the baseline reuirements of the CA/Browser Forum. 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. The OID for "anyPolicy" (2.5.29.32.0) MAY be set.

(08) [SSL] [DFN-CA] Sub CA certificates SHALL contain at least one OID that confirms compliance with the baseline requirements of the CA/Browser Forum. 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. The OID for "anyPolicy" (2.5.29.32.0) SHALL NOT be set. The qualifier "cPSuri" with a reference (http URL) to this certificate policy MAY be set.

(08) [EVCP] [DFN-CA] Sub CA certificates SHALL contain at least one OID describing the implemented EV policy of the TSP. In addition, the reference to the CPS of the Root CA SHALL be included (OID 1.3.6.1.5.5.7.2.1 and an http URL). The OID for "anyPolicy" (2.5.29.32.0) MAY be set.

(09) [LCP] [NCP] [NCP+] [QCP] End entity certificates for natural or legal persons (not SSL server certificates) SHALL include at least one Certificate Policy OID that reflects the practices and procedures performed by the TSP. The OIDs reserved by ETSI MAY 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
- [QCP-w] 0.4.0.194112.1.4

(10) [SSL] End entity 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
- EV Code Signing 2.23.140.1.3
- Non-EV Code Signing 2.23.140.1.4.1

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

(10) [EVCP] In end entity certificates, the applicable EV policy OID of the TSP and the reference to the relevant CPS of the TSP (OID 1.3.6.1.5.5.7.2.1 and an http URL) SHALL be set.

subjectAltName

(11) The extension "subjectAltName" MAY be set in the certificates of all hierarchy levels. If this is set, all verifiable[3] content SHALL have been validated by the TSP.

(12) [SSL] In end user certificates, at least one entry SHALL be included in the "subjectAltName" extension. Permitted entries are FQDNs (as "dNSName") or IP addresses of servers (as "iPAddress"). Wildcard FQDNs MAY be entered. FQDNs SHALL NOT consist of metacharacters only and SHALL NOT contain the "underscore" ("_") character. Reserved IP addresses or internal names SHALL NOT be entered.

(12) [EVCP] FQDNs included in end entity certificates SHALL be owned or controlled by the end entity and associated with its service.

[3] Not verifiable are details like, e.g., the User Principal Name (UPN) for Microsoft Smartcard Logon

BasicConstraints

(13) In Root and Sub CA certificates the "cA" flag SHALL be set to "true". In Sub CA certificates a maximum path length MAY be indicated in "pathLenConstraints", in Root CA certificates this indication SHOULD NOT be made.

(14) In end entity certificates, the "cA" flag SHALL be set to "false". The "pathLenConstraints" field SHALL NOT be set.

NameConstraints

(15) [SSL] [SMIME] Name restrictions MAY be included in Sub CA certificates. They SHALL be included if the certificates are to be technically constrained. For further details, please refer to section 7.1.5.

extendedKeyUsage

(16) [SSL] The OID 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) SHALL be set in Sub CA certificates[4]. In addition, the OID 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) MAY be set. The OIDs 1.3.6.1.5.7.3.4 (id-kp-emailProtection), 1.3.6.1.5.7.3.3 (id-kp-codeSigning), 1.3.6.1.5.7.3.8 (id-kp-timeStamping), and 2. 5.29.37.0 (anyExtendedKeyUsage) SHALL NOT be included, other OIDs SHOULD NOT be included.

(17) [SMIME] The OID 1.3.6.1.5.5.7.3.4 (id-kp-emailProtection) SHALL be set in Sub CA certificates[4]. Other OIDs MAY be set, but the OIDs 2.5.29.37.0 (anyExtendedKeyUsage), 1.3.6.1.5.7.3. 3 (id-kp-codeSigning), 1.3.6.1.5.7.3.8 (id-kp-timeStamping) and 1.3.6.1.5.7.3.1 (id-kp-serverAuth) SHALL NOT be included.

Note: In Sub CA certificates below the public Telekom Security Root CAs, which are not used to issue TLS certificates, the OID 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) SHALL NOT be set.

(18) [SSL] In end entity certificates, the OID 1.3.6.1.5.7.3.1 (id-kp-serverAuth) or the OID 1.3.6.1.5.7.3.2 (id-kp-clientAuth) SHALL be set; both OIDs MAY also be entered. Further OIDs SHALL NOT be set.

(19) [SMIME] In end entity certificates, the OID 1.3.6.1.5.7.3.4 (id-kp-emailProtection) SHALL be set. In addition, other OIDs MAY be set, the OIDs 2.5.29.37.0 (anyExtendedKeyUsage), 1.3.6.1.5.7.3.3 (id-kp-codeSigning), 1.3.6.1.5.7.3.8 (id-kp-timeStamping) and 1.3.6.1.5.7.3.1 (id-kp-serverAuth) SHALL NOT be set.

(20) In OCSP signer certificates the OID 1.3.6.1.5.5.7.3.9 (id-kp-OCSPSigning) SHALL be set.

[4] This requirement applies to all Sub CA certificates issued after 01.01.2019 and does not apply to cross certificates.

cRLDistributionPoints

(21) In Root and Sub CA certificates the extension cRLDistributionPoints SHALL be set if no OCSP information is provided for these certificates, otherwise this extension MAY be set.

(22) [SSL] [SMIME] In Sub CA certificates the extension cRLDistributionPoints SHALL be set with at least one http URL in the field distributionPoints.

(23) [SSL] [SMIME] In end entity certificates, the cRLDistributionPoints extension SHALL be set with at least one http URL in the distributionPoints field.

(23) [3145] [LCP] [NCP] [NCP+] [QCP] In end entity certificates, the cRLDistributionPoints extension MAY be set. If set, it SHALL contain at least one http or ldap URL in the distributionPoints field.

authorityInfoAccess

(24) In Root and Sub CA certificates the extension authorityInfoAccess SHALL be set if no revocation lists are provided for these certificates, otherwise this extension MAY be set.

(25) [SSL] In Sub CA certificates, the http URL of the OCSP responder SHALL be included (accessMethod 1.3.6.1.5.7.48.1 (ocsp)). In addition, the http URL of the relevant Root CA certificate SHOULD also be included (accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers)).

(26) In end entity certificates, the authorityInfoAccess extension SHALL be set and SHALL contain at least the http URL of the OCSP responder (accessMethod 1.3.6.1.5.7.48.1 (ocsp)).

(27) [LCP] [NCP] [NCP+] [QCP] [SMIME] In end entity certificates, the authorityInfoAccess extension SHALL additionally contain the http URL of the relevant Sub CA certificate (accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers)).

(27) [SSL] In end entity certificates, the authorityInfoAccess extension SHOULD additionally contain the http URL of the relevant Sub CA certificate (accessMethod 1.3.6.1.5.7.48.2 (caIssuers)).

qcStatements

(28) [QCP] The following QC statements SHALL be set in end entity certificates:

- 0.4.0.1862.1.1 (QcCompliance, esi4-qcStatement-1)
- 0.4.0.1862.1.5 (QcPDS, esi4-qcStatement-5)
- 0.4.0.1862.1.6 (QcType (esi4-qcStatement-6)

The QC statement 0.4.0.1862.1.6 SHALL be set with one of the following values.

- 0.4.0.1862.1.6.1 qct-esign
- 0.4.0.1862.1.6.2 qct-eseal
- 0.4.0.1862.1.6.3 qct-web

In addition, the following QC statements MAY be set:

- 0.4.0.1862.1.2 (QcLimitValue, esi4-qcStatement-2)
- 0.4.0.1862.1.3 (QcRetentionPeriod, esi4-qcStatement-3)

The following QCStatement SHALL NOT be set:

- 0.4.0.1862.1.7 (QcCClegislation statement, esi4-qcStatement-7)

Regarding the syntax of the QC statements to be used, the specifications of ETSI EN 319 412-5 [ETS4125] SHALL be considered.

(28) [QCP-n-qscd] [QCP-l-qscd] In end entity certificates, the QC statement 0.4.0.1862.1.4 (id-etsi-qcs-QcSSCD, esi4-qcStatement-4) SHALL be set.

cabfOrganizationIdentifier

(29) [EVCP] In end entity certificates, the cabfOrganizationIdentifier attribute SHALL be set if the organizationIdentifier attribute is set in the subjectDN and SHALL contain a reference to a subject registration. Refer to [CABFEV] for the syntax.

7.1.3 Algorithm object identifiers

Root or Sub CA certificates that are based on an RSA keys SHALL use one of the following signature algorithms to sign the certificates they issue:

- sha256WithRSAEncryption, OID 1.2.840.113549.1.1.11,
  Hex-coded value of the AlgorithmIdentifier: 300d06092a864886f70d01010b0500
- sha384WithRSAEncryption, OID 1.2.840.113549.1.1.12,
  Hex-coded value of the AlgorithmIdentifier: 300d06092a864886f70d01010c0500
- sha512WithRSAEncryption, OID 1.2.840.113549.1.1.13,
  Hex-coded value of the AlgorithmIdentifier: 300d06092a864886f70d01010d0500
- RSASSA-PSS, OID 1.2.840.113549.1.1.10
  - MGF-1 with SHA-256, and a salt length of 32 bytes, Hex-coded value of the AlgorithmIdentifier:304106092a864886f70d01010a3034a00f300d0609608648016503040201050 0a11c301a06092a864886f70d010108300d060960864801650304020105 00a203020120
  - MGF-1 with SHA-384, and a salt length of 48 bytes, Hex-coded value of the AlgorithmIdentifier:304106092a864886f70d01010a3034a00f300d0609608648016

5030402020500a11c301a06092a864886f70d010108300d060960864801650304
02020500a203020130

- MGF-1 with SHA-512, and a salt length of 64 bytes, Hex-coded value of the AlgorithmIdentifier:304106092a864886f70d01010a3034a00f300d0609608648016
5030402030500a11c301a06092a864886f70d010108300d060960864801650304
02030500a203020140

Root or Sub CA certificates based on a P256 ECDSA key SHALL use the following signature algorithm to sign the certificates they issue:

- ecdsa-with-SHA256, OID 1.2.840.10045.4.3.2,
  Hex-coded value of the AlgorithmIdentifier: 300a06082a8648ce3d040302

Root or Sub CA certificates based on a P384 ECDSA key SHALL use the following signature algorithm to sign the certificates they issue:

- ecdsa-with-SHA384, OID 1.2.840.10045.4.3.3,
  Hex-coded value of the AlgorithmIdentifier: 300a06082a8648ce3d040303

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

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

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

The TSP SHALL list in the CPS the algorithms and parameters they use.

7.1.4 Name forms

General regulations:

- The name of the issuer in a certificate ("issuerDN") SHALL correspond to the "subjectDN" of the issuing certificate "byte-by-byte".
- Attributes SHALL NOT be set in Root and Sub CA certificates if they are not explicitly required, i.e. "default deny" applies in principle.
- In Root and Sub CA certificates, all attributes SHALL NOT be set more than once.
- In end entity certificates, the attributes commonName, orgnaizationIdentifier, organizationName and countryName SHALL NOT be set more than once.
- The subjectDN SHALL NOT include unverified subject information.
- The subjectDN SHALL be unique for each subject, but multiple certificates with the same subjectDN MAY be issued for a subject.
- Test certificates SHALL be clearly identified as such in the subjectDN.

The following table provides an overview of mandatory and optional certificate attributes for Root CA, Sub CA, end entity and OCSP signer certificates[5]. Attributes that are not listed there SHALL NOT be used. 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.
- ***(nn)*** Reference to the description of the contents to be set following the table. References in the "Subject-DN attribute" column mean that the listed specifications apply to all certificate types.

Table 7 - Name forms

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

The following is a list of the content to be used in the attributes, if there are any supplementary requirements for this beyond the standards.

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

commonName

(01) [SSL] In Root or Sub CA certificates, the commonName attribute 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.

(01) [SSL] [SMIME] In Root CA certificates the names SHALL NOT be reused, i.e. in subsequent certificates other names SHALL be assigned.

(02) [SSL] In end entity certificates, the commonName attribute MAY be set. If set, it SHALL contain exactly one IP address or FQDN that is also contained in the SubjectAltName. Internal names or reserved IP addresses SHALL NOT be set.

(02) [EVCP] In end entity certificates, the commonName attribute 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). Widcard certificates SHALL NOT be issued, with the exception of "onion" certificates[6].

serialNumber

(03) [LCP] [NCP] [NCP+] [QCP] In end entity certificates the attribute serialNumber SHALL be set if the attributes countryName, commonName as well as givenName and surname or pseudonym are not sufficient to ensure the uniqueness of the name.

(03) [EVCP] In end entity certificates, the serialNumber attribute SHALL be set as follows:

- Private organization: The serialNumber attribute SHALL contain the legally assigned number (incorporation number or similar number) of the subject. If no such number has been assigned, the date of incorporation in a common date format SHALL be placed in this field.
- Government entity: For government entities that do not have a registration number or incorporation date, the CA SHALL include an appropriate description in the serialNumber attribute to indicate that the subject is a government entity.
- Business entity: The registration number of the company SHALL be set in the serialNumber attribute. If no such number has been assigned, the date of incorporation SHALL be set in a common date format.
- Non-commercial entity: no stipulation.

There are no stipulations regarding the syntax of the serialNumber.

[6] See Appendix F of CABF EV Guidelines

givenName

(04) [SSL] In end entity certificates for natural persons the givenName attribute MAY be set, otherwise it SHALL NOT be set. If the givenName attribute is set, it SHALL contain the name of the subject together with the surname attribute, and the policy OID 2.23.140.1.2.3 SHALL be set.

(05) [LCP] [NCP] [NCP+] [QCP] In end entity certificates for natural persons either the attributes surname and givenName or the attribute pseudonym SHALL be set, in end entity certificates for legal persons these fields SHALL NOT be set.

surname

(06) [SSL] In end entity certificates for natural persons the surname attribute MAY be set, otherwise it SHALL NOT be set. If the surname attribute is set, it SHALL contain the name of the subject together with the givenName attribute, and the policy OID 2.23.140.1.2.3 SHALL be set.

(07) [LCP] [NCP] [NCP+] [QCP] In end entity certificates for natural persons either the attributes surname and givenName or the attribute pseudonym SHALL be set, in end entity certificates for legal persons these fields SHALL NOT be set.

pseudonym

(08) [LCP] [NCP] [NCP+] [QCP] In end entity certificates for natural persons the attribute pseudonym SHALL be set if the attributes surname and givenName are not set, otherwise the attribute pseudonym SHALL NOT be set.

streetAddress

(09) [SSL] [EVCP] In end entity certificates, the streetAddress attribute MAY be set if the surname and givenName or organizationName attributes are set, otherwise the streetAddress attribute SHALL NOT be set.

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

localityName

(10) [SSL] [EVCP] In end entity certificates, the localityName attribute SHALL be set if the surname and givenName or organizationName attributes are set and the stateOrProvinceName attribute is not set. It MAY be set if the stateOrProvinceName attribute and the surname and givenName or organizationName attributes are set. It SHALL NOT be set if the surname and givenName or organizationName attributes 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.

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

stateOrProvinceName

(11) [SSL] [EVCP] In end entity certificates, the stateOrProvinceName attribute SHALL be set if the surname and givenName or organizatioName attributes are set and the localityName attribute is not set. The attribute stateOrProvinceName MAY be set if the attributes localityName, surname and givenName or organizationName are set. It SHALL NOT be set if the attributes surname and givenName or organizationName are not set.

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

postalCode

(12) [SSL] [EVCP] In end entity certificates, the postalCode attribute MAY be set if the surname and givenName or organizatioName attributes are set. It SHALL NOT be set if the surname and givenName or organizatioName attributes are not set.

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

businessCategory

(13) [EVCP] In end entity certificates, the businessCategory attribute SHALL be set with the applicable one of the following values[7]:

- Private Organization,
- Government Entity,
- Business Entity or
- Non-Commercial Entity.

[7] See CABF EV Guidelines #8.5

organizationalUnitName

(14) [SSL] [EVCP] In end entity certificates, the attribute organizationalUnitName MAY be set if the attributes organizationName, givenName, surname, localityName and countryName are set.

(14) [EVCP] The organizationalUnitName attribute SHALL NOT contain only meta characters such as ".", "-", spaces or other indications that the value is not present, incomplete or not applicable.

organizationIdentifier

(15) [LCP] [NCP] [NCP+] [QCP] In Sub CA certificates the attribute 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[8],
- a hyphen ("-"),
- reference assigned according to the identified registration scheme.

[SSL] In Sub CA certificates, the organizationIdentifier attribute SHALL NOT be set.

(16) [EVCP] In end entity certificates for legal entities, the organizationIdentifier attribute MAY be set. If set, it SHALL include a reference to the registration of the legal entity as follows:

- three characters for the identifier of the registration scheme (VAT, NTR or PSD)
- two characters for the country code[8],
- a hyphen ("-"),
- reference assigned according to the identified registration scheme.

(17) [LCP] [NCP] [NCP+] [QCP-l] In end entity certificates for legal entities, the organizationIdentifier SHALL be set and SHALL include a reference to the registration of the legal entity 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 [8],
- a hyphen ("-"),
- reference assigned according to the identified registration scheme.

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

jurisdictionOfIncorporationLocalityName

(18) [EVCP] In end entity certificates, the jurisdictionOfIncorporationLocalityName attribute SHALL be set if the registration entity acts at the municipal level. If the registration authority acts on national or state level, the attribute jurisdictionOfIncorporationStateOrProvinceName SHALL NOT be set.

jurisdictionOfIncorporationStateOrProvinceName

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

jurisdictionOfIncorporationCountryName

(20) [EVCP] In end entity certificates the attribute jurisdictionOfIncorporationCountryName SHALL be set[8].

organizationName

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

(22) [SSL] In end entity certificates, the organizationName attribute MAY be set. If set, it must contain the validated name or trade name ("DBA") of the subject. This may be set in slightly modified form (e.g. common abbreviations or usages), provided that this is traceable.

(22) [EVCP] In end entity certificates, the organizationName attribute SHALL be set and SHALL contain the full legal name of the certificate owner. 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 or DBA MAY be included at the beginning of the field, if the full legal name is added thereafter.

(23) [LCP] [NCP] [NCP+] [QCP-l] In end entity certificates for legal entities, the organizationName attribute SHALL be set and it SHALL contain the full legal name of the subject.

countryName

(24) [SSL] [EVCP] In end entity certificates the attribute countryName SHALL be set if the attributes surname and givenName or organizationName are set, otherwise it MAY be set.

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

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

7.1.5 Name constraints

Name restrictions SHALL NOT be set in Root CA certificates and end entity certificates. Name restrictions MAY be set in Sub CA certificates.

[SSL] [SMIME] Name restrictions SHALL be set in Sub CA certificates if the Sub CA certificates are to be technically constrained. In this case, the extension extendedKeyUsage SHALL also be set with one of the values "id-kp-serverAuth" or "id-kp-emailProtection". If the extendedKeyUsage extension is set with the "id-kp-serverAuth" value, the nameConstraints extension SHALL contain constraints for dNSName, iPAddress, and/or DirectoryName. If the extension extendedKeyUsage is set with the value "id-kp- emailProtection", the extension nameConstraints must contain constraints for rfc822Name with at least one allowed name.

7.1.6 Certificate policy object identifier

See section 7.1.2.

7.1.7 Usage of Policy Constraints extension

No stipulation.

[LCP, NCP, NCP+, QCP] The Policy Constraints extension SHALL NOT be set in end entity certificates.

7.1.8 Policy qualifiers syntax and semantics

The policy qualifiers SHALL be set conforming to RFC 5280 with the contents defined in section 7.1.2.

7.1.9 Processing semantics for the critical Certificate Policies extension

The Certificate Policies extension 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 RFC 5280 and be signed either by the CA itself or by a CRL signer whose certificate has been issued by the CA.

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 revocation list extensions.

The ARLs issued by the Root CA SHALL contain the CRL entry extension reasonCode.

[QCP] 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 the "ExpiredCertsOnCRL" extension.

All extensions SHALL NOT be marked as critical.

7.3 OCSP Profile

All OCSP responses SHALL meet the requirements of RFC 6960 and 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 RFC 6960, one of the following options SHALL be chosen for the OCSP signer certificate:

- The TSP MAY specify that the OCSP signer can be trusted for the lifetime of the OCSP signer certificate. In this case, the id-pkix-ocsp-nocheck extension SHALL be set in the OCSP Signer certificate and contain the value NULL. The cRLDistributionPoints and authorityInfoAccess extensions SHOULD NOT be set in the OCSP Signer certificate in this case, 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.
- The TSP MAY specify a checking capability of the OCSP Signer certificate in the cRLDistributionPoints and/or authorityInfoAccess extensions.
- The TSP MAY specify that it does not define a method for checking the status of the OCSP signer, leaving it up to the verifier to decide whether and how to check the status of the OCSP signer certificate.

[SSL] If the OCSP responses are signed by a dedicated OCSP signer, the first of the above variants SHALL be selected for the OCSP signer certificate, i.e. the id-pkix-ocsp-nocheck extension SHALL be set in the OCSP signer certificate and contain the value NULL.

7.3.1 Version number(s)

OCSP in version 1 according to RFC 6960 SHALL be used.

7.3.2 OCSP extensions

No stipulation.

[QCP] The "ArchiveCutOff" extension is to be set in the response with the time of the validity start of the referenced CA certificate.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

No stipulation.

[SSL] [SMIME] Root and Sub CA certificates as well as cross certificates that are suitable to issue further Sub CA certificates SHALL either be technically restricted (see section 7.1.2 and 7.1.5) or publicly announced and fully verified in accordance with all requirements of this section.

8.1 Frequency or circumstances of assessment

8.1.1 Internal audits

No stipulation.

[SSL] TSPs SHALL monitor compliance with the requirements of this CP and the applicable CPS, as well as their quality of service, through appropriate internal audits during the period in which they issue end user certificates. These internal audits SHALL be conducted at least quarterly and SHALL include random sampling of at least three percent of the end entity certificates issued since the last internal audit.

For TSPs issuing technically constrained Sub CAs, the above-mentioned requirements apply analogously, i.e. they SHALL verify end entity certificates issued by all technically constrained Sub CAs in the same manner.

[EVCP] In deviation from the above-mentioned requirements on [SSL], the TSP SHALL perform internal audits on an ongoing basis.

8.1.2 External Audits

No stipulation.

[SSL] [SMIME] The TSP SHALL be audited in an continuous sequence of audit periods according to an audit scheme listed in section 8.4 and applicable to [SSL] or [SMIME] ("period-of-time audits"), whereby a period SHALL NOT exceed the duration of one year

TSPs that have not yet been audited in a period-of-time audit SHALL conduct a certificate readiness audit in accordance with the appropriate audit scheme at some point within 12 months prior to issuing public certificates ("point-in-time audit"). After issuance of the first public certificate, the TSP SHALL be fully audited in a period-of-time audit within 90 days. TSP that have already been audited in a period-of-time audit do not require a point-in-time audit prior to the issuance of certificates.

Note: "Point-in-time" audits MAY be used, for example, to demonstrate that non-conformances found in a previous audit have been corrected, but they SHALL NOT replace a period-of-time audit.

[EVCP] The above requirements for [SSL] [SMIME] apply analogously to [EVCP] using the audit schemes listed in section 8.4 and applicable to [EVCP]. In addition, for [EVCP], a point-in-time audit SHALL always be performed within 12 months prior to the first issuance of EV certificates, regardless of whether or not a period-of-time audit has already been performed.

[3145] The TSP SHALL be audited annually by an independent external ISO27001 auditor.

8.1.3 Audits of subcontractors and delegated third parties

No stipulation.

[SSL] Analogously to the internal audits according to section 8.1.1, the TSP SHALL audit certificates issued by delegated third parties or containing information audited by delegated third parties at least quarterly, unless the delegated third party is audited itself according to section 8.1.2. For this audit, the TSP SHALL use its own validation specialist

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

[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.

[SSL] [SMIME] External auditors performing audits in accordance with section 8.1.2 SHALL be qualified auditors who have the following qualifications and skills:

- they SHALL be independent of the audited item,
- they SHALL be able to perform audits that meet the criteria specified in appropriate test schemes according to section 8.4,
- they SHALL employ individuals competent in auditing PKI technologies, information security tools and techniques, information technologies and security auditing, and proficient in the third party attestation function,
- they SHALL be bound by law, government regulations, or rules of professional ethics; and
- they 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 auditors SHALL also be accredited according to ISO 17065 using the requirements defined in ETSI EN 319 403.

For auditing according to the Webtrust standards, the auditors shall also be licensed by WebTrust.

[QCP] The TSP SHALL be tested by Conformity Assessment Bodies meeting the requirements of ETSI EN 319 403.

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.

[SSL] [SMIME] The TSP SHALL be audited according to one of the following schemes:

- WebTrust Principles and Criteria for Certification Authorities from version 2.1 incl. WebTrust for CAs SSL Baseline with Network Security from version 2.3
- ETSI EN 319 411-1 from version 1.2.2 or ETSI 319 411-2 from version 2.2.2

[SSL] Applicable policies of the above-mentioned ETSI documents are
- LCP in connection with DVCP or OVCP or
- QCP-w.

[SMIME] Applicable policies of the above-mentioned ETSI documents are
- LCP,
- NCP,
- NCP+,
- QCP-l,
- QCP-l-qscd,
- QCP-n oder
- QCP-n-qscd.

[EVCP] The Root TSP and the TSP SHALL be audited according to one of the following schemes:

- WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL from version 1.6.2,
- ETSI EN 319 411-1 from version 1.2.2, when using QCP-w additionally ETSI 319 411-2 from version 2.2.2
  Applicable policies of the above-mentioned ETSI documents are
  - NCP in connection with EVCP or
  - QCP-w in connection with EVCP

[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 deadlines set by the internal or external auditors.

[SSL] [SMIME] Deficiencies that violate the [BR], [MSRP], [MOZRP], [GGLRP] or [APLRP] SHALL be reported to the affected root programs. Provided that faulty certificates are found defective, the revocation reasons and deadlines according to section 4.9.1 SHALL be taken into account.

8.6 Communication of results

No stipulation.

[SSL] [SMIME] The TSP SHALL publish the audit attestations of all technically unrestricted Root and Sub CAs issued by the external auditors in the "Common CA Database" (CCADB).

The TSP SHOULD publish these attestations within three months after the end of the audit. In case of a delay of more than three months, the TSP SHALL provide a letter of explanation signed by the external auditor.

When preparing the audit attestations, the external auditors SHALL take into account the requirements on form and content from section 5.1 of the CCADB policy ("Audit Statement Content", see https://www.ccadb.org/policy).

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.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

The TSP 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 TSP 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 TSP SHALL have a liability insurance policy with respect to its services and obligations under this CP as follows:

- a general liability insurance with coverage of at least $2 million; and
- 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,
  - an violation of third party proprietary rights (excluding copyright and trademark violations),
  - an violation of privacy; or
  - a violation of advertising.

This insurance SHALL be arranged with a company that has a rating of at least "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

The TSP SHALL adequately protect confidential business information according to its classification.

9.4 Privacy of personal information

9.4.1 Privacy plan

The TSP SHALL comply with the requirements of the German "Bundesdatenschutzgesetz" [BDSG] and SHALL NOT collect data that is not relevant or appropriate for the provision of the service.

The TSP SHALL describe in their privacy plans how they implement the provisions of the [BDSG] with regard to the data collected in the registration process. The TSP SHALL take appropriate technical and organizational measures to maintain integrity and confidentiality during transmission and storage to protect the personal data against unauthorized or unlawful processing as well as against accidental loss or destruction of, or damage to, such data.

9.4.2 Information treated as private

The TSP SHALL describe in their CPS the information to be treated as private.

9.4.3 Information not deemed private

TSP SHALL describe in their CPSs the information that is not deemed to be private.

9.4.4 Responsibility to protect private information

The TSP SHALL describe in its CPS the responsibility for protecting private information.

9.4.5 Notice and consent to use private information

The TSP SHALL describe in their CPS the methods for notifying individuals and obtaining consent for the use of private information.

9.4.6 Disclosure pursuant to judicial or administrative process

The TSP SHALL describe in their CPS the conditions for disclosing personal data in the context of judicial or administrative proceedings.

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 TSP SHALL be reliable and operate their services in a trustworthy and legal manner compliant with this CP and their CPS.

The TSP SHALL retain overall responsibility for compliance with this CP and their CPS even if they outsource activities to subcontractors or third parties. To this end, the TSP SHALL define the tasks of the third parties and the associated procedures, responsibilities and liability conditions, and contractually oblige them to implement all the required measures.

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

The services operated by the TSP 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 TSP's terms and conditions of service.

The services and products offered to end entities 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.

The TSP SHALL offer third parties the possibility to validate and test all offered certificate types, e.g. by publishing PKCS#12 certificates on their website.

Prior to entering into a contractual relationship with an end entity, the TSP SHALL inform the end entity about the terms of use for the use of the certificates according to section 9.6.3.

[SSL] The Root TSP SHALL be responsible for

- the services and warranties of the TSP,
- the TSP's compliance with these CP,
- all liabilities and indemnification obligations of the TSP under these requirements,

as if it were itself the TSP issuing the certificates.

For each certificate they issue, the TSP SHALL guarantee to both the end subscribers and the application software vendors with whom the Root TSP has an agreement to include the Root CA certificates in the Trusted Root Stores, as well as to all relying third parties, that

- the end subscriber has the right to use the domain names or IP addresses listed in the certificate (in the subjectDistinguishedName and/or subjectAltName)sofern anwendbar, der Vertreter des Endteilnehmers autorisiert war, das Zertifikat im Namen des Endteilnehmers zu beantragen,
- they were authorized by the end entities to issue the certificates,

- the accuracy of all content included in the certificate, with the exception of the information in the organizationalUnitName attribute, has been verified and the information in the organizationalUnitName attribute is not likely to be misleading,
- the applicant has been identified according to section 3.2,
- if the end entity is not affiliated with the TSP, they have entered into a legally valid and enforceable contract with the end entity that meets all relevant requirements,
- if the end entity is affiliated with the TSP, a representative of the entity has acknowledged the terms and conditions of use,
- they operate status services in accordance with section 4.10 at least until the expiration date of the certificates and make status information available to the public on a 24-hour basis
- they revoke a certificate if one of the reasons for revocation listed in the CPS applies,
- they comply with the requirements of this CP and their own CPS during the entire validity period of a certificate

The TSP SHALL describe the processes and measures required to comply with the aforementioned certificate guarantees in their CPS.

The TSP SHOULD have an appropriate communication channel to all end entities to inform them about changes if needed.

The TSP SHALL ensure that the agreements with end entities including the terms of use (see section 9.6.3) are legally enforceable. Acceptance of the agreement MAY be electronic, if legally enforceable. The TSP MAY accept a separate agreement for each certificate or also an agreement that applies to multiple certificates.

[EVCP] For each EV certificate issued, the TSP SHALL ensure that

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

[QCP] The TSP that manages the private keys of the end entities during the validity period of the corresponding certificates SHOULD describe this in their CPS. In addition, this information MAY also be listed in the certificate of the end entity.

9.6.2 RA representations and warranties

See section 5.3.7, 6.5.1 and 9.6.1.

9.6.3 Subscriber representations and warranties

The TSP SHALL define the terms of use for the end entity certificates towards the end entities and have the end entities confirm their acceptance before the certificates are issued. These terms of use SHALL take into account at least the following obligations of the end entity:

a) an obligation to provide accurate and complete information to the TSP,
b) an obligation to use the key pair only in accordance with any restrictions communicated to the end entity,
c) a prohibition on the unauthorized use of the private end entity keys,
d) an obligation to notify the TSP immediately if any of the following events occur during the validity period of a certificate:
   - a private key has been lost, stolen, or possibly compromised,
   - control over a private key has been lost, e.g., due to compromise of activation data (e.g., PIN code) or for other reasons,
   - incorrectness or necessary changes to the certificate contents are detected,
e) an obligation, following compromise of a private key, to immediately and permanently cease using that key, except for key decryption,
f) an obligation to revoke or have a certificate revoked without delay if there is a reason for revocation in accordance with section 4.9.1.2.
g) an obligation to immediately and permanently cease using the corresponding private key, with the exception of key decryption, after revocation of the end entity certificate,
h) an obligation to immediately and permanently cease using the private end entity key, with the exception of key decryption, once the compromise of the issuing Sub CA has become known,
i) in the event that an end subscriber generates its keys itself: An obligation to generate the keys using suitable algorithms and key lengths in accordance with section 6.1.5,
j) in the case where an end-user 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,
k) in the case where an end entity is a legal entity 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,

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

n) [SSL] an obligation to take all reasonable measures to ensure confidentiality and control over the private keys and activation data,
o) [SSL] an obligation to verify the content of the certificate for accuracy,
p) [SSL] an obligation to install the certificate only on servers that can be accessed under the names listed in the certificate attribute subjectAltName,
q) [SSL] an obligation to use the certificate only in accordance with all applicable laws and with the concluded agreement and the terms of use,
r) [SSL] 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,

s) [SSL] 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,

t) [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)
u) [3145] in the event that an end entity generates the keys itself:
- an obligation to generate and retain the keys in accordance with the specifications (cf. ss) and tt)),
- an obligation to protect the keys from unauthorized access and manipulation,
v) [3145] in the event that the TSP generates and hands over the keys of the end entity 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,
w) [3145] an obligation to verify the end entity certificate as well as the issuing Sub CA certificate,

x) [QCP-n-qscd] an obligation to generate electronic signatures only using a QSCD,
y) [QCP-n-qscd] an obligation to keep the key under its sole control,
z) [QCP-l-qscd] an obligation to keep the key under the control of the subject of the certificate,
aa) [QCP-n-qscd] an obligation to use the key only for generating electronic signatures,
bb) [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:

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

oo) [3145] the way in which the end entities can transmit the registration data,
pp) [3145] regulations on the acceptance of new versions of the terms of use by the end entities in accordance with the applicable laws,
qq) [3145] a definition of the various roles of the end entities (e.g., applicant, subject of the certificate), the various possible subjects of a certificate (e.g., natural persons, natural persons associated with a legal entity, legal entities), and other significant roles in the certificate management processes

rr) [3145] a time limit after which final participants must confirm that their registration data is still valid,
ss) [3145] further requirements for end entities depending on the required security level (e.g. virus protection, firewalls as well as regular 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] in the event that an end entity generates the keys itself: the requirements for the hardware and software used to generate the keys,
uu) [3145] in the event that the TSP generates the keys of the end entities: the process of handing over the keys,
vv) [3145] in the event that the TSP generates and hands over the keys of the end entities on tokens: the process of handing over the tokens,
ww) [3145] the process of publishing new Sub CA certificates,
xx) [3145] the requirements for certificate renewal with or without key change and for issuing a replacement certificate,
yy) [3145] information about the process of terminating a TSP or RA (see section 5.8),
zz) [3145] Information about the time limits for the execution of revocations and their effectiveness in the status services,
aaa) information about the periods of the regular updates of the status services.

In case the applicant is not the subject of the certificate and the subject of the certificate is a natural or legal person

1) the above-mentioned obligations c), d), e), f), g), h) j) and l) 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 end entity SHALL consist of two parts,
   a) the first part SHALL be signed by the applicant and SHALL cover the following aspects:
      i) i) consent to the obligations of the applicant,
      ii) ii) consent to the use of a secure cryptographic module, if required,
      iii) 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) iv) conditions for publication of the certificate at the request of the applicant with the consent of the subject of the certificate,
      v) v) confirmation of correctness of all data to be included in the certificate,
      vi) 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 take into account 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.

   Note: Both parts of the agreement MAY be signed together by one person, if the applicant is at the same time an official representative of the legal entity, which is also the subject of the certificate, or if the official representative of the applicant is also at the same time the subject of the certificate.

[3145] The terms of use SHALL be provided permanently to the end entities in an integer manner.

In the case of relevant changes, the Terms of Use SHALL be adjusted, given a new version number and/or date, and provided to end entities and relying parties in an appropriate manner. Acceptance of a new version by end entities SHALL be validated by the TSP.

9.6.4 Relying party representations and warranties

The TSP SHALL include the following recommendations for relying parties in the terms of use (see also section 9.6.3): Relying parties SHOULD

- check the validity of the certificates via the offered status services according to section 4.9.10 and 4.10,
- take into account 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

See section 9.6.

9.8 Limitations of liability

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

The TSP MAY limit their liability in accordance with applicable law. They SHALL describe their limitations of liability in their CPS as well as in the Terms of Use, see also section 9.6.3 para. ii).

[SSL] In the case that the TSP outsources tasks to a third party, they MAY contractually allocate liability with the third party internally according to the tasks, but they SHALL retain overall responsibility externally according to this CP and their CPS.

[EVCP] The TSP SHALL NOT limit its liability to end entities or relying parties for legally recognized and provable claims to a monetary amount of less than two thousand U.S. dollars per end entity or relying party per end entity certificate.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

No stipulation.

9.10.2 Termination

See section 5.8 and 9.2.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

The TSP SHALL communicate relevant changes to end entities and relying parties and, where applicable, assessment bodies and supervisory or other regulatory authorities, see section 1.5.4, 9.6.1 and 9.6.3.

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

The TSP SHALL establish and describe in their CPS and Terms of Service (see section 9.6.3 para. kk)) policies and procedures for resolving complaints and disputes received from end entities or relying parties regarding services provided.

9.14 Governing law

The TSP SHALL set German law as the applicable law in their CPS.

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.

[SSL] In the case of a conflict between [BR] and a law, a TSP MAY modify any conflicting requirement 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, the TSP SHALL include in section 9.16.3 of its CPS a detailed reference to the law requiring modification of those requirements under this section, as well as the specific modification of those requirements made by the TSP, and inform the CA/Browser Forum of the relevant passages of the modified section before issuing a certificate under the modified requirement (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 TSP's CPS, 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.