Deutsche Telekom Security GmbH
Trust Center Certificate Policy

Version: 02.00

Valid from: 02.03.2022

Status: RELEASE

Last Review: 28.02.2022

HISTORY

Table 1 - Change history

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

TABLE OF CONTENTS

History 2
Table of contents 3
List of tables 11
1 Introduction 12
1.1 Overview 12
1.2 Document name and identification 14
1.3 PKI participants 14
1.3.1 Certification Authorities (CA) 14
1.3.2 Registration Authorities (RA) 14
1.3.3 Subscribers 15
1.3.4 Relying parties 15
1.3.5 Other participants 15
1.4 Certificate usage 15
1.4.1 Appropriate certificate uses 15
1.4.2 Prohibited certificate uses 16
1.5 Policy administration 16
1.5.1 Organization administering the document 16
1.5.2 Contact person 16
1.5.3 Person determining CPS suitability for the policy 17
1.5.4 CPS approval procedures 17
1.6 Definitions and acronyms 17
2 Publication and repository responsibilities 18
2.1 Respositories 18
2.2 Publication of certification information 18
2.3 Time or frequency of publication 19
2.4 Access controls on repositories 19
3 Identification and Authentication 20
3.1 Naming 20
3.1.1 Types of names 20
3.1.2 Need for names to be meaningful 20
3.1.3 Anonymity or pseudonymity of subscribers 20
3.1.4 Rules for interpreting various name forms 20
3.1.5 Uniqueness of names 20
3.1.6 Recognition, authentication, and role of trademarks 20
3.2 Initial identity validation 21
3.2.1 Method to prove possession of private key 21

3.2.2 Authentication of organization identity 21
3.2.3 Authentication of individual identity 22
3.2.4 Non-verified subscriber information 23
3.2.5 Validation of authority 23
3.2.6 Criteria for interoperation 23
3.2.7 Validation of control over a domain or IP-address 23
3.2.8 Validation of control over an e-mail address 24
3.3 Identification and authentication for re-key requests 25
3.3.1 Identification and authentication for routine re-key 25
3.3.2 Identification and authentication for re-key after revocation 25
3.4 Identification and authentication for revocation request 25
4 Certificate Life-cycle operational requirements 26
4.1 Certificate Application 26
4.1.1 Who can submit a certificate application? 26
4.1.2 Enrollment process and responsibilities 26
4.2 Certificate application processing 28
4.2.1 Performing identification and authentication functions 28
4.2.2 Approval or rejection of certificate applications 30
4.2.3 Time to process certificate applications 30
4.3 Certificate issuance 30
4.3.1 CA actions during certificate issuance 30
4.3.2 Notification to subscriber by the CA of issuance of certificate 31
4.4 Certificate acceptance 32
4.4.1 Conduct constituting certificate acceptance 32
4.4.2 Publication of the certificate by the CA 32
4.4.3 Notification of certificate issuance by the CA to other entities 32
4.5 Key pair and certificate usage 32
4.5.1 Private key and certificate usage 32
4.5.2 Relying party public key and certificate usage 33
4.6 Certificate renewal 33
4.6.1 Circumstance for certificate renewal 33
4.6.2 Who may request renewal 33
4.6.3 Processing certificate renewal requests 33
4.6.4 Notification of new certificate issuance to subscriber 33
4.6.5 Conduct constituting acceptance of a renewal certificate 33
4.6.6 Publication of the renewal certificate by the CA 34
4.6.7 Notification of certificate issuance by the CA to other entities 34
4.7 Certificate re-key 34

4.7.1 Circumstance for certificate re-key 34
4.7.2 Who may request certification of a new public key 34
4.7.3 Processing certificate re-keying requests 34
4.7.4 Notification of new certificate issuance to subscriber 35
4.7.5 Conduct constituting acceptance of a re-keyed certificate 35
4.7.6 Publication of the re-keyed certificate by the CA 35
4.7.7 Notification of certificate issuance by the CA to other entities 35
4.8 Certificate modification 35
4.8.1 Circumstance for certificate modification 35
4.8.2 Who may request certificate modification 35
4.8.3 Processing certificate modification requests 35
4.8.4 Notification of new certificate issuance to subscriber 36
4.8.5 Conduct constituting acceptance of modified certificate 36
4.8.6 Publication of the modified certificate by the CA 36
4.8.7 Notification of certificate issuance by the CA to other entities 36
4.9 Certificate revocation and suspension 36
4.9.1 Circumstances for revocation 37
4.9.2 Who can request revocation 39
4.9.3 Procedure for revocation request 39
4.9.4 Revocation request grace period 40
4.9.5 Time within which CA must process the revocation request 40
4.9.6 Revocation checking requirement for relying parties 41
4.9.7 CRL issuance frequency 41
4.9.8 Maximum latency for CRLs 41
4.9.9 On-line revocation/status checking availability 41
4.9.10 On-line revocation checking requirements 41
4.9.11 Other forms of revocation advertisements available 41
4.9.12 Special requirements re key compromise 42
4.9.13 Circumstances for suspension 42
4.9.14 Who can request suspension 42
4.9.15 Procedure for suspension request 42
4.9.16 Limits on suspension period 42
4.10 Certificate status services 42
4.10.1 Operational characteristics 43
4.10.2 Service availability 44
4.10.3 Optional features 44
4.11 End of subscription 44
4.12 Key escrow and recovery 45

4.12.1 Key escrow and recovery policy and practices 45
4.12.2 Session key encapsulation and recovery policy and practices 45
5 Facility, Management an operational controls 46
5.1 Physical controls 47
5.1.1 Site location and construction 47
5.1.2 Physical access 47
5.1.3 Power and air conditioning 47
5.1.4 Water exposures 48
5.1.5 Fire prevention and protection 48
5.1.6 Media storage 48
5.1.7 Waste disposal 48
5.1.8 Off-site backup 48
5.2 Procedural controls 49
5.2.1 Trusted roles 49
5.2.2 Number of persons required per task 49
5.2.3 Identification and authentication for each role 49
5.2.4 Roles requiring separation of duties 50
5.3 Personnel controls 51
5.3.1 Qualifications, experience, and clearance requirements 51
5.3.2 Background check procedures 51
5.3.3 Training requirements 52
5.3.4 Retraining frequency and requirements 52
5.3.5 Job rotation frequency and sequence 52
5.3.6 Sanctions for unauthorized actions 52
5.3.7 Independent contractor requirements 52
5.3.8 Documentation supplied to personnel 53
5.4 Audit logging procedures 53
5.4.1 Types of events recorded 53
5.4.2 Frequency of processing log 54
5.4.3 Retention period for audit log 54
5.4.4 Protection of audit log 54
5.4.5 Audit log backup procedures 55
5.4.6 Audit collection system (internal vs. external) 55
5.4.7 Notification to event-causing subject 55
5.4.8 Vulnerability assessments 55
5.5 Records archival 55
5.5.1 Types of records archived 55
5.5.2 Retention period for archive 56

5.5.3 Protection of archive 56
5.5.4 Archive backup procedures 56
5.5.5 Requirements for time-stamping of records 56
5.5.6 Archive collection system (internal or external) 56
5.5.7 Procedures to obtain and verify archive information 57
5.6 Key changeover 57
5.7 Compromise and disaster recovery 57
5.7.1 Incident and compromise handling procedures 57
5.7.2 Computing resources, software, and/or data are corrupted 58
5.7.3 Entity private key compromise procedures 58
5.7.4 Business continuity capabilities after a disaster 59
5.8 CA or RA termination 59
6 Technical security controls 60
6.1 Key pair generation and installation 60
6.1.1 Key pair generation 60
6.1.2 Private key delivery to subscriber 62
6.1.3 Public key delivery to certificate issuer 62
6.1.4 CA public key delivery to relying parties 62
6.1.5 Key sizes 63
6.1.6 Public key parameters generation and quality checking 63
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 64
6.2 Private Key Protection and Cryptographic Module Engineering Controls 64
6.2.1 Cryptographic module standards and controls 64
6.2.2 Private key (n out of m) multi-person control 64
6.2.3 Private key escrow 65
6.2.4 Private key backup 65
6.2.5 Private key archival 65
6.2.6 Private key transfer into or from a cryptographic module 66
6.2.7 Private key storage on cryptographic module 66
6.2.8 Method of activating private key 66
6.2.9 Method of deactivating private key 66
6.2.10 Method of destroying private key 66
6.2.11 Cryptographic Module Rating 67
6.3 Other aspects of key pair management 67
6.3.1 Public key archival 67
6.3.2 Certificate operational periods and key pair usage periods 67
6.4 Activation data 68
6.4.1 Activation data generation and installation 68

6.4.2 Activation data protection 68
6.4.3 Other aspects of activation data 68
6.5 Computer security controls 68
6.5.1 Specific computer security technical requirements 68
6.5.2 Computer security rating 70
6.6 Life cycle technical controls 70
6.6.1 System development controls 70
6.6.2 Security management controls 70
6.6.3 Life cycle security controls 71
6.7 Network security controls 71
6.8 Time-stamping 73
7 CERTIFICATE, CRL, AND OCSP PROFILES 74
7.1 Certificate profiles 74
7.1.1 Version number(s) 74
7.1.2 Certificate extensions 74
7.1.3 Algorithm object identifiers 81
7.1.4 Name forms 82
7.1.5 Name constraints 88
7.1.6 Certificate policy object identifier 89
7.1.7 Usage of Policy Constraints extension 89
7.1.8 Policy qualifiers syntax and semantics 89
7.1.9 Processing semantics for the critical Certificate Policies extension 89
7.2 CRL profile 89
7.2.1 Version number(s) 89
7.2.2 CRL and CRL entry extensions 89
7.3 OCSP Profile 90
7.3.1 Version number(s) 90
7.3.2 OCSP extensions 90
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 91
8.1 Frequency or circumstances of assessment 91
8.1.1 Internal audits 91
8.1.2 External Audits 91
8.1.3 Audits of subcontractors and delegated third parties 92
8.2 Identity/qualifications of assessor 92
8.3 Assessor's relationship to assessed entity 93
8.4 Topics covered by assessment 93
8.5 Actions taken as a result of deficiency 94
8.6 Communication of results 94

9 OTHER BUSINESS AND LEGAL MATTERS 95
9.1 Fees 95
9.1.1 Certificate issuance or renewal fees 95
9.1.2 Certificate access fees 95
9.1.3 Revocation or status information access fees 95
9.1.4 Fees for other services 95
9.1.5 Refund policy 95
9.2 Financial responsibility 95
9.2.1 Insurance coverage 95
9.2.2 Other assets 96
9.2.3 Insurance or warranty coverage for end entities 96
9.3 Confidentiality of business information 96
9.3.1 Scope of confidential information 96
9.3.2 Information not within the scope of confidential information 96
9.3.3 Responsibility to protect confidential information 96
9.4 Privacy of personal information 97
9.4.1 Privacy plan 97
9.4.2 Information treated as private 97
9.4.3 Information not deemed private 97
9.4.4 Responsibility to protect private information 97
9.4.5 Notice and consent to use private information 97
9.4.6 Disclosure pursuant to judicial or administrative process 97
9.4.7 Other information disclosure circumstances 97
9.5 Intellectual property rights 98
9.6 Representations and warranties 98
9.6.1 CA representations and warranties 98
9.6.2 RA representations and warranties 100
9.6.3 Subscriber representations and warranties 100
9.6.4 Relying party representations and warranties 103
9.6.5 Representations and warranties of other participants 103
9.7 Disclaimers of warranties 104
9.8 Limitations of liability 104
9.9 Indemnities 104
9.10 Term and termination 104
9.10.1 Term 104
9.10.2 Termination 104
9.10.3 Effect of termination and survival 104
9.11 Individual notices and communications with participants 104

9.12 Amendments 105
9.12.1 Procedure for amendment 105
9.12.2 Notification mechanism and period 105
9.12.3 Circumstances under which OID must be changed 105
9.13 Dispute resolution provisions 105
9.14 Governing law 105
9.15 Compliance with applicable law 106
9.16 Miscellaneous provisions 106
9.16.1 Entire agreement 106
9.16.2 Assignment 106
9.16.3 Severability 106
9.16.4 Enforcement (attorneys' fees and waiver of rights) 106
9.16.5 Force Majeure 106
9.17 Other provisions 106
APPENDIX 107
Appendix A: Abbreviations 107
Appendix B: References 109
Appendix C: Definitions 111

LIST OF TABLES

Table 1 - Change history 2
Table 2 - Certificate extensions 75
Table 3 - Name forms 83
Table 4 - Abbreviations 107
Table 5 - References 109
Table 6 - Definitions 111

1 INTRODUCTION

1.1 Overview

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

As a TSP, Telekom Security operates various 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 Group.

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

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

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

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

Furthermore, this CP applies to all Trust Services of the DFN via which certificates are issued below the public Sub CAs of the DFN issued by Telekom Security.

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

- Requirements that are not specifically marked apply in general for all certificate types.
- Framed requirements that begin with the specification of one or more certificate types in square brackets apply only to the certificate types concerned. The following certificate types are distinguished in this document:
  - [TLS] 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 "CA/Browser Forum Baseline Requirements" [BR].
    Note: unless explicitly stated otherwise, the requirements of [TLS] also implicitly apply TLS certificates issued in accordance with [DVCP], [OVCP], [IVCP], [EVCP] or [QNCP-w] or [QEVCP-w].
  - [SMIME] identifies all S/MIME certificates for email security that are issued under the Telekom Security public Root CAs integrated in the Trusted Root Stores of Microsoft [MSRP], Mozilla [MOZRP], Google [GCRP] and Apple [APLRP].

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

- [3145] identifies all certificates issued by Telekom Security in accordance with the [TR3145] under the BSI Root CAs.
- [VS-NfD] identifies all certificates that are issued in accordance with [3145] and also meet the requirements for “VS-NfD” (“Verschlusssache, nur für den Dienstgebrauch”, classified information) in accordance with the extension of the [TR3145] for VS-NfD [TR3145NfD].
- [LCP] identifies all certificates issued according to the "Lightweight Certificate Policy" defined in ETSI EN 319 411-1 [ETS411-1].
  Note: Unless explicitly stated otherwise, the requirements of [LCP] also implicitly apply to [DVCP], [IVCP] and [OVCP].
- [NCP] or [NCP+] identify all certificates issued according to the "Normalized Certificate Policy" or the "Extended Normalized Certificate Policy" defined in [ETS411-1].
  Note: Unless explicitly stated otherwise, the requirements of [NCP] also implicitly apply to [NCP+], [QNCP-w] and [EVCP].
- [EVCP] identifies all certificates issued according to the "CA/Browser Forum Extended Validation Certificate Guidelines" [EVCG] and the "Extended Validation Certificate Policy" defined in [ETS411-1].
  Note: Unless explicitly stated otherwise, the requirements of [EVCP] implicitly apply to [QEVCP-w].
- [DVCP] identifies all certificates issued according to the "Domain Validation Certificate Policy" defined in [ETS411-1].
- [IVCP] identifies all certificates issued according to the "Individual Validation Certificate Policy" defined in [ETS411-1].
- [OVCP] identifies all certificates issued according to the "Organizational Validation Certificate Policy" defined in [ETS411-1].
- [QCP] identifies all 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.
  - [QNCP-w] qualified web server certificates based on [TLS] and [NCP].
  - [QEVCP-w] qualified web server certificates based on [EVCP].

Requirements that affect only one of the two TSPs in scope of this CP are identified analogously by a mark in square brackets:

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

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.

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

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

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

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

[TLS] [SMIME] Compliance with the requirements from the relevant Trusted Root Programs from Microsoft [MSRP], Mozilla [MOZRP], Google [GCRP], and Apple [APRP] SHALL be explicitly confirmed in the CPS.

1.2 Document name and identification

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

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

1.3 PKI participants

1.3.1 Certification Authorities (CA)

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

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

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

1.3.2 Registration Authorities (RA)

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

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

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

1.3.3 Subscribers

Subscribers within the scope of this CP MAY only be natural or legal persons.

Subjects of the subscriber certificates within the scope of this CP MAY be

- natural persons,
- natural persons identified in association with a legal person,
- legal persons, including organizational units[2], identified in association with a legal person,
- devices[3] operated by or on behalf of a natural or legal person.

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

[EVCP] Subscribers MAY only be the following legal entities: ▪ Private Organizations according to [EVCG#8.5.2] ▪ Government Entities according to [EVCG#8.5.3] ▪ Business Entities according to [EVCG#8.5.4] ▪ Non-Commercial Entities according to [EVCG#8.5.5]

1.3.4 Relying parties

No stipulation.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

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

[2] organizational units identified in association with a legal person are hereinafter subsumed under the term "legal persons", unless explicitly stated otherwise
[3] the term "devices" hereinafter also subsumes systems, functions and IT processes, unless explicitly stated otherwise

1.4.2 Prohibited certificate uses

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

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

1.5 Policy administration

1.5.1 Organization administering the document

This document is administered by:

Deutsche Telekom Security GmbH

Trust Center & ID Security

Untere Industriestraße 20

57250 Netphen

Germany

1.5.2 Contact person

The contact for this CP is the Trust Center's Root Team, which can be reached as follows:

Phone: +49 (0) 1805 268 204[4]

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

E-Mail: FMB_Trust_Center_Rootprogram@t-systems.com

[TLS] [SMIME] To report suspected compromise of a key, misuse, or other types of fraud or inappropriate behavior, well-defined processes SHALL be established. These SHALL be described/published on the TSP's public web pages as well as in the CPSs in section 1.5.2. Note: For accepted methods to evidence key compromise, see section 4.9.12.

[VS-NfD] Contacts are the Trust Center's Information Security Officer and his or her deputy, who can be reached as follows: **E-Mail:** FMB-ISMS-TrustCenter@telekom.de

[4] Costs incurred when calling from Germany: landline 0.14 €/min, mobile networks max. 0.42 €/min

1.5.3 Person determining CPS suitability for the policy

Responsible for determining the conformity of a CPS to this CP is the Trust Center's Root Team, for contacts see section 1.5.2.

1.5.4 CPS approval procedures

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

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

1.6 Definitions and acronyms

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

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

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Respositories

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

2.2 Publication of certification information

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

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

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

The relevant terms of use and CPSs SHALL be easily identifiable to the certificates. The CPSs as well as the Root, Cross and Sub CA certificates SHOULD be published in the above-mentioned PKI repository analogously to this CP, unless otherwise specified.

In addition, the subscriber certificates MAY be published with the subscriber's consent.

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

All issued certificates or alternatively all "pre-certificates" (see section 4.3.1), including at least all Sub CA certificates (Root CA optional) from its chain, SHALL be published in a sufficient number of "Certificate Transparency Logs" (CTLogs). For the number of CTLogs, see section 7.1.2 (39).

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

The CPSs SHALL be published on the TSP's official website.

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

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

For publishing the Sub CA certificates in the Trusted Lists (national TSL and EU-TSL) the conformity assessment reports (see section 8.6) SHALL be submitted to the German Federal Network Agency.

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

[3145] It SHALL be ensured that new Sub CA certificates or information about them are delivered to subscribers in an authentic form. Therefore, the fingerprints of the Sub CA certificates SHALL be published via a different channel than the Sub CA certificate.

[TLS] For each public Root CA certificate below which TLS server certificates are issued, test web pages SHALL be provided that are secured with corresponding TLS server certificates that chain up to the respective Root CA.

Web pages with one valid, one expired and one revoked certificate SHALL be provided.

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

2.3 Time or frequency of publication

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

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

New Sub CA certificates SHALL be published before they are put into service, but no later than 7 days after their issuance.

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

The timing or frequencies of the publications listed in section 2.2 SHALL be described in the CPSs.

2.4 Access controls on repositories

The directories SHALL be 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] The subscribers SHALL be able to decide for themselves whether their 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

3.1.1 Types of names

The subject names SHALL be included in all certificates at least in the subject attribute in the form of a distinguished name in accordance with [X500] ("Subject-DN"), see section 7.1.4.

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

3.1.2 Need for names to be meaningful

Certificates issued for testing purposes SHALL be clearly identified as such in the Subject-DN.

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

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

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

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

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

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

Evidence MAY be submitted in paper form or electronically.

The authenticity of the evidence provided SHALL be checked for alterations and forgeries to the extent possible.

Only evidence necessary for verification of identity SHALL be requested.

The information collected from the subscribers and its validation SHALL be described in the CPSs.

[TLS] [SMIME] All information provided by the subscriber to be included in the certificate SHALL be verified via an independent information source or alternative communication channel.

A reliable method of communication (definition see Appendix C) SHALL be used to verify the authenticity of the certificate request.

3.2.1 Method to prove possession of private key

For key pairs not generated by the TSP, the certificate request verification process SHALL cover ownership or control of the private key.

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

3.2.2 Authentication of organization identity

The data of an organization to be included in a certificate MAY be validated through the following sources, for example:

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

[OVCP] The identity, address, company name, or brand name of an organization to be included in a certificate SHALL be validated through the sources listed above.

Prior to using a data source as a reliable data source, the source SHALL be evaluated for reliability, accuracy, and resistance to alteration or forgery, and the following SHALL be considered:

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

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

[NCP] Evidence of the identity of the legal person as subscriber, as well as the attributes to be verified, SHALL be verified against a duly authorized representative either directly by the physical presence of a person or indirectly by means that provide security equivalent to physical presence.

[EVCP] To uniquely identify the authorized sources used to validate identities, sufficient information, such as name, jurisdiction, and website, SHALL be published online in an appropriate and easy-to-access manner, and it SHALL be described in the CPSs in Section 3.2 where this information is published. In addition, the approved values to the fields listed below SHALL be published based on the 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)

3.2.3 Authentication of individual identity

No stipulation.

[NCP] Evidence of the identity of a natural person as subscriber (also in association with a legal person) 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.

[IV] [SMIME] At a minimum, a legible copy of a valid, government-issued photo ID that recognizably shows the face of the applicant SHALL be used for name verification.

For address verification, a form of identification that the TSP deems trustworthy SHALL be relied upon. Official photo identification used for name verification or utility bills or bank or credit card statements MAY be used.

[VS-NfD] The identity of the applicant SHALL be verified by means of an official identification document.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

For applicants who are not the subscriber, the full name and authorization of the applicant to act on behalf of the subscriber SHALL be verified as follows:

- For applicants representing a natural person not associated with a legal person, an authorization of the natural person to apply for certificates on its behalf SHALL be provided.
- For applicants representing a legal person or a natural person associated with a legal person, an authorization of the legal person to apply for certificates on its behalf or on behalf of its employees SHALL be provided.
- For applicants, that are legal entities representing another subscriber, this legal entity SHALL in turn be represented by an authorized natural person and his authorization to represent SHALL be verified.

[OVCP] The authenticity of certificate requests SHALL be verified using a reliable communication method, which MAY be based on the above sources.

The authenticity of a certificate request SHALL be confirmed either directly by the organization's representative or also by entities within the organization that are considered to be authoritative by the TSP, such as headquarters, branch offices, human resources offices, or IT departments.

In addition, organizations SHALL be provided the opportunity to nominate authorized individuals to apply for certificates. If an organization has nominated authorized individuals in writing, certificate applications SHALL NOT be accepted from individuals other than the nominated individuals. Upon a written request from an organization, a list of the organization's designated authorized individuals SHALL be provided.

3.2.6 Criteria for interoperation

No stipulation.

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

3.2.7 Validation of control over a domain or IP-address

No stipulation.

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

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

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

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

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

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

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

The methods used SHALL be listed in the CPSs including a reference to the relevant section of the [BR].

3.2.8 Validation of control over an e-mail address

No stipulation.

[SMIME] Appropriate and secure methods SHALL be used to verify the applicant's control over the email address referenced in the certificate or the applicant's authorization to act on behalf of the actual owner of the email address.

After a successful validation of the Authorization Domain Name (ADN, according to [BR]) of the domain portion of email addresses of an organization, the validation of sub-domains of this ADN MAY be waived when validating further email addresses of this organization.

The verification methods used SHALL be described in the CPSs.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The existence and validity of the certificate to be renewed and the validity of the information verifying the identity and attributes of the subject SHALL be checked prior to routine certificate renewals 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.

[TLS] Verification of information used for certificate renewal SHALL NOT be older than 398 days, otherwise the information SHALL be checked for validity and accuracy.

[EVCP] To ensure that the certificate request is authorized and the information is still accurate and valid, all authentication and verification tasks SHALL be performed according to [EVCG].

If an applicant already has a valid EV certificate from the TSP at the time of application, prior authentication and verification MAY be relied upon in accordance with [EVCG#11.14.1].

For the issuance of replacement certificates, already verified certificate requests MAY be reused, 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 information in the Subject-DN and the subjectAltName remain identical.

3.3.2 Identification and authentication for re-key after revocation

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

3.4 Identification and authentication for revocation request

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

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The requirements listed below SHALL be implemented for all certificates, including certificates issued by the TSPs for themselves or their employees.

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

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

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

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

[EVCP] The issuance of subscriber certificates SHALL be restricted to the following organizational forms (definitions see Annex C):

- Business entities
- Government entities
- Private organizations
- Non-commercial entities

4.1.2 Enrollment process and responsibilities

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

From applicants for subscriber certificates

- a physical address or other contact information and
- any attributes to be included in the certificate in the Subject-DN or subjectAltName extension

shall be requested.

If the applicant of a subscriber certificate 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 for a subscriber certificate 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. In this case, however, the requests SHALL be confirmed by a traceable action (e.g. checking a box or signing).

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

[TLS] For requesting a certificate, the subscribers SHALL be required to submit both a formal certificate request with the above information and an electronic certificate request (e.g. in PKCS#10 format) containing the public key and at least one of the requested names.

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

The following roles (definitions see Annex C) SHALL be implemented for the applicants:

- certificate requester
- certificate approver
- contract signer
- 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

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

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

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

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

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

4.2.1 Performing identification and authentication functions

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

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

- Full name of the person (last name, first name)
- Date and place of birth in accordance with national or other applicable birth registration conventions
- Reference to an official identification document or other attributes that can be used for unique identification

If the subject of a subscriber certificate 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 legal person
- Relevant registration information of the legal person according to national or other applicable identification procedures
- Affiliation of the natural person with the legal person
- Confirmation by the legal person and the natural person that the attributes of the subscriber also identify the organization

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

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

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

If the subject of a subscriber certificate is a device or system operated on behalf of a legal person or an organizational unit identified in connection with a legal person, then the identifier of the device or system (e.g., Internet domain name) SHALL additionally be verified.

[TLS] A validation performed MAY be used to issue multiple certificates, but the validation SHALL NOT have been performed more than 398 days prior to the certificate issuance.

If not all required information is included in a certificate request, the missing information SHALL be requested from the applicant or, upon receipt via another reliable means, be confirmed from the applicant.

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

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

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

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

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

The requirements in [BR#Appendix A] SHALL be considered and section 4.2 of the CPSs SHALL list the issuer domain names accepted by the TSPs.

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

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

[EVCP] If not all required information is included in a certificate application, the missing information SHALL be confirmed by the certificate approver or contract signer and not by the certificate requester (definitions see Appendix C).

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

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

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

4.2.2 Approval or rejection of certificate applications

Certificate requests MAY only be approved after successful identification and authentication in accordance with section 4.2.1.

If a key generated by the subscriber is submitted for an application that does not meet the requirements of sections 6.1.5 and 6.1.6, the application SHALL be rejected.

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

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

the application SHALL be rejected

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

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

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The integrity and authenticity SHALL be ensured when issuing the certificates and appropriate measures (technical, organizational or personnel) to protect against falsification of the data SHALL be taken 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.

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

[TLS] Subscriber certificates SHALL be published as "pre-certificates" in a sufficiently large number of CTLog servers (Certificate Transparency according to RFC 6962) before issuance. The time-stamped confirmations returned in this process SHALL be included in the “leaf certificates” as an extension with the OID 1.3.6.1.4.1.11129.2.4.2 („Embedded Signed Certificate Timestamps“ (SCT)). Regarding the number of CTLogs see section 7.1.2.

[3145] Before issuing certificates, it SHALL be checked that no certificates with the same attributes but different keys exist. In this case, no further certificate with these attributes SHOULD be generated.

If the use of cryptographic tokens is required

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

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

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

- the keys are delivered to the correct recipient,
- the confidentiality of the keys is guaranteed during delivery,
- keys are deleted in the systems of the TSPs after delivery to the correct recipient, unless the TSPs provide key backup for subscriber certificates.

The procedures for handing over the keys SHALL be described in the terms of use and the CPSs.

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

4.3.2 Notification to subscriber by the CA of issuance of certificate

If applicable, the issued subscriber certificates SHALL be provided to the subscribers, i.e., the applicant and/or the subject of the certificate, in usable form. In the case, that the TSPs manage the private keys on behalf of the subscribers, the subscribers shall be notified of the issuance.

Note: The subscriber certificates do not have to be provided in usable form immediately after issuance.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

Subscriber certificates SHALL be made available to subscribers.

Subscriber certificates MAY only be made available to certificate users after the consent of the subscriber. The processes of publication SHALL be described in the CPSs, see also section 2.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

[TLS] Root and Sub CA certificates SHALL be published in the CCADB, subscriber certificates in multiple CTLog servers, see also section 2.

4.5 Key pair and certificate usage

4.5.1 Private key and certificate usage

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

- Sub CA certificates,
- OCSP and, if applicable, CRL signer certificates and
- revocation lists.

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

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

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

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

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

4.5.2 Relying party public key and certificate usage

No stipulation.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

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

Certificates SHALL NOT be renewed if they have been revoked due to a security incident. Certificates SHALL NOT be renewed if any information in the certificates has changed.

[3145] The time periods and circumstances under which renewal is allowed SHALL be described in the CPSs as well as in the terms of use.

Revoked certificates SHALL NOT be renewed.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

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

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

[3145] The necessary processes in case the integrity of the original data is no longer given, SHALL be described in the CPSs.

4.6.4 Notification of new certificate issuance to subscriber

See section 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

See section 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

See section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

See section 4.4.3.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

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

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

[3145] The time periods and circumstances under which re-keying is allowed, SHALL be described in the CPS as well as in the terms of use. Re-keying SHALL NOT be allowed for revoked certificates.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

If the actual terms of use have been changed from the terms of use in effect at the time the preceeding certificate was applied for, the new terms of use SHALL be accepted by the subscriber before issuing a new certificate.

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

If information to be included in the new certificate has changed or the preceding certificate has been revoked, the registration information SHALL be verified, recorded and confirmed by the subscriber in the same way as for an initial application.

[EVCP] In a renewed subscriber certificate, the same expiration date and Subject-DN SHALL be set as in the preceding certificate

[3145] The processes required in the event that the integrity of the original data is no longer maintained, SHALL be described in the CPSs. The generation of new keys SHALL be enforced.

4.7.4 Notification of new certificate issuance to subscriber

See section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

See section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

See section 4.4.3.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

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

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

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

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

[3145] The time periods and circumstances under which modification of certificate data is permitted or required SHALL be described in the CPSs as well as in the terms of use.

4.8.2 Who may request certificate modification

See section 4.1.1.

4.8.3 Processing certificate modification requests

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

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

[3145] The processes required in the event that the integrity of the original data is no longer maintained, SHALL be described in the CPSs.

The generation of new keys SHALL be enforced.

4.8.4 Notification of new certificate issuance to subscriber

See section 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

See section 4.4.1.

4.8.6 Publication of the modified certificate by the CA

See section 4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

See section 4.4.3.

4.9 Certificate revocation and suspension

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

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

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

Regarding the interfaces to report problems, see section 1.5.2.

Note: The requirements listed below do not apply to "short-term certificates" if these are generally not revoked due to their very short validity. If such short-term certificates are issued, it SHALL be described in the CPSs which certificates are such short-term certificates and how they are handled.

4.9.1 Circumstances for revocation

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

4.9.1.1 Reasons for revoking a Sub CA certificate

A Sub CA certificate SHALL be revoked if

- a written revocation request, even without giving reasons, has been made by the operator of the Sub CA,
- 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 operation is not in compliance with this CP,
- it is determined that any information in the certificate is incorrect or misleading,
- the operation of the Root CA or the Sub CA will be terminated and no arrangements have been made for the continuation of the revocation service,
- the right of the operator of the Root CA or Sub CA to issue certificates in accordance with the requirements of this CP expires or is revoked or terminated and no arrangements have been made for the continued operation of the revocation services.

4.9.1.2 Reasons for revoking a subscriber certificate

Subscriber certificates must be revoked for various reasons. Since different revocation time lines are defined depending on the revocation reasons, the revocation reasons are listed below sorted by the time lines.

4.9.1.2.1 Short-term revocation within 24 hours

Subscriber certificates 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.

[TLS] In addition, subscriber certificates 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 or
- it is determined that that the subscriber's private key is a weak key that can be easily calculated based on the public key (e.g., "Debian weak key").

[S/MIME] In addition, subscriber certificates SHALL also be revoked if it is determined that the email address included in a certificate may no longer legally be used.

[QCP] In addition, subscriber certificates SHALL be revoked if it is determined that the private key of a certificate has been lost.

4.9.1.2.2 Medium-term revocation within five days

Subscriber certificates 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 or this CP (and thus also of the requirement sources referenced in section 1.1.),
- 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 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,
- it is determined that there have been significant changes on the information included in the certificate.

[TLS] In addition, subscriber certificates SHALL be revoked if

- the TSP's right to issue certificates has expired or has been revoked or terminated in accordance with the [BR] and no arrangements have been made for continuing the revocation services,
- it is determined that the use of an FQDN or IP address in a 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 period deviating from the time limits

Subscriber certificates 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.

[TLS] [SMIME] Subscriber certificates SHALL be revoked if sufficient reasons are provided by the relevant Trusted Root Programs listed in section 1.1. The time limits listed in section 4.9.1.2.1 and 4.9.1.2.2 generally apply. However, the TSPs SHALL also be able to revoke certificates in justified cases on a date specified by a Trusted Root Program that deviates from the time limits above.

[3145] In addition, subscriber certificates SHALL be revoked if

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

[QCP-n-qscd] [QCP-l-qscd] Subscriber certificates SHALL be revoked if the QSCD used (see section 6.2.1) loses its certification.

The reasons for revocation mentioned above usually require further checks or coordination, so that no time limits 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 operator of the Sub CA. If one of the revocation reasons listed in section 4.9.1.1 is identified by or reported to Telekom Security as operator of the Root CA, the revocation MAY also be initiated by Telekom Security without an existing revocation request. The further organizational and procedural requirements SHALL be described in [CPS_Root].

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

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

[3145] In addition, subscriber certificates SHALL be revoked if the subscriber is suspended.

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

4.9.3 Procedure for revocation request

For 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 not verified as a legitimate revocation reason.

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.

[TLS] [SMIME] After revocation of a Sub CA certificate, the corresponding entry in the CCADB SHALL be updated. If the revocation of the Sub CA certificate is required due to a security incident, the CCADB SHALL be updated within 24 hours, otherwise within 7 days.

[VS-NfD] The processes for revoking subscriber certificates including the specified time lines SHALL be apporved by the security officer.

4.9.4 Revocation request grace period

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

4.9.5 Time within which CA must process the revocation request

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

Sub CA certificates SHALL be revoked within seven days after receipt of an authorized revocation request. This period includes the time to handover the revocation status to the certificate status services.

Subscriber certificates SHALL be revoked as soon as possible, but no later than within 24 hours after receipt of an authorized revocation request. This period includes the time to handover the revocation status to the certificate status services. If a revocation request cannot be authorized within 24 hours, it does not have to be executed.

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

For revocations that are not based on authorized revocation requests, the time limits listed in section 4.9.1 apply.

[TLS] Within 24 hours of receipt of a problem report, the facts and circumstances SHALL be investigated and initial feedback on the findings available until then SHALL be provided to the subscriber and the reporting person. Subsequently, the results of the analysis SHALL be discussed with the subscriber and the reporting person and a decision SHALL be made as to whether a revocation is required. If revocation is required, 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 subscriber
- the entity that set the message
- the relevant legislation

4.9.6 Revocation checking requirement for relying parties

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

For short-term certificates identified by the extension "Validity Assured" (id-etsi-ext-valassured-ST-certs), relying parties MAY waive to check the status according to chap. 4.10.

4.9.7 CRL issuance frequency

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

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

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

4.9.8 Maximum latency for CRLs

No stipulation.

4.9.9 On-line revocation/status checking availability

See section 4.10.

4.9.10 On-line revocation checking requirements

If relying parties check the status of certificates via OCSP, they SHOULD use RFC6960-compliant OCSP client components, i.e. they SHOULD 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

No stipulation.

[TLS] [SMIME] Accepted methods for evidence of key compromise SHALL be described in the CPSs in section 4.9.12. Note: Regarding the reporting of suspected key compromise, see section 1.5.2.

4.9.13 Circumstances for suspension

If suspension is offered, the circumstances for suspension SHALL be specified in the CPSs.

[TLS] Subscriber certificates SHALL NOT be suspended.

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

4.9.14 Who can request suspension

If suspension is offered, the eligible applicants for suspension SHALL be defined in the CPSs.

4.9.15 Procedure for suspension request

If suspension is offered, the procedures for suspension SHALL be defined in the CPSs.

4.9.16 Limits on suspension period

If suspension is offered, the time periods and time limits for suspension SHALL be specified in the CPSs.

4.10 Certificate status services

Authentic and integer certificate status services in the form of revocation lists or OCSP information SHALL be provided at least over the validity period of all issued Sub CA and subscriber certificates.

OCSP information SHOULD be provided for the subscriber certificates.

[TLS] [SMIME] Revocation lists and OCSP information SHALL be provided for Sub CA and subscriber certificates

[QCP] Certificate status services SHALL be provided beyond certificate validity.

[QCP-n] [QCP-l] CRLs MAY be provided. If CRLs are provided, they SHALL be provided at least until all certificates in the scope of a CRL have expired or are revoked. The provisioning time beyond the certificate validity period SHALL be described in the CPSs and the integrity of the CRLs 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. Differing update timelines, if any, SHALL be listed in the CPSs and a description SHALL be provided of how differing verification results are to be interpreted.

4.10.1.1 Operational characteristics for the provision of the OCSP responder

The OCSP responders SHALL operate in conformance with 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 operates:

- 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 produce such an answer 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 is able to produce a valid OCSP response 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.

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

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

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

The OCSP responses created MAY be cached and reused within their validity for further requests.

[TLS] [SMIME] The following conditions apply to the reuse of valid OCSP responses:

- If OCSP responses have a validity of less than 16 hours, they SHALL NOT be reused after the 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 issuing and no longer than 8 hours before expiring.

OCSP requests for unassigned serial numbers SHOULD be logged.

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.

[TLS] [SMIME] CARLs SHALL NOT exceed a validity of 12 months. CRLs 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 CRLs after expiring, but they SHALL still be in the next regular CRL after their expiry date.

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

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.

[TLS] [SMIME] 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 maximum downtime of the systems SHALL be listed in the CPSs.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

If key escrow is offered,

- encryption keys MAY be deposited,
- authentication keys and signature keys SHALL NOT be stored in a form that allows decryption of these keys without control of the owner,
- it SHALL be ensured 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

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

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

[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

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

5.1.1 Site location and construction

Systems SHALL be operated in appropriate locations in secure premises with adequate physical protection 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 considered as guidance.

5.1.2 Physical access

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

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

The granted access authorizations SHALL be checked regularly.

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

5.1.7 Waste disposal

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

5.1.8 Off-site backup

No stipulation.

5.2 Procedural controls

5.2.1 Trusted roles

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

- Head of 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

[TLS] In addition to the roles listed above, the role of the Validation Specialist SHALL be established.

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

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 subscriber certificates SHALL be validated and released using the dual control principle. In order to ensure the dual control principle, auditable security controls SHALL be implemented.

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

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.

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

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

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

- the areas 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 structure that ensures impartiality of operation SHALL be documented.

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

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

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

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

5.2.4 Roles requiring separation of duties

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 roles above SHALL NOT also be applicants for subscriber certificates. Exceptions to this are

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

The exceptions SHALL be described in the CPSs.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The management of the TSP SHALL have

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

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

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

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

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

5.3.3 Training requirements

See section 5.3.1.

[TLS] All staff involved in validating certificate applications SHALL be trained on the following topics:

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

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

In addition, all validation specialists SHALL be required 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 staff SHOULD be trained regularly (at least annually) on current threats and security practices.

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

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Personnel SHALL be accountable for their actions. Appropriate sanctions SHALL be imposed 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.

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

[3145] Towards involved third parties, their responsibilities as well as the relevant practices SHALL be clearly defined, and appropriate arrangements SHALL be made to ensure that they 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, the role descriptions SHALL distinguish between general and specific roles.

5.4 Audit logging procedures

5.4.1 Types of events recorded

5.4.1.1 Activities of persons

The following activities of TSP staff, authenticated subscribers, and external RAs, with date, time, and identity of the person acting, SHALL be recorded:

- all activities related to registration and processing of requests for issuance, renewal and revocation of certificates of all hierarchical levels
- all activities related to the lifecycle of Root CAs, Sub CAs and, where applicable, subscriber keys and certificates. This includes, at a minimum, key generation, storage, backup, recovery, archiving and destruction, generation and, where applicable, revocation.
- all activities related to the lifecycle of the HSM

[TLS] In addition, the following activities SHALL be recorded:

- all validations according to the [BR] and the CPSs,
- commissioning of new certificate templates and decommissioning of no longer used ones

[NCP+] In addition, all events related to the preparation or provision of subscriber's token SHALL be recorded.

5.4.1.2 Technical system events

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

- all significant certificate and key management events
- generation of revocation lists and OCSP responses
- all security relevant events on the PKI and security systems, in particular changes to the systems' security policies, system startup and shutdown, system crashes and hardware failures, time synchronization events, firewall and router activities, and successful and unsuccessful PKI system access attempts
- installation, update and uninstallation of software on the PKI systems
- all (physical) entries and exits to/from the security zones

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

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 section 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 for a reasonable period of time, taking into account privacy requirements, both to ensure the continuity of the Trusted Services and, if applicable, due to legal requirements. The retention periods SHALL be described in the CPSs, see also section 5.5.2.

There is no specification regarding the retention period of the events listed in chap. 5.4.1.2, the retention periods SHOULD be described in the CPSs.

[TLS] The events listed in section 5.4.1.2 SHALL be retained for at least two years after their occurrence.

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. It SHALL be described in the CPSs how the protection of these records is ensured.

[TLS] [SMIME] The record retention SHALL be monitored (e.g., in internal audits).

[3145] The technical system events according to section 5.4.1.2 SHALL be stored 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

Safeguarding procedures necessary to achieve the protection objectives listed in section 5.4.4 over the retention periods listed in section 5.4.3 SHALL be established.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

[3145] 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 records SHALL be archived 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 following data SHALL be archived:

- 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 CPs or CPSs
- 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

[QCP] In addition, other information SHALL possibly be archived that has been issued and received by the TSP and may be needed as evidence in legal proceedings.

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

Taking into account the relevant privacy aspects, additional data MAY be archived. In the CPSs and terms of use SHALL be described which data are archived.

5.5.2 Retention period for archive

Data related to a certificate SHALL be archived for at least 7 years after the expiration of the certificate's validity. The retention period (if applicable per certificate type) SHALL be described in the CPSs as well as in the terms of use.

[TLS] It SHALL be verified that third parties contracted by the TSP, meet the requirements for document retention and event logging as specified in section 5.4.1.

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. It SHALL be described in the CPSs how the protection of the archived information is ensured.

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

5.5.4 Archive backup procedures

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 SHALL be established.

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

The ways of accessing archived information SHALL be defined and documented.

5.6 Key changeover

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

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

Emergency documentation SHALL include the following aspects:

- emergency prevention:
  - requirements to back up critical cryptographic material at another location
  - requirements to regularly back up all relevant data needed to 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 emergency documentation SHALL be disclosed to auditors upon request.

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

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

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

[TLS] [SMIME] Violations of the Mozilla Root Store Policy SHALL be immediately reported to Mozilla in the form of an incident report (in "Bugzilla"), issuing the affected certificate types SHOULD be stopped until the cause of the violation is resolved.

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

See section 5.7.1.

5.7.3 Entity private key compromise procedures

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

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

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

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

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

5.7.4 Business continuity capabilities after a disaster

See section 5.7.1.

5.8 CA or RA termination

Precautions taken to terminate services SHALL be described in the CPSs, at a minimum these include:

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

[QCP] The procedures for providing status information on subscriber certificates after termination of a Trusted Service SHALL be described in the CPSs.

An up-to-date termination plan SHALL be maintained.

Potential disruption to subscribers and relying parties SHALL be minimized in case of termination. In particular, the certificate status services SHALL be continued (by other entities).

[3145] Instead of continuation of a service by another entity, the service MAY be terminated, provided secure termination of the service can be guaranteed.

Before terminating a service

- all affected parties (subscribers, 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) SHALL be informed,
- relaying parties SHALL be provided with the information about the termination,
- agreements with external RAs SHALL be terminated,
- a reliable entity SHALL be engaged to retain all information necessary to demonstrate operation of the TSP for a reasonable period of time as agreed upon with subscribers and others, if applicable. This shall include, at a minimum:
    - Registration information
    - certificate status information
    - event log archives
- the private CA keys SHALL be destroyed or taken out of service in such a way that they cannot be reused,
- the CA certificates SHALL be revoked,
- if applicable, any cross certificates SHALL be revoked.

The CA certificate SHALL be provided either by the TSP for a reasonable period of time after termination or another entity SHALL be engaged to do so.

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

[3145] All keys, certificates and customer data SHALL be deleted.

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 Team staff member and approval by the Trust Center management or a representative. Generation SHALL be performed by at least two trusted Trust Center 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

The key ceremony SHALL be monitored by an internal and a qualified external auditor (see section 8.2). The correct performance SHALL be confirmed in their protocol.

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

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.

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] The key ceremony SHALL be supervised by 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] 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

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

6.1.1.4 Subscriber key pair generation

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

[TLS] Subscriber keys that can be used to authenticate servers, SHALL NOT be generated by the TSP.

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

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

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

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

6.1.2 Private key delivery to subscriber

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

- 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 escrowed with the TSP on behalf of the subscriber (see section 6.2.3).

[LCP] [NCP] If subscriber keys are generated by the TSP, the keys SHALL be handed over to the registered subscriber in a secure way, unless the TSP manages the keys on behalf of the subscriber.

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

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

[QCP-n-qscd] [QCP-l-qscd] If the TSP is managing the subscribers QSCD, it SHALL be ensured that they can be used only under the sole control of the subscriber.

6.1.3 Public key delivery to certificate issuer

No stipulation.

[TLS] The formats and methods of accepted electronic certificate requests SHOULD be specified in the CPSs or in documents referenced by the CPSs.

6.1.4 CA public key delivery to relying parties

Root and Sub CA certificates SHALL be provided with integrity and authenticity. 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

All keys SHALL be generated according to the requirements listed below. Keys submitted by subscribers that do not meet these requirements SHALL NOT be accepted.

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

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

[TLS] [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] SHALL be applied.

6.1.6 Public key parameters generation and quality checking

No stipulation.

[TLS] The following requirements for the keys SHALL be implemented for the keys generated by the TSP or SHALL be checked for the keys submitted from subscribers:

- 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 keys SHOULD be validated using either the ECC routine for full public key validation or the ECC routine for partial public key validation.

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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

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

Subscriber keys that are not used in cryptographic modules, are not discussed further here. The measures and requirements for this SHALL be described in the CPSs 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 140-2 Level 3.

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

[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 QSCDs SHALL be certified according to [eIDAS#Art.29-30]. The certification status of the QSCDs SHALL be monitored until the expiration of the validity of the subscriber certificates and appropriate measures SHALL be taken if the certification status changes before expiration of the subscriber certificates.

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

No stipulation.

[QCP-n-qscd] [QCP-l-qscd] The usage of private subscriber keys SHALL be in the sole control of the subscribers, regardless of whether they own the QSCDs themselves or have them managed by a TSP on their 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), the presence of an external auditor MAY be dispensed with. In addition, it SHALL be ensured that access to the backups requires at least two trusted employees of the TSP.

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

- the subscriber keys SHALL be stored encrypted,
- individual secrets generated by the Sub CA SHALL be used to encrypt the subscriber keys in each case,
- the individual secrets used for encryption SHALL also be encrypted and SHALL be securely stored separately from the subscriber keys, ensuring their integrity and confidentiality,
- the subscribers SHALL be securely identified in the event of a back-up request (along the lines of identification at the time of application, (see section 4.2.1),
- the backup SHALL be handed over to the subscriber in the same way as the original keys (see section 6.1.2)

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

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

6.2.5 Private key archival

No stipulation.

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

6.2.6 Private key transfer into or from a cryptographic module

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), the presence of an external auditor MAY be dispensed with.

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

6.2.7 Private key storage on cryptographic module

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 subscribers SHALL be stored and used in secure cryptographic modules.

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

6.2.8 Method of activating private key

If keys for subscribers are generated and handed over it SHALL be ensured that the activation by the subscribers is done in a secure manner. The required measures and requirements SHALL be described in the CPSs and, if applicable, in the terms of use.

6.2.9 Method of deactivating private key

If keys for subscribers are generated and handed over by means of cryptographic modules (e.g., smart cards), it SHALL be ensured that their deactivation and, if necessary, reactivation by the subscribers is done in a secure manner. The required measures and requirements SHALL be described in the CPSs 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 CA certificate, or termination of service. The destruction of the keys SHALL be performed in a key ceremony and all copies of the keys SHALL be considered. The same requirements apply here as for the generation of the keys, if applicable (see sections 6.1.1.1 resp. 6.1.1.2).

If cryptographic modules are taken out of service 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

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

6.3 Other aspects of key pair management

6.3.1 Public key archival

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.

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

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

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

[3145] The use of the private key of a Sub CA SHALL be disabled, e.g. by deactivation, if

- this is not to be used until a defined point in time (e.g., commissioning of a new Sub CA certificate planned for the future),
- this is not to be used for a certain period of time due to a special use case.

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

[SMIME] Subscriber certificates SHOULD NOT be valid for more than 825 days and SHALL NOT be valid for more than 1095 days.

6.4 Activation data

6.4.1 Activation data generation and installation

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

6.4.2 Activation data protection

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

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

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

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

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

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

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

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

[SMIME] Multi-factor authentication SHALL be implemented for all accounts

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

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

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

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

For trusted roles log in to the systems with personal accounts for traceability SAHLL be ensured.

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

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

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

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

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

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

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

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

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

The CA, certificate management, security and frontend systems and, if applicable, other internal systems supporting 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.

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

Separate systems SHALL be used 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

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

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.

It SHALL be ensured that

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

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

- 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
- configuration changes that were not made on the basis of an authorized change

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

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

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

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

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

6.6.3 Life cycle security controls

Appropriate security controls for the management of all cryptographic keys and cryptographic devices throughout their lifecycle SHALL be implemented.

6.7 Network security controls

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

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

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

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

[VS-NfD] [ISI LANA] SHALL be used 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 SHALL be operated offline or separate from all other networks. Security procedures that protect the systems and communications between systems within secure zones SHALL be implemented.

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

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

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

The rules above SHALL be reviewed on a regular basis.

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

If high availability of external access to the TSP's systems is required, the external network connections SHALL be redundant.

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

Penetration testing of the systems SHALL be performed when systems 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 execution of the penetration tests SHALL be documented, indicating the qualification of the person or organization performing the testing.

[TLS] [SMIME] The above-mentioned vulnerability scans SHALL be performed within one week upon request of the CA/Browser Forum and in case of significant changes to the infrastructure or applications.

Within 48 hours after the discovery of a critical vulnerability

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

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.

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profiles

Certificate profiles SHALL comply with RFC5280 and ITU-T X.509 recommendations and be described in the CPSs.

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

[TLS] [SMIME] The serial numbers SHALL be generated using a cryptographically secure random number generator and SHALL have at least 64 bit.

Pre-certificates according to RFC 6962 ("Certificate Transparency") are not considered valid certificates in the sense of RFC 5280.

[NCP] 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.

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[5]. 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.
- ***(#)*** Reference to the description of the parameters or contents to be set following the table.

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

Table 2 - Certificate extensions

Extension acc. to RFC5280 (OID)	Root CA	Sub CA	Subscriber	OCSP-Signer
AuthorityKeyIdentifier (2.5.29.35)	O	M (01)	M (01)	M (01)
SubjectKeyIdentifier (2.5.29.14)	M (02)	M (02)	S	S
KeyUsage (2.5.29.15)	M c (03)	M c (03)	M c [TLS] O (04)(05)	M c
CertificatePolicies (2.5.29.32)	O [TLS] SN (06)	O [TLS] M (06)(07)(08)(09)(10)	M (06)(11)(13)(14)	N
subjectAltName (2.5.29.17)	O (15)	O (15)	O [TLS] [SMIME] M (15)(16)(17)(18)	N
BasicConstraints (2.5.29.19)	M c (19)	M c (19)	O (c) (20)	O (c) (20)
NameConstraints (2.5.29.30)	N	O [TLS] [SMIME] (M) c (21)	N	N
ExtendedKeyUsage (2.5.29.37)	N	SN [TLS] [SMIME] M (22)(23)(24)(25)(26)	O [TLS] [SMIME] M (22)(26)(27)(28)	M (22)(29)
cRLDistributionPoints (2.5.29.31)	N	(M) [TLS] [SMIME] M (30)(31)	(M) [TLS] [SMIME] M (30)(32)(33)	O[6] [TLS] N
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	N	(M) [TLS] [SMIME] M (34)(35)	(M) [TLS] [SMIME] M (34)(36)	O[6] [TLS] SN
qcStatements (1.3.6.1.5.5.7.1.3)	N	N	N [QCP] M (37)(38)	N
validity model 1.3.6.1.4.1.8301.3.5	N	N [QCP] O	N [QCP] M	N
IssuerAlternativeName (2.5.29.18)	SN	SN	O	SN
SubjectDirectoryAttributes (2.5.29.9)	SN	SN	O	N
id-pkix-ocsp-nocheck (1.3.6.1.5.5.7.48.1.5)	N	N	N	(M)[6] [TLS] M
cabfOrganizationIdentifier (2.23.140.3.1)	N	N	N [EVCP] (M) (39)	N
signedCertificateTimestampList (1.3.6.1.4.1.11129.2.4.2)	N	N	N [TLS] M (40)	O
id-etsi-ext-valassured-ST-certs (0.4.0.194121.2.1)	N	N	(M) (41)	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.

[6] See section 7.3.

AuthorityKeyIdentifier

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

SubjectKeyIdentifier

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

KeyUsage

(03) 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 SHALL NOT be set. Other bits SHALL NOT be set.

(04) In subscriber certificates, the bits for keyCertSign and cRLSign SHALL NOT be set, other bits SHALL be set according to [RFC5280#4.2.1.3]. If the extension "ExtendedKeyUsage" is set, the bits of the KeyUsage SHALL be set consistently to the parameters of the ExtendedKeyUsage according to [RFC5280# 4.2.1.12].

(05) [LCP] [NCP] [NCP+] [QCP] In subscriber 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

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

(07) [TLS] [TSEC] 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) [TLS] [DFN] 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.

(09) [SMIME] In Sub CA certificates the OID for „anyPolicy“ (2.5.29.32.0) SHOULD NOT be set.

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

(11) [LCP] [NCP] [NCP+] [QCP] Subscriber 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

The OID for “anyPolicy” (2.5.29.32.0) SHALL NOT be set.

(12) [TLS] Subscriber certificates SHALL contain at least one of the following OIDs reserved by the CA/Browser Forum:

- [EVCP] 2.23.140.1.1
- [DVCP] 2.23.140.1.2.1
- [OVCP] 2.23.140.1.2.2
- [IVCP] 2.23.140.1.2.3

If the certificates are qualified website certificates, one of the following OIDs SHOULD also be included:

- [QEVCP-w] 0.4.0.194112.1.4 (formerly QCP-w)
- [QNCP-w] 0.4.0.194112.1.5

In addition, the TSP's own OIDs described in the TSP's relevant CPS and/or subsequent ETSI reserved OIDs MAY be used:

- [EVCP] 0.4.0.2042.1.4
- [DVCP] 0.4.0.2042.1.6
- [OVCP] 0.4.0.2042.1.7
- [IVCP] 0.4.0.2042.1.8

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

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

(14) [3145] In subscriber certificates, the qualifier "userNotice" SHALL NOT be set.

subjectAltName

(15) The extension "subjectAltName" MAY be set in the certificates of all hierarchy levels. If set, all verifiable[7] content SHALL have been validated by the TSP.

(16) [TLS] In Root and Sub CA certificates the extension “subjectAltName” SHALL NOT be set.
In subscriber 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") or Wildcard Domain Names. The FQDNs as well as the FQDN portions of Wildcard Domain Names SHALL consist exclusively of "P-Labels" or "Non-Reserved LDH-Labels". Reserved IP addresses or internal names SHALL NOT be included.

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

(18) [SMIME] In subscriber certificates, at least one rFC822Name-entry SHALL be included in the “subjectAltName”.

BasicConstraints

(19) 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.

(20) In subscriber an OCSP-Signer certificates, the "cA" flag SHALL be set to "false". The "pathLenConstraints" field SHALL NOT be set.

NameConstraints

(21) [TLS] [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.

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

extendedKeyUsage

(22) If the extendedKeyUsage is set, the bits of the KeyUsage SHALL be set consistently with the extendedKeyUsage parameters according to [RFC5280#4.2.1.12].

(23) [TLS] The OID 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) SHALL be set in Sub CA certificates[8]. 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.

(24) [SMIME] The OID 1.3.6.1.5.5.7.3.4 (id-kp-emailProtection) SHALL be set in Sub CA certificates[8]. 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.

(25) [TLS] [SMIME] 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.

(26) [TLS] [SMIME] The OIDs set in Sub CA and subscriber certificates SHALL correspond to each other, i.e. subscriber certificates SHALL NOT be issued by a Sub CA with OIDs that are not contained in the Sub CA certificate itself ("EKU chaining"). This does not apply to OCSP signer certificates, which MAY also be issued by Sub CAs that do not contain the OID 1.3.6.1.5.5.7.3.9 (id-kp-OCSPSigning).

(27) [TLS] In subscriber 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.

(28) [SMIME] In subscriber 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.

(29) In OCSP signer certificates the OID 1.3.6.1.5.5.7.3.9 (id-kp-OCSPSigning) SHALL be set. Other OIDs SHALL NOT be set.

cRLDistributionPoints

(30) In all certificates whose issuer offers revocation lists, the cRLDistributionPoints extension SHALL be set in the distributionPoints field with at least one http URL pointing to the TSP's revocation list.

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

(31) [TLS] [SMIME] In Sub CA certificates the extension cRLDistributionPoints SHALL be set with at least one http URL in the field distributionPoints pointing to the TSP's revocation list.

(32) [TLS] [SMIME] In subscriber certificates, the cRLDistributionPoints extension SHALL be set with at least one http URL in the distributionPoints field pointing to the TSP's revocation list.

(33) [3145] [LCP] [NCP] [NCP+] [QCP] In subscriber certificates, the cRLDistributionPoints extension SHALL be set if the issuing Sub CA offers revocation lists. If set, it SHALL contain at least one publicly accessible http or ldap URL in the distributionPoints field.

authorityInfoAccess

(34) In all certificates which are OCSP-verifiable, the extension authorityInfoAccess 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)).

(35) [TLS] In Sub CA and subscriber certificates, the extension “authorityInfoAccess” SHALL be set and SHALL contain the http URL of the OCSP responder (accessMethod 1.3.6.1.5.7.48.1 (ocsp)). In addition, the http URL of the relevant CA certificate SHOULD also be included (accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers)).

(36) [LCP] [NCP] [NCP+] [QCP] [SMIME] In subscriber certificates, the authorityInfoAccess extension SHALL be set and SHALL at least contain the http URL of the relevant Sub CA certificate (accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers)).

qcStatements

(37) [QCP] The following QC statements SHALL be set in subscriber 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 [ETS4125] SHALL be considered.

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

cabfOrganizationIdentifier

(39) [EVCP] In subscriber 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 [EVCG] for the syntax.

signedCertificateTimestampList

(40) [TLS] In subscriber certificates the following SCT SHALL be included:

- at least one SCT of any CT-Log-Server, with the status „qualified“, „usable“ or „readOnly“ at the time of verification,
- at least one SCT of a CT-Log-Server operated by Google, with the status „qualified“, „usable“, „readOnly“ oder „retired“ at the time of verification,
- at least one SCT of a CT-Log-Server, that is not operated by Google, with the status „qualified“, „usable“, „readOnly“ oder „retired“ at the time of verification.

id-etsi-ext-valassured-ST-certs

(41) In short-term subscriber certificates the extension “id-etsi-ext-valassured-ST-certs” SHALL be set as follows:

- in short-term certificates, that cannot be revoked, “id-etsi-ext-valassured-ST-certs” SHALL be set,
- in short-term certificates, that can be revoked, “id-etsi-ext-valassured-ST-certs” SHOULD NOT be set.
- In subscriber ceritficates, that are not short-term certificates, “id-etsi-ext-valassured-ST-certs” SHALL NOT be set.

7.1.3 Algorithm object identifiers

The algorithms used for signing the certificates of all hierarchy levels SHALL comply with the requirements from [SOGIS].

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:304106092a864886f70d01010a3034a00f300d0609608648016

5030402010500a11c301a06092a864886f70d010108300d060960864801650304
02010500a203020120

- 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 algorithms and parameters used SHALL be listed in the CPSs.

7.1.4 Name forms

General regulations:

- The name of the issuer in a certificate ("Issuer-DN") SHALL correspond to the "Subject-DN" 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 subscriber certificates, the attributes commonName, orgnaizationIdentifier, organizationName and countryName SHALL NOT be set more than once.
- In subscriber certificates issued to natural persons in association with legal persons, the certificate attributes identifying the organization SHALL reflect the legal persons and the subject in the certificates SHOULD be the natural persons.

The following table provides an overview of mandatory and optional certificate attributes for Root CA, Sub CA, end entity and OCSP signer certificates[9]. 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.
- ***(#)*** Reference to the description of the contents to be set following the table.

Table 3 - Name forms

Subject-DN attribute (OID)	Root CA	Sub CA	Subscriber	OCSP-Signer[10]
commonName (2.5.4.3)	M (01)	M (01)	M [TLS] O (02)	M
serialNumber (2.5.4.5)	N	N	(M) (03)	N
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)	N
localityName (2.5.4.7)	N	N	(M) (10)	N
stateOrProvinceName (2.5.4.8)	N	N	(M) (11)	N
postalCode (2.5.4.17)	N	N	(M) (12)	N
businessCategory (2.5.4.15)	N	N	(M) (13)	N
organizationalUnitName (2.5.4.11)	N	N	O (14)	N
organizationIdentifier (2.5.4.97)	N [QCP] O	(S) (15)	(M) (16) (17)	N
jurisdictionOfIncorporation-LocalityName (1.3.6.1.4.1.311.60.2.1.1)	N	N	(M) (18)	N
jurisdictionOfIncorporation-StateOrPr.Name (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 [TLS] (M) (24)	M
Other attributes	N	N	O [EVCP] N	N

[9] CRL Signer certificates are not listed due to CRLs being directly issued by the corresponding CA.
[10]The requirements listed here apply to all OCSP signers of the public root or sub-CAs, but in the absence of other requirements for OCSP signers and for the sake of standardization, they should generally be applied to all OCSP signers.

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

commonName

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

(02) [TLS] In subscriber certificates, the commonName attribute MAY be set. If set, it SHALL contain exactly one entry that is also contained in the SubjectAltName. Regarding the encoding of the commonName applies:

- IPv4 addresses SHALL be encoded according to RFC3986,
- IPv6 addresses SHALL be encoded according to RFC5952#4,
- FQDN and wildcard domain names SHALL be a character-by-character copy of the corresponding dNSName entry from the subjectAltName (see chapter 7.1.2).

(02) [EVCP] In subscriber 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[11].

serialNumber

(03) [LCP] [NCP] [NCP+] [QCP] In subscriber 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. The serialNumber attribute has no defined semantics beyond ensuring the uniqueness of the Subject-DN.

(03) [EVCP] In subscriber 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.

[11] See Appendix F of CABF EV Guidelines

givenName

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

(05) [LCP] [NCP] [NCP+] [QCP] In subscriber 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) [IVCP] In subscriber certificates the surname attribute MAY be set. If the surname attribute is set, it SHALL contain the name of the subject together with the givenName attribute.

(07) [LCP] [NCP] [NCP+] [QCP] In subscriber 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 subscriber 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) [TLS] In subscriber 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) [TLS] In subscriber 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) [TLS] In subscriber 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) [TLS] In subscriber 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 subscriber certificates, the businessCategory attribute SHALL be set with the applicable one of the following values[12]:

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

organizationalUnitName

(14) [TLS] In subscriber certificates that are issued before 1.09.2022, 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.

[12] See CABF EV Guidelines #8.5

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[13]
- a hyphen ("-")
- reference assigned according to the identified registration scheme

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

(16) [EVCP] In subscriber certificates 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[13]
- a hyphen ("-")
- reference assigned according to the identified registration scheme

(17) [LCP] [NCP] [NCP+] [QCP-l] In subscriber certificates for legal persons, 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 [13]
- a hyphen ("-")
- reference assigned according to the identified registration scheme

jurisdictionOfIncorporationLocalityName

(18) [EVCP] In subscriber 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 subscriber 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.

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

jurisdictionOfIncorporationCountryName

(20) [EVCP] In subscriber certificates the attribute jurisdictionOfIncorporationCountryName SHALL be set[13].

organizationName

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

(22) [TLS] In subscriber 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 subscriber 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 subscriber certificates for legal persons, the organizationName attribute SHALL be set and it SHALL contain the full legal name of the subject.

countryName

(24) [TLS] [EVCP] In subscriber 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 and subscriber certificates, but MAY only be set in Sub CA certificates.

[TLS] [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 subscriber 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.

CARLs 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 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.
- A checking capability of the OCSP Signer certificate in the cRLDistributionPoints and/or authorityInfoAccess extensions is set.
- No method for checking the status of the OCSP signer is specified, leaving it up to the verifier to decide whether and how to check the status of the OCSP signer certificate.

[TLS] [SMIME] If the OCSP responses are signed by a dedicated OCSP signer, the first of the variants above 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.

[TLS] [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 audited in accordance with all requirements of this section.

8.1 Frequency or circumstances of assessment

8.1.1 Internal audits

No stipulation.

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

[EVCP] Internal audits SHALL be performed on an ongoing basis.

8.1.2 External Audits

No stipulation.

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

TSPs that have not yet been audited in a period-of-time audit SHALL be audited in 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 [TLS] [SMIME] apply analogously to [EVCP]. In addition, 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.

[TLS] Analogously to the internal audits according to section 8.1.1, certificates issued by delegated third parties or containing information verified by delegated third parties SHALL be audited at least quarterly, unless the delegated third party is audited itself according to section 8.1.2. For this audit, a validation specialist of the TSP SHALL be used.

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

[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.

[TLS] [SMIME] External auditors performing audits in accordance with section 8.1.2 SHALL be qualified auditors who have the following qualifications and skills, i.e., they SHALL:

- be independent of the audited item
- be able to perform audits that meet the criteria specified in appropriate test schemes according to section 8.4
- 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
- be bound by law, government regulations, or rules of professional ethics; and
- maintain a professional liability errors and omissions insurance with coverage of at least one million dollars

For auditing according to the ETSI standards, the evaluation body SHALL also be accredited by “DAkkS” (German Accreditation Body) according to ISO 17065 using the requirements defined in ETSI EN 319 403.

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

[QCP] The TSP SHALL be audited 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.

[TLS] [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

[TLS] 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 or
- NCP+.

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

[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 time lines set by the internal or external auditors.

[TLS] [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 time lines according to section 4.9.1 SHALL be taken into account.

8.6 Communication of results

No stipulation.

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

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

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

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

9.2.1 Insurance coverage

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

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

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

Confidential business information SHALL be protected according to its classification.

9.4 Privacy of personal information

9.4.1 Privacy plan

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

In the privacy plans SHALL be described how the provisions of the [BDSG] with regard to the data collected in the registration process are implemented. 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
- to protect the personal data against accidental loss or destruction or damage

SHALL be taken.

9.4.2 Information treated as private

The information to be treated as private SHALL be described in the CPSs.

9.4.3 Information not deemed private

The information that is not deemed to be private SHALL be described in the CPSs.

9.4.4 Responsibility to protect private information

The responsibility for protecting private information SHALL be described in the CPSs.

9.4.5 Notice and consent to use private information

The methods for notifying individuals and obtaining consent for the use of private information SHALL be described in the CPSs.

9.4.6 Disclosure pursuant to judicial or administrative process

The conditions for disclosing personal data in the context of judicial or administrative proceedings SHALL be described in the CPSs.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

No stipulation.

9.6 Representations and warranties

9.6.1 CA representations and warranties

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

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

If trust service components provided by a Trusted Service component provider are used, it SHALL be ensured,

- that the use of the component's interface complies with the requirements specified by the trust service component provider,
- that the security and functionality required by the trust service component comply with the relevant requirements of this CP and the relevant CPSs.

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

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

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

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

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

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

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

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

- the subscriber has the right to use the domain names or IP addresses listed in the certificate (in the subjectDistinguishedName and/or subjectAltName)
- if applicable, the subscriber's representative was authorized to apply for the certificate on behalf of the subscriber,
- she was authorized by the subscribers 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 subscriber is not affiliated, she has entered into a legally valid and enforceable contract with the subscribers that meets all relevant requirements,
- if the subscriber is affiliated, a representative of the subscriber has acknowledged the terms and conditions of use,
- she operates status services in accordance with section 4.10 at least until the expiration date of the certificates and makes status information available to the public on a 24-hour basis
- she revokes a certificate if one of the reasons for revocation listed in the CPS applies,
- she complies with the requirements of this CP and the respective CPSs during the entire validity period of a certificate

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

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

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

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

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

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

9.6.2 RA representations and warranties

See sections 5.3.7, 6.5.1 and 9.6.1.

9.6.3 Subscriber representations and warranties

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

a) an obligation to provide accurate and complete information,
b) an obligation to use the key pair only in accordance with any restrictions communicated to the subscriber,
c) a prohibition on the unauthorized use of the private subscriber 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 private key, except for key decryption, after revocation of the subscriber certificate,
h) an obligation to immediately and permanently cease using the private key, except for key decryption, once the compromise of the issuing Sub CA has become known,

i) if a 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 the subscriber is a natural person and generates its keys itself and these are used for a "signed content commitment" (see section 7.1.2 (06) regarding KeyUsage "nonRepudiation"): a commitment that the private key is kept under the sole control of the end entity,
k) in the case where the subscriber is a legal person and generates its own keys and uses them for a "signed content commitment" (see section 7.1.2 (06) regarding KeyUsage „nonRepudiation“): a commitment that the private key is kept under the sole control of the end entity,

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 subscriber: a commitment to generate the keys within the secure cryptographic module,

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

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] if the subscriber 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] if the TSP generates and hands over the keys of the subscriber on a token: an obligation to report a compromise of the activation data in the course of token handover, which leads to a revocation of the certificate,
w) [3145] an obligation to verify the subscriber 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 subscribers can transmit the registration data,
pp) [3145] regulations on the acceptance of new versions of the terms of use by the subscribers in accordance with the applicable laws,
qq) [3145] a definition of the various roles of the subscribers (e.g., applicant, subject of the certificate), the various possible subjects of a certificate (e.g., natural persons, natural persons associated with a legal person, legal persons), and other significant roles in the certificate management processes
rr) [3145] a time limit after which subscribers must confirm, that their registration data is still valid,
ss) [3145] further requirements for subscribers depending on the required security level (e.g. virus protection, firewalls as well as 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] if the subscriber generates the keys itself: the requirements for the hardware and software used to generate the keys,
uu) [3145] if the TSP generates the keys of the subscribers: the process of handing over the keys,
vv) [3145] if the TSP generates and hands over the keys of the subscribers on token: the process of handing over the token,
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 termination according to section 5.8,
zz) [3145] Information about the time limits for processing 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 subscriber SHALL consist of two parts,

a) the first part SHALL be signed by the applicant and SHALL consider 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 consider the following aspects:
   i) consent to the obligations of the subject of the certificate (see section 1)),
   ii) consent to the use of a secure cryptographic module, if required,
   iii) consent to the processing of the collected data and, if applicable, the transfer of such data to third parties contracted by the TSP, including a transfer of the data in the event of termination of the service.

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 person, 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 subscribers 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 subscribers and relying parties in an appropriate manner. Acceptance of a new version by the subscribers SHALL be validated by the TSP.

9.6.4 Relying party representations and warranties

The following recommendations for relying parties SHALL be included in the terms of use (see also section 9.6.3) and/or the PDS.

Relying parties SHOULD

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

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

See section 9.6.

9.8 Limitations of liability

The liability of the TSP MAY be limited in accordance with applicable law. The limitations of liability SHALL be described in the CPSs as well as in the terms of use, see also section 9.6.3 para. ii).

[TLS] In the case that the TSP outsources tasks to a third party, the liability MAY be contractually allocated with the third party internally according to the tasks, but the TSP SHALL retain overall responsibility externally according to this CP and their CPSs.

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

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

9.9 Indemnities

No stipulation.

9.10 Term and termination

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

9.12.1 Procedure for amendment

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

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

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

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

9.12.2 Notification mechanism and period

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

New versions of a CPS SHALL be published according to the specifications of section 2.2. If changes have been made to a CPS that could affect the acceptance of the service by the subscribers or third parties, the changes SHALL be announced in due time to the subscribers, the third parties and, if applicable, evaluation bodies and supervisory or other regulatory authorities, see also section 9.6.1 and 9.6.3. When announcing the changes, reference SHALL be made to changed documents in the repository about the details..

9.12.3 Circumstances under which OID must be changed

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

9.13 Dispute resolution provisions

Policies and procedures for resolving complaints and disputes received from subscribers or relying parties regarding the Trusted Services SHALL be established and described in the CPSs and terms of use (see section 9.6.3 para. kk).

9.14 Governing law

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

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

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

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.

APPENDIX

Appendix A: Abbreviations

Table 4 - Abbreviations

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

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

Appendix B: References

Table 5 - References

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

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

Appendix C: Definitions

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

Table 6 - Definitions

Begriff	Bedeutung
Advanced electronic seal	Electronic seal according to [eIDAS#Art.36]
Advanced electronic signature	Electronic signature according to [eIDAS#Art.26]
Applicant	Natural or legal person who applies for a certificate for himself or for another *Subscriber*
Business Entity	[EVCP] All subscribers that do not belong to the categories ▪ Private Organization, ▪ Government Entity or ▪ Non-Commercial Entity e.g. general partnerships, unincorporated associations, sole proprietorships, etc.
Certficate User	Natural or legal persons who act in trust of the certificate, i.e., verify electronic signatures, authenticate persons or devices, or encrypt data by means of the certificates, for example. In this document, the terms "certificate user" and "relying third party" are used interchangeably
Certificate Approver	[EVCP] A natural person who is expressly authorized to represent the *Subscriber* of a certificate in order to ▪ act as a *Certificate Requester* himself/herself, ▪ authorize other employees of the *subscriber* or third parties to act as *Certificate Requesters*, ▪ approve certificate requests submitted by other *Certificate Requestors*
Certificate Management System	A system used by a TSP or a Delegated Third Party to process, approve, or store the issuance of certificates or certificate status information, including database, database server, and storage
Certificate Requester	[EVCP] A natural person expressly authorized to represent the *Subscriber* to complete and submit a Certificate Request on the *Subscriber's* behalf
Certification Authority Authorization (CAA)	[TLS] DNS resource record that allows the owner of a DNS domain name to specify the TSPs that are authorized to issue certificates for that domain
Contract Signer	[EVCP] A natural person who is expressly authorized to represent the *Subscriber* and sign Subscriber Agreements on its behalf
Government Entity	[EVCP] A legal entity, agency, department, or other related organizational unit operated by a government
High-Risk Certificate Request	[TLS] Certificate requests the TSP flags for additional review based on internal criteria. These may include: ▪ names that are at higher risk for phishing or other fraudulent use, ▪ names included in previously rejected certificate requests or revoked certificates,

	▪ names listed on the Miller Smiles phishing list or the Google Safe Browsing list; or ▪ names that a TSP identifies based on their own risk mitigation criteria.
Hish security zone	A specific physical location of the security zone of the TSP or a Delegated Third Party where the private keys or cryptographic hardware are located
Issuing System	A system used to sign certificates or validity status information.
Leaf Zertifikat	[TLS] A TLS certificate that was previously published as a pre-certificate
Non-commercial entity	[EVCP] An international organization created under a charter, treaty, convention, or equivalent instrument signed by or on behalf of more than one government of a country
Non-Reserved LDH-Label	[TLS] Component of a domain name that does not have a '-' in the third and fourth positions
P-Label	[TLS] Component of a domain name that has a '-' in the third and fourth positions ("XN label") and is followed from the fifth position by a valid output of the punycode algorithm according to [RFC3492# 6.3]
Pre-Certificate	[TLS] Certificate according to [RFC6962] for public logging of a yet-to-be-issued TLS certificate. The pre-certificate is generated from the yet-to-be-issued certificate plus the special critical extension "Certificate Transparency precertificate poison extension" (OID 1.3.6.1.4.1.11129.2.4.3). Pre-Certificates are not considered certificates according to [RFC5280] and cannot be validated by standard X.509v3 clients. The (real) TLS certificate generated later from the Pre-certificate is called a *Leaf Certificate*.
Private Organization	[EVCP] A non-governmental legal entity whose existence has been established by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation
Pseudonym	Fictitious identity that a person assumes for a specific purpose and that is different from his or her original or true identity. NOTE: A pseudonymous identity, unlike an anonymous identity, can be linked to the person's true identity. The true identity is known to the TSP
Reliable Method of Communication	[TLS] [SMIME] A communication method verified against a source other than the applicant's representative (e.g., address, phone number, or email address)
Secure Zone	Logical or physical area protected by measures that adequately protect the confidentiality, integrity, and availability of the Certficiate Systems used by the TSP
Security support system	System used to provide security functions, which may include authentication, network boundary control, audit logging, vulnerability scanning, or intrusion detection, for example
Short-term certificate	Certificate whose validity period is shorter than the maximum processing time for a revocation request specified in the CPS
Subject of a certificate	Entity identified in a certificate as the owner of the private key associated with the public key specified in the certificate. Subjects can be natural or legal persons or also organizational entities associated with them or also processes, functions or devices operated on their behalf. The subject of a certificate may also be at the same time, but need not be, the *Subscriber* and/or the *Applicant*

Subscriber	A natural or legal person to whom a certificate is issued and who is legally bound by terms of use or a contract with a TSP. A subscriber may also be both the *Subject* of a certificate and/or the *Applicant*, but does not have to be
Technically constraint CA	[TLS] A Sub CA where a combination of values in the extendedKeyUsage and nameConstraints extensions is used to limit the scope within which this Sub CA is allowed to issue subscriber or additional Sub CA certificates.
Token	Hardware module that generates and/or handles cryptographic keys in a secure manner
Validation Specialist	[TLS] Employee of a TSP or a RA who performs the information verification duties specified in [BR].
Verified method of communication	[EVCP] The use of a telephone number, fax number, email address, or postal address that has been verified by a TSP as a reliable way of communicating with the *Applicant* in accordance with [EVCG#11.5]
Verschlussache - Nur für den Dienstgebrauch	[3145] A classification of German government information to be protected
Wildcard Certificate	[TLS] A certificate with a *Wildcard Domain Name*
Wildcard Domain Name	[TLS] A domain name consisting of a single asterisk followed by a single dot ("*.") followed by a FQDN.