Deutsche Telekom Security GmbH
Certification Practice Statement Public

Version: 03.00

Valid from: 22.08.2022

Status: Release

Last Review: 17.08.2022

VERSION HISTORY

Table 1: Version history

Version	Date	Changes / Comments
01.00	24.09.2021	Initial version structured according to RFC 3647
02.00	15.03.2022	Include new CA certificate
03.00	13.08.2022	Addition of OV, general revision

TABLE OF CONTENT

Version history 2
Table of Content 3
List of tables 11
1 Introduction 12
1.1 Overview 12
1.2 Document name and identification 12
1.3 PKI participants 13
1.3.1 Certification Authorities 13
1.3.2 Registration Authorities 13
1.3.3 Subscribers 13
1.3.4 Relying parties 14
1.3.5 Other participants 14
1.4 Certificate usage 14
1.4.1 Appropriate certificate uses 14
1.4.2 Prohibited certificate uses 14
1.5 Policy administration 14
1.5.1 Organization administering the document 14
1.5.2 Contact person 14
1.5.3 Person determining CPS suitability for the policy 15
1.5.4 CPS approval procedures 15
1.6 Definitions and acronyms 15
2 Publication and repository Responsibilities 16
2.1 Repositories 16
2.2 Publication of certification information 16
2.3 Time or frequency of publication 17
2.4 Access controls on repositories 17
3 Identification and authentication 18
3.1 Naming 18
3.1.1 Types of names 18
3.1.2 Need for names to be meaningful 18
3.1.3 Anonymity or pseudonymity of subscribers 18
3.1.4 Rules for interpreting various name forms 18
3.1.5 Uniqueness of names 18
3.1.6 Recognition, authentication, and role of trademarks 18
3.2 Initial identity validation 18
3.2.1 Methods to prove possession of private key 19

3.2.2 Authentication of organization identity 19
3.2.3 Authentication of individual identity 19
3.2.4 Non-verified subscriber information 19
3.2.5 Validation of authority 20
3.2.6 Criteria for interoperation 20
3.2.7 Validation of Domain Authorization or Control 20
3.3 Identification and authentication for re-key requests 21
3.3.1 Identification and authentication for routine re-key 21
3.3.2 Identification and authentication for re-key after revocation 21
3.4 Identification and authentication for revocation request 21
4 Certificate life-cycle operational requirements 22
4.1 Certificate application 22
4.1.1 Who can submit a certificate application 22
4.1.2 Enrollment process and responsibilities 22
4.2 Certificate application processing 22
4.2.1 Performing identification and authentication functions 22
4.2.2 Approval or rejection of certificate applications 23
4.2.3 Time to process certificate applications 24
4.3 Certificate issuance 24
4.3.1 CA actions during certificate issuance 24
4.3.2 Notification to subscriber by the CA of issuance of certificate 24
4.4 Certificate acceptance 24
4.4.1 Conduct constituting certificate acceptance 24
4.4.2 Publication of the certificate by the CA 24
4.4.3 Notification of certificate issuance by the CA to other entities 24
4.5 Key pair and certificate usage 24
4.5.1 Subscriber private key and certificate usage 24
4.5.2 Relying party public key and certificate usage 25
4.6 Certificate renewal 25
4.6.1 Circumstance for certificate renewal 25
4.6.2 Who may request renewal 25
4.6.3 Processing certificate renewal requests 25
4.6.4 Notification of new certificate issuance to subscriber 25
4.6.5 Conduct constituting acceptance of a renewal certificate 25
4.6.6 Publication of the renewal certificate by the CA 25
4.6.7 Notification of certificate issuance by the CA to other entities 25
4.7 Certificate re-key 26
4.7.1 Circumstance for certificate re-key 26

4.7.2 Who may request certification of a new public key 26
4.7.3 Processing certificate re-keying requests 26
4.7.4 Notification of new certificate issuance to subscriber 26
4.7.5 Conduct constituting acceptance of a re-keyed certificate 26
4.7.6 Publication of the re-keyed certificate by the CA 26
4.7.7 Notification of certificate issuance by the CA to other entities 26
4.8 Certificate modification 26
4.8.1 Circumstance for certificate modification 26
4.8.2 Who may request certificate modification 26
4.8.3 Processing certificate modification requests 27
4.8.4 Notification of new certificate issuance to subscriber 27
4.8.5 Conduct constituting acceptance of modified certificate 27
4.8.6 Publication of the modified certificate by the CA 27
4.8.7 Notification of certificate issuance by the CA to other entities 27
4.9 Certificate revocation and suspension 27
4.9.1 Circumstances for revocation 27
4.9.2 Who can request revocation 28
4.9.3 Procedure for revocation request 28
4.9.4 Revocation request grace period 28
4.9.5 Time within which CA must process the revocation request 29
4.9.6 Revocation checking requirement for relying parties 29
4.9.7 CRL issuance frequency 29
4.9.8 Maximum latency for CRLs 29
4.9.9 On-line revocation/status checking availability 29
4.9.10 On-line revocation checking requirements 30
4.9.11 Other forms of revocation advertisement available 30
4.9.12 Special requirements re key compromise 30
4.9.13 Circumstances for suspension 30
4.9.14 Who can request suspension 30
4.9.15 Procedure for suspension request 30
4.9.16 Limits on suspension period 30
4.10 Certificate status services 30
4.10.1 Operational characteristics 31
4.10.2 Service availability 31
4.10.3 Optional features 31
4.11 End of subscription 31
4.12 Key escrow and recovery 32
4.12.1 Key escrow and recovery policy and practices 32

4.12.2 Session key encapsulation and recovery policy and practice 32
5 Facility, Management, and Operational controls 33
5.1 Physical controls 33
5.1.1 Site location and construction 33
5.1.2 Physical access 33
5.1.3 Power and air conditioning 33
5.1.4 Water exposures 34
5.1.5 Fire prevention and protection 34
5.1.6 Media storage 34
5.1.7 Waste disposal 34
5.1.8 Off-site backup 34
5.2 Procedural controls 34
5.2.1 Trusted roles 34
5.2.2 Number of persons required per task 35
5.2.3 Identification and authentication for each role 35
5.2.4 Roles requiring separation of duties 36
5.3 Personnel controls 36
5.3.1 Qualifications, experience, and clearance requirements 36
5.3.2 Background check procedures 36
5.3.3 Training requirements 37
5.3.4 Retraining frequency and sequence 37
5.3.5 Job rotation frequency and requirements 37
5.3.6 Sanctions for unauthorized actions 37
5.3.7 Independent contractor requirements 37
5.3.8 Documentation supplied to personnel 37
5.4 Audit logging procedures 37
5.4.1 Types of events recorded 37
5.4.2 Frequency of processing log 38
5.4.3 Retention period for archive 38
5.4.4 Protection of audit log 38
5.4.5 Audit log backup procedures 38
5.4.6 Audit collection system 38
5.4.7 Notification to event-causing subject 38
5.4.8 Vulnerability assessment 39
5.5 Records archival 39
5.5.1 Types of records archived 39
5.5.2 Retention period for archive 39
5.5.3 Protection of archive 39

5.5.4 Archive backup procedures 39
5.5.5 Requirements for timestamping of records 39
5.5.6 Archive collection system 39
5.5.7 Procedures to obtain and verify archive information 39
5.6 Key changeover 39
5.7 Compromise and disaster recovery 40
5.7.1 Incident and compromise handling procedures 40
5.7.2 Computing resources, software, and/or data are corrupted 40
5.7.3 Entity private key compromise procedures 40
5.7.4 Business continuity capabilities after a disaster 40
5.8 CA or RA termination 41
6 Technical security controls 42
6.1 Key pair generation and installation 42
6.1.1 Key pair generation 42
6.1.2 Private key delivery to subscriber 42
6.1.3 Public key delivery to certificate issuer 42
6.1.4 CA public key delivery to relying parties 42
6.1.5 Key sizes 42
6.1.6 Public key parameters generation and quality checking 43
6.1.7 Key usage purposes 43
6.2 Private key protection and cryptographic module engineering controls 43
6.2.1 Cryptographic module standards and controls 43
6.2.2 Private key (n out of m) multi-person control 43
6.2.3 Private key escrow 43
6.2.4 Private key backup 43
6.2.5 Private key archival 44
6.2.6 Private key transfer into or from a cryptographic module 44
6.2.7 Private key storage on cryptographic module 44
6.2.8 Method of activating private key 44
6.2.9 Method of deactivating private key 44
6.2.10 Method of destroying private key 44
6.2.11 Cryptographic module rating 44
6.3 Other aspects of key pair management 45
6.3.1 Public key archival 45
6.3.2 Certificate operational periods and key pair usage periods 45
6.4 Activation data 45
6.4.1 Activation data generation and installation 45
6.4.2 Activation data protection 45

6.4.3 Other aspects of activation data 45
6.5 Computer security controls 45
6.5.1 Specific computer security technical requirements 45
6.5.2 Computer security rating 46
6.6 Life cycle technical controls 46
6.6.1 System development controls 46
6.6.2 Security management controls 46
6.6.3 Life cycle security controls 47
6.7 Network security controls 47
6.8 Timestamping 48
7 Certificate, CRL, and OCSP Profiles 49
7.1 Certificate Profile 49
7.1.1 Version number 49
7.1.2 Certificate extensions 49
7.1.3 Algorithm object identifiers 49
7.1.4 Name forms 50
7.1.5 Name constraints 50
7.1.6 Certificate policy object identifier 50
7.1.7 Usage of Policy Constraints extension 50
7.1.8 Policy qualifiers syntax and semantics 51
7.1.9 Processing semantics for the critical Certificate Policies extension 51
7.2 CRL profile 51
7.2.1 Version number 51
7.2.2 CRL and CRL entry extensions 51
7.3 OCSP profile 51
7.3.1 Version number 52
7.3.2 OCSP extensions 52
8 Compliance audit and other assessments 53
8.1 Frequency or circumstances of assessment 53
8.2 Identity/qualifications of assessor 53
8.3 Assessor’s relationship to assessed entity 53
8.4 Topics covered by assessment 53
8.5 Actions taken as a result of deficiency 54
8.6 Communication of results 54
9 Other business and legal matters 55
9.1 Fees 55
9.1.1 Certificate issuance or renewal fees 55
9.1.2 Certificate access fees 55

9.1.3 Revocation or status information access fees 55
9.1.4 Fees for other services 55
9.1.5 Refund policy 55
9.2 Financial responsibility 55
9.2.1 Insurance coverage 55
9.2.2 Other assets 55
9.2.3 Insurance or warranty coverage for end-entities 56
9.3 Confidentiality of business information 56
9.3.1 Scope of confidential information 56
9.3.2 Information not within the scope of confidential information 56
9.3.3 Responsibility to protect confidential information 56
9.4 Privacy of personal information 56
9.4.1 Privacy plan 56
9.4.2 Information treated as private 57
9.4.3 Information not deemed as private 57
9.4.4 Responsibility to protect private information 57
9.4.5 Notice and consent to use private information 57
9.4.6 Disclosure pursuant to judicial or administrative process 57
9.4.7 Other information disclosure circumstances 57
9.5 Intellectual property rights 57
9.6 Representations and warranties 57
9.6.1 CA representations and warranties 57
9.6.2 RA representations and warranties 58
9.6.3 Subscriber representations and warranties 58
9.6.4 Relying party representations and warranties 58
9.6.5 Representations and warranties of other participants 58
9.7 Disclaimer of warranties 58
9.8 Limitations of liability 58
9.9 Indemnities 58
9.10 Term and termination 59
9.10.1 Term 59
9.10.2 Termination 59
9.10.3 Effect of termination and survival 59
9.11 Individual notices and communications with participants 59
9.12 Amendments 59
9.12.1 Procedure for amendment 59
9.12.2 Notification mechanism and period 59
9.12.3 Circumstances under which OID must be changed 60

9.13 Dispute resolution provisions 60
9.14 Governing law 60
9.15 Compliance with applicable law 60
9.16 Miscellaneous provisions 60
9.16.1 Entire agreement 60
9.16.2 Assignment 60
9.16.3 Severability 60
9.16.4 Enforcement 60
9.16.5 Force Majeure 60
9.17 Other provisions 61

LIST OF TABLES

Table 1: Version history.....2
Table 2: Sub CA certificates within the scope of this CPS.....13

1 INTRODUCTION

1.1 Overview

Deutsche Telekom Security GmbH (hereinafter referred to as Telekom Security) operates various Root Certification Authorities (Root CAs) and Subordinate Certification Authorities (Sub CAs) in its Trust Center for issuing certificates to customers and employees of the Deutsche Telekom AG.

This document is a Certification Practice Statement (CPS) of the Telekom Security Trust Center. It describes, in the structure of RFC3647, the implementation of the requirements from

- Telekom Security CP (OID 1.3.6.1.4.1.7879.13.42),
- ETSI EN 319 401,
- ETSI EN 319 411-1,
- Requirements published at http://www.cabforum.org:
  - “CA/Browser Forum Baseline Requirements” [BR],
  - “CA/Browser Forum Network and Certificate System Security Requirements”,
- Various Root Store Policies (Mozilla, Microsoft, Google, Apple)

to the Telekom Security PKI operation of the Public Certificate Service Platform and thus represents a supplement to the Telekom Security CPS Root.

In the event of any inconsistency between this CPS and the sources referenced above, the regulations from the referenced sources take precedence.

1.2 Document name and identification

This document is named „Telekom Security CPS Public” and is identified by the OID 1.3.6.1.4.1.7879.13.43. The OID is composed as follows:

{iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) T-Telesec (7879) PolicyIdendifier (13) Telekom Security CPS Public (43)}

1.3 PKI participants

1.3.1 Certification Authorities

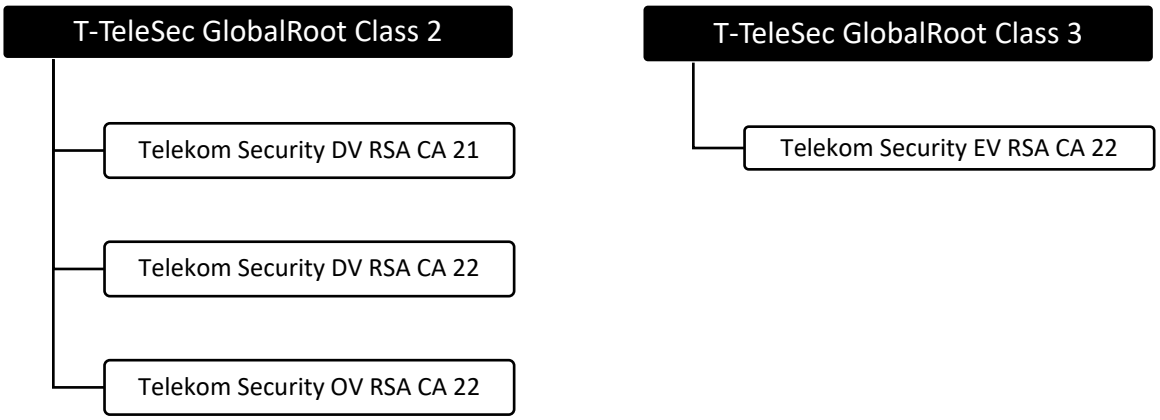
The following certification authorities (Sub CAs) are within the scope of this CPS:

Table 2: Sub CA certificates within the scope of this CPS

Common Name	Key type	Serialnumber	Validity period	Fingerprint (SHA1)
Telekom Security DV RSA CA 21	RSA 2048	2cf3c72f3f7d0fb31fc 362d6b869558e	2021-04-21 until 2031-04-21	99cc84f820818cf0eefe81d df572cace4b3acb78
Telekom Security DV RSA CA 22	RSA 4096	2103be2c2aa30a5b 5b1f0e1a4456239a	2022-02-22 until 2032-02-22	01648268a45f9e0990acb5 d391ad1876ccee0bed
Telekom Security OV RSA CA 22	RSA 4096	343262b23269e3db 202a1478136ac1af	2022-06-21 until 2032-06-21	32cd823131f8abb068fAa0 e2f495ad9fbc89afa4
Telekom Security EV RSA CA 22	RSA 4096	1cd786631ec0cfba0 b52fa9b5e0287b1	2022-06-21 until 2032-06-21	578fc66913edC923f12df29 c5993e6f25f9965dc

The Telekom Security EV RSA 22 is currently not yet active. The Sub CA certificates within the scope of this CPS are part of the following PKI hierarchy:

PKI-Hierarchie der Public Certificate Services Platform



The operation of the Root CAs is part of the scope of the Telekom Security Root CPS.

1.3.2 Registration Authorities

The Trust Center of Telekom Security acts as RA.

1.3.3 Subscribers

Subscribers are all natural and legal persons obtaining subscriber certificates under the CAs or Trust Services named in this CPS. Certificate subscribers therefore require a registered account with Telekom Security, e.g., via a corresponding service portal.

Subjects of subscriber certificates are domains or webserver, potentially in association with a legal person.

1.3.4 Relying parties

Relying parties are persons, systems or IT processes that trust certificates issued under this CPS and use them for the verification of digital signatures.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

CA certificates are only used for signing delegated OCSP responder and subscriber certificates as well as certificate revocation lists. For this, the certificate extensions according to section 7.1.2 are taken into account.

The appropriate use cases of subscriber certificates are specified by the certificate extensions KeyUsage and ExtendedKeyUsage. Additionally, the subscriber has to comply with applicable law.

1.4.2 Prohibited certificate uses

All certificates are not intended, designed or approved for use in control equipment in hazardous environments or environments where fail-safe operation must be ensured and failure may result in damage such as personal injury, death, moderate and severe environmental damage, other disasters. These include nuclear facilities, aircraft navigation or communication systems, air traffic control systems, weapons control systems.

1.5 Policy administration

1.5.1 Organization administering the document

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

1.5.2 Contact person

Contact for this CPS is the Root-Team of the Trust Center:

TrustCenter-Roots@telekom.de

Certificate misuse, key compromises, faulty or non-compliant certificates, other security-related certificate problems or suspicions of such incidents can be reported to the named email address by all parties. Regarding key compromise, the instructions made in section 4.9.12 are to be considered.

1.5.3 Person determining CPS suitability for the policy

The Trust Center Root-Team is responsible for determining the conformity of this CPS to the CP. For contact information see section 1.5.2.

1.5.4 CPS approval procedures

Each version of this CPS is released by the Trust Center management after conformity with the Telekom Security CP has been established and retains its validity for newly issued certificates and for existing certificates until it is revoked or replaced by a new version.

1.6 Definitions and acronyms

See Telekom Security CP.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Telekom Security operates a repository with information and documents (see section 2.2) as well as certificate status services (see section 4.9 and 4.10 in particular).

2.2 Publication of certification information

Telekom Security publishes the following information and documents (current as well as superseded versions) in the PKI repository of the Trust Center (https://www.telesec.de/de/service/downloads/pki-repository/):

- Telekom Security CP
- Certification Practice Statements (CPS, including this document)
- PKI Disclosure Statements (PDS)
- All CAs within the scope of this CPS
- Audit attestations for public Root CA certificates of Telekom Security (link to the Auditor's official web pages)
- Terms of use, services descriptions and Terms and conditions

The CPS Public is published in German and English. The German and English versions always have the same version number and are synchronized in terms of content. In case of dispute, however, the German version is authoritative.

Telekom Security publishes all required information on CA certificates in the "Common CA Database" (CCADB) in accordance with the CCADB policy (see https://www.ccadb.org).

Test web pages with one valid, one expired and one revoked TLS server certificate are operated for all public root CAs under which TLS server certificates are issued. The corresponding URLs for each Root CA can be found on the Trust Center website.

All TLS server certificates are published as "pre-certificates" in a sufficient number of CT Logs before their final issuance.

2.3 Time or frequency of publication

New versions of this CPS will be published at least annually in the above repository prior to their effective date.

New CA certificates within the scope of this CPS are published both in the CCADB and in the repository within 7 days of their issuance and in any case before they go into operation.

Audit attestations are published or linked in the CCADB as well as in the repository within 7 days after their issuance.

2.4 Access controls on repositories

The information listed in section 2.2 are publicly accessible in a read-only manner without access restrictions. The availability and integrity of the information provided are ensured by appropriate technical measures.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The names of the certificate holders are included in all certificates in the form of a distinguished name according to [x500]. In addition, TLS server certificates always include a subjectAltName. See chapter 7.1.4 for details.

3.1.2 Need for names to be meaningful

No stipulation.

3.1.3 Anonymity or pseudonymity of subscribers

Not applicable.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

A SubjectDN is unique in its assignment to the certificate subscribers, i.e. it is not assigned to different certificate subscribers. If the data of several subscribers matches, additional identifiers are added to make the SubjectDN unique.

Exceptions to this rule are domain validated certificates. In this case, a SubjectDN can be assigned to a new subscriber if the subscriber has demonstrated control over the domain.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

For the initial validation of the identity of a natural or legal person, only direct evidence or attestations from appropriate and authorized sources are used. The proofs can be collected in paper form or electronically and only such proofs are requested which are necessary for identification.

The authenticity of evidence provided will be checked for alterations and forgeries as far as possible.

3.2.1 Methods to prove possession of private key

A certificate request (PKCS#10) signed with the corresponding private key is necessary for issuance of a certificate.

3.2.2 Authentication of organization identity

The following methods are used to validate an organization identity.

(QGIS - Qualified Government Information Source) The existence and identity of an organization are validated via government-held sources that are deemed reliable for identification. Examples of QGIS include commercial registers, professional bodies under public law, and the Federal Central Tax Office. For a check, the information provided by the applicant is used for an automated or manual search in the relevant registers. Results are compared with the information provided.

(QIIS - Qualified Independent Information Source) The existence and identity of an organization are validated through sources maintained under private law and deemed reliable for identification purposes. These sources are evaluated for timeliness and reliability before being classified as QIIS by Telekom Security. Examples of QIIS are credit reporting agencies. For a check, the information provided by the applicant is used for an automated or manual search in the QIIS databases. Resulting results are matched against the information provided.

(Attestation) The applicant proves the existence and identity of an organization by submitting an attestation letter issued by a notary. A prerequisite for the acceptance of such evidence is that the notary is listed in an appropriately recognized notary directory.

(Secondary Source) The applicant proves the address of an organization by submitting a government-issued tax notice, bank statement, invoice, or the like. The timeliness, reliability and relevance of the submitted evidence will be evaluated individually by the registration staff and accepted or rejected as necessary to prove individual attributes.

3.2.3 Authentication of individual identity

An authentication of natural persons is not required in the context of domain or organizational validated TLS server certificates.

3.2.4 Non-verified subscriber information

Only information validated according to chapter 3.2.2 or 3.2.7 is included in a certificate.

3.2.5 Validation of authority

For organization validated TLS server certificates, the authenticity of the certificate request is validated via proof of the applicant's authorization to request certificates on behalf of the organization (the certificate subject).

3.2.6 Criteria for interoperation

Not applicable.

3.2.7 Validation of Domain Authorization or Control

The following methods are used to validate domain control:

DNS Change (Method according to [BR#3.2.2.4.7]):

The applicant proves control over an FQDN by providing a unique given random value in the DNS TXT record of the Domain prefixed with a given domain label. The prefix begins with an underscore and the requirements of [BR] regarding this method are complied with.

This method can also be used for validating wildcard certificates.

Validating Applicant as a Domain Contact (Method according to [BR#3.2.2.4.12]):

The control over an FQDN is validated via the Domain Contact.

This method is only allowed for domains (including wildcard certificates) of Deutsche Telekom AG.

The requirements of [BR] regarding this method are complied with.

Agreed-Upon Change to Website v2 (Method according to [BR#3.2.2.4.18]):

The applicant proves control over an FQDN by providing a unique given random value in a file under the “/.well-known/pki-validation” directory. The requirements of [BR] regarding this method are complied with.

Agreed-Upon Change to Website – ACME (Method according to [BR#3.2.2.4.19]):

The applicant proves control over an FQDN via the ACME HTTP challenge as defined in RFC 8555 section 8.3 and supplemented by the requirements of [BR].

For wildcard certificates, the requirements of [BR] chapter 3.2.2.6 are complied with, based on the ICANN-Domains listed in the Public Suffix List.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Identification and authentication is performed, taking into account the validity period of validations and proofs according to chapter 4.2.1, by successfully logging in to the customer account, e.g. via username and password or another form of secret.

3.3.2 Identification and authentication for re-key after revocation

A renewal of certificates after revocation is not provided.

3.4 Identification and authentication for revocation request

Authorized revocation requests can be made by using the ACME protocol to prove control over a domain contained in the certificate, compromise of the key, or the identity of the revocation requestor as the ACME account holder corresponding to the certificate to be revoked.

Certificate requesters can also authorize revocation of their own certificates via their own customer account.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Certificate applications can generally be submitted by all natural persons and legal entities or their authorized representatives, provided they have registered a customer account with the Trust Center of Deutsche Telekom Security GmbH that is linked to a valid e-mail address. However, entities with which business is not permitted due to legal or Group-internal regulations are excluded from this.

4.1.2 Enrollment process and responsibilities

The application process for subscriber certificates includes the following points depending on the certificate type:

- Generation of a key pair in accordance with the applicable requirements of this CPS
- Provision of the information to be included in the certificate in the form of a certificate request including a signed certificate signing request for the previously generated key pair and which includes the desired domains (at least one domain)
- Provision of a handwritten or electronically signed power of attorney by an authorized signatory of the organization
- Acceptance of the privacy policy, general terms and conditions, terms of use
- Confirmation of the correctness of the information provided in the certificate application and the correct generation of the key pair
    - If applicable, additional verification documents

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Certificate applications are checked for completeness, correctness and authenticity by automated mechanisms as well as registration staff. In particular, the information is validated with reliable sources in accordance with chapter 3.2. Validations and verifications that have already been performed may be used, provided that the deadlines specified in Section 4.2.2 are met.

For TLS server certificates, control over any domains contained in the certificate request is validated using one of the methods described in Section 3.2.7.

For OV certificates, the identity of the organization is validated using the methods described in Section 3.2.2. Specifically, the following methods are used for the respective attributes:

- Organizationname: QGIS, QIIS, Attestation
- Country: QGIS, QIIS, Attestation
- Locality: QGIS, QIIS, Attestation

- PostalCode: QGIS, QIIS, Attestation
- StreetAddress (optional) : QGIS, QIIS, Attestation, Secondary Source
- StateOrProvinceName (optional) : QGIS, QIIS, Attestation, Secondary Source

The applicant's authorization to request certificates on behalf of an organization is validated for organization validated TLS server certificates according to Section 3.2.5.

Manual activities associated with identification and authentication are performed exclusively by personnel in trusted roles at Telekom Security's Trust Center.

4.2.2 Approval or rejection of certificate applications

Incomplete or incorrect certificate applications will be rejected or the remaining information will be obtained from the applicant or, after being obtained from a reliable, independent data source, confirmed by the applicant.

Certificate requests for Internal Names (as defined in the Baseline Requirements [BR]) are rejected.

For TLS server certificates, the CAA records in the DNS are checked at the start of an application and immediately before a certificate is issued for all FQDN entries contained in the application. A certificate request is rejected if there is an entry in "issue" or "issuewild" that is not "telesec.de". "iodef" entries are evaluated but not followed upon. Further entries of the CAA record are not supported. The CAA check is valid for 8 hours. If the query of a CAA record fails, the issuance of the certificate is nevertheless continued, provided that

- the error is outside Telekom Security’s infrastructure,
- the query has been repeated at least once, and
- the zone of the domain has no DNSSEC validation chain to the ICANN root.

Certificate requests are rejected if the key is considered to be compromised or does not meet the quality criteria according to Section 6.1.5 and Section 6.1.6.

Telekom Security maintains denied lists and high risk lists for applicants as well as domains. Certificate entries are rejected accordingly or subjected to an extended check if the applicant or a domain are included in the lists mentioned. This includes, for example, organization names and domains for which Telekom Security is not permitted to issue certificates due to internal or national regulations or which have an increased risk of being the target of phishing, misuse or fraud attacks due to their attractiveness.

For all applications, it is verified that the FQDNs are under an ICANN domain that is listed in the Public Suffix List. For wildcard certificates whose FQDN portion is of the type "public suffix" (definition according to [BR], ICANN domain), the applicant must prove its lawful control over the entire domain namespace. The Public Suffix List is consulted regularly for this purpose, but at the latest every 30 days.

If all validation steps according to chapter 4.2.1 have been performed successfully and none of the checks mentioned above led to a rejection, the certificate issuance is approved. Nonetheless, Telekom Security is entitled to refuse certificate applications without giving reasons.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Telekom Security ensures that the integrity and authenticity of the data to be written to the certificate are guaranteed by technical, organizational and personnel measures when issuing the certificates.

All TLS server certificates are published as "pre-certificates" in a sufficient number of CT log servers (Certificate Transparency according to RFC 6962) before the actual issuance and the Signed Certificate Timestamps (SCTs) are included in the actual certificate. The number of SCTs depends on the certificate type (see chapter 7.1.2).

4.3.2 Notification to subscriber by the CA of issuance of certificate

After issuance of a certificate, it is made available via the selected interfaces. There is no separate notification of the applicant.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

Subscribers can obtain certificates issued to them via the provided interfaces. Apart from that, TLS server certificates are not published in any way.

4.4.3 Notification of certificate issuance by the CA to other entities

Prior to issuance, TLS server certificates are published in several CT log servers, see section 2.2 or 4.3.1.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers are obligated via general terms and conditions to use certificates exclusively in accordance with this CPS and the intended uses for the certificate, and to protect the private keys throughout their entire lifecycle.

In particular, TLS server certificates are only allowed to be installed on webservers that are available under one of the domain names listed in the subjectAltName extension.

4.5.2 Relying party public key and certificate usage

Relying parties have the responsibility to check the entire context and chain of trust including the provided revocation and status information before using a certificate. Failure to check certificate information or ignoring a check result is on the relying party's own risk.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

A certificate renewal is handled as a new certificate application.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Certificate re-key is handled as a new certificate application.

4.7.2 Who may request certification of a new public key

Not applicable.

4.7.3 Processing certificate re-keying requests

Not applicable.

4.7.4 Notification of new certificate issuance to subscriber

Not applicable.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Not applicable.

4.7.6 Publication of the re-keyed certificate by the CA

Not applicable.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

Certificate modification is handled as a new certificate application.

4.8.2 Who may request certificate modification

Not applicable.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 Notification of new certificate issuance to subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6 Publication of the modified certificate by the CA

Not applicable.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A subscriber certificate is revoked within 24 hours if one or more of the following occurs:

- The subscriber requests in writing that Telekom Security revokes the certificate.
- The subscriber notifies Telekom Security that the original certificate request was not authorized and does not retroactively grant authorization.
- Telekom Security obtains evidence that the subscriber's private key corresponding to the public key in the certificate suffered a key compromise.
- Telekom Security is made aware of a demonstrated or proven method that can easily compute the subscriber's private key based on the public key in the certificate (such as Debian weak key).
- Telekom Security obtains evidence that the validation of domain authorization or control for any Fully Qualified Domain Name in the certificate should not be relied upon.

A subscriber certificate is, if possible, revoked within 24 hours, but at the latest within 5 days if one or more of the following occurs:

- The certificate no longer complies with the requirements of section 6.1.5 and section 6.1.6.
- Telekom Security obtains evidence that the certificate was misused.
- Telekom Security is made aware that a subscriber has violated one or more of its material obligations under the subscriber agreement or terms of use.

- Telekom Security is made aware of any circumstances indicating that use of a Fully Qualified Domain Name in the certificate is no longer legally permitted (e.g., a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name).
- Telekom Security is made aware that a Wildcard certificate has been used to authenticate a fraudulently misleading subordinate Fully Qualified Domain Name.
- Telekom Security is made aware of a material change in the information contained in the certificate.
- Telekom Security determines or is made aware that any of the information appearing in the certificate is inaccurate.
- Telekom Security's right to issue certificates under the [BR] expires or is revoked or terminated unless Telekom Security has made arrangements to continue maintaining the CRL/OCSP repository.
- Revocation is required by Telekom Security's Certificate Policy.
- Telekom Security is made aware of a demonstrated or proven method that exposes the subscriber's private key to compromise or if there is clear evidence that the specific method used to generate the private key was flawed.

Revoked certificates will not be reinstated.

4.9.2 Who can request revocation

Revocation of a certificate can be requested by Telekom Security, the subscriber or a representative of the subscriber.

In addition, the revocation of a certificate can be triggered by any party if it can be proven to the Trust Center that one of the revocation reasons listed in Section 4.9.1 applies. See Chapters 1.5.2 and 4.9.12 for more information.

4.9.3 Procedure for revocation request

Authorized revocation requests can be made by using the ACME protocol to prove control over a domain contained in the certificate, compromise of the key, or the identity of the revocation requestor as an ACME account holder corresponding to the certificate to be revoked.

Certificate applicants can also authorize revocation of their own certificates via their customer account.

The Trust Center also offers an e-mail interface for reporting certificate misuse and problem messages (see Section 1.5.2). Telekom Security processes these reports and, if there is a corresponding reason for revocation, initiates the revocation of affected certificates. The person reporting the problem is informed of the receipt of the message and, if applicable, of any resulting revocations of the affected certificates.

4.9.4 Revocation request grace period

Certificate subscribers are obligated via the terms of use to submit a revocation request without delay as soon as a revocation reason is identified in accordance with Section 4.9.1.

4.9.5 Time within which CA must process the revocation request

If there is an authorized revocation request for a subscriber certificate, the revocation is carried out by the system within a few minutes. If one of the reasons listed in Chapter 4.9.1 is identified for a subscriber certificate, the revocation will be carried out as quickly as possible, taking the circumstances into account. For TLS server certificates, the facts and circumstances are investigated within 24 hours of receipt of a problem report and initial feedback is given to the subscriber and the reporting person on the findings up to that point. Subsequently, the results of the analysis are discussed with the subscriber and the reporting person and a decision is made as to whether a revocation is required. If revocation is necessary, the time of the revocation will be determined, taking into account the time guidelines from chapter 4.9.1 and considering the following aspects:

- the nature of the suspected problem (scope, context, severity, extent, risk of harm)
- the impact of blocking (direct and collateral impact on end-participants trusting third parties)
- the number of problem reports for a certificate or end-entity
- the entity that posted the notification
- the relevant legal provisions

The revocation of a certificate includes the implementation of the revocation status in the certificate status services. Exceptions to this are revocations requested for a later date. In this case, the requested date for revocation of the certificate listed in the revocation request is decisive.

4.9.6 Revocation checking requirement for relying parties

Trusting third parties are recommended to query the status of certificates using the certificate status services provided in accordance with Section 4.10 before trusting a certificate.

4.9.7 CRL issuance frequency

Certificate revocation lists (CRLs) for subscriber certificates are published regularly every 24 hours.

4.9.8 Maximum latency for CRLs

Newly issued CRLs usually are published in the repositories immediately after generation.

4.9.9 On-line revocation/status checking availability

Online status information is provided for all certificates via OCSP.

The "Authority Information Access" certificate extension of each certificate contains the URL of the relevant OCSP responder.

4.9.10 On-line revocation checking requirements

Third parties are required to take into account the specifications for processing OCSP responses according to RFC6960 when checking a certificate status via OCSP (see Telekom Security CP).

4.9.11 Other forms of revocation advertisement available

No stipulation.

4.9.12 Special requirements re key compromise

Any party can report a key compromise via the ACME protocol function mentioned in 4.9.3 or via the contact described in Section 1.5.2. For the latter, sufficient information or references to information proving the fact of a key compromise must be provided. If possible, a CSR signed with the compromised private key should be provided with commonName "Compromised Key" in Base64 format. In addition, the affected certificate itself should be referenced.

Subscribers can also report a key compromise via the revocation function of their account and specifying "Key compromise" as the reason for revocation.

4.9.13 Circumstances for suspension

Certificate suspension is not supported.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

Over the entire validity period of all certificates issued, revocation lists signed by the CAs and OCSP responses signed by delegated OCSP responders are provided, of which the authenticity and integrity are ensured by technical as well as organizational measures.

4.10.1 Operational characteristics

All certificate status information (revocation lists and OCSP) is time-synchronized regularly before generation, but at the latest every 24 hours.

Taking into account the different update periods of both methods, the provided status information of revocation lists and OCSP information is consistent after 24 hours at the latest.

4.10.1.1 Operational characteristics for the provisioning of OCSP

Delegated OCSP responders are operated in compliance with RFC6960. Requests for certificates with unknown certificate serial numbers are answered with the status "unknown".

The value of “nextUpdate” is 5 days after the thisUpdate-entry but are only cached for further status requests for a maximum of 2 hours as far as the status of the corresponding certificate does not change within a shorter period.

OCSP requests for unused serial numbers are monitored.

4.10.1.2 Operational characteristics for the provisioning of CRLs

The value of the nextUpdate field of a revocation list is 5 days after the value of the thisUpdate field.

Revoked certificates are listed in all CRLs until at least the next regular CRL issued after the validity period of the revoked certificates.

4.10.2 Service availability

The certificate status services are available 7x24h. Measures have been taken to ensure that availability of the certificate status services is restored within 12 hours in the event of a disruption. In addition, the greatest possible efforts are made to rectify disruptions as quickly as possible.

Sufficient capacities are available so that the response time does not exceed 3 seconds under normal operating conditions.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

If an end of subscription is linked to a revocation of certificates, the provisions described in section 4.9 apply.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practice

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The Trust Center of Deutsche Telekom Security GmbH is within the scope of a security guideline approved by management and an associated Information Security Management System (ISMS), which is certified in accordance with ISO 27001.

The ISMS itself as well as other security guidelines, security concepts and other documents ensure compliance with the requirements specified in the Telekom Security CP (section 5). In particular, risk management comprises a risk analysis including probabilities of occurrence and extent of damage as well as appropriate risk treatment including final (residual) risk acceptance. The risk management processes are carried out at least once a year and on an ad hoc basis.

5.1 Physical controls

Trust Center facilities, media and information are protected against loss, theft, damage or compromise by physical measures according to their criticality. These measures are set forth in internal security concepts and other documents.

5.1.1 Site location and construction

The Trust Center infrastructure is located in two geo-redundant data centers (so-called twin-core data center) within Germany. When selecting the locations, environmental conditions such as susceptibility to natural disasters and other sources of danger were taken into account, based on an appropriate risk analysis. The building's construction and infrastructure are designed for the secure operation of critical systems and meet the requirements for a high-security zone.

The areas relevant to Trust Center operations are separated from other areas by additional enclosures and are audited and certified to "Trusted Site Infrastructure TSI V3.2 Dual Site".

5.1.2 Physical access

The data centers have extensive physical security measures, including security personnel, secured entrances, intrusion detection systems, and multi-level access systems. Specifically, Trust Center operating rooms are accessible only to authorized individuals in trusted roles and visitors are permitted only when accompanied by such an individual.

Access rights will be reviewed and adjusted as necessary on a regular basis and as needed.

5.1.3 Power and air conditioning

The data centers are equipped with redundant power supplies and air conditioning systems. The systems are protected against voltage fluctuations and are protected by uninterruptible power supplies (short- and long-term bridges) with cross-cabling.

5.1.4 Water exposures

The data centers are located outside the danger zone of floods or other sources of danger. In addition, the operating rooms themselves are protected from water intrusion or water damage by additional measures.

5.1.5 Fire prevention and protection

The data centers are protected against fire damage by structural measures in accordance with the critical protection requirements and applicable fire protection regulations.

5.1.6 Media storage

Media are stored exclusively in the Trust Center's operating rooms, protected from the effects of fire and water and from unauthorized access.

5.1.7 Waste disposal

Confidential documents and data media are disposed of securely and only through certified waste disposal companies. In addition, all data media are erased using certified processes prior to disposal. Media is not reused for other purposes.

5.1.8 Off-site backup

Backup data is being stored geo-redundantly.

5.2 Procedural controls

5.2.1 Trusted roles

The Trust Center is organized based on the following trusted roles:

- Head of TSP: holds the overall responsibility for the Trust Center services
- (Information) Security Officer: plans and supervises the implementation of security measures, manages the ISMS
- ISMS team member: supports the information security officer in his tasks
- Administrator: configures and maintains the IT infrastructure (networks, databases, servers, applications etc.)
- CA Operator: generates CA keys and certificates
- Internal auditor: audits certificates, processes, documentation, and ceremony compliance on a regular basis and in the event of inconsistencies
- Root/Compliance-Team: coordinates implementation of requirements, monitors requirement sources (mailing lists, root store policies, ETSI), handles external communication with root store operators and "Bugzilla", advises on incidents and

changes, is responsible for CP and various CPS, processes certificate applications for CA issuances
- RA/Validation specialist: validates certificate applications, triggers certificate issuance and manual revocation of certificate

5.2.2 Number of persons required per task

For all roles listed in section 5.2.1 there is at least one representative appointed.

Technical and organizational measures are in place to ensure that security-relevant or security-critical activities are performed only by persons in trusted roles and only under the dual control principle. The number of employees performing such security-relevant or -critical activities is kept to a minimum, taking into account deputy regulations and work-related circumstances.

The security-relevant and security-critical activities for which dual control (or more) is required are:

- CA key generation, backup and recovery
- any activities at the Offline CA or access to the Offline CA:
  - issuance of certificates and revocation lists
  - revocation of certificates
  - changes to the configuration
- any access to the offline HSMs (incl. backup HSMs)
- assessment of security incidents

5.2.3 Identification and authentication for each role

The identification of suitable persons to fill roles, the transfer of roles (authentication) and their revocation are carried out according to a documented process, which includes clarification of the need, exclusion of conflicts of interest, the willingness of the person to take on the activities, approval by the manager and documentation of evidence for this.

Prior to the transfer of a trusted role (or even at the time of hire as an employee), the appropriate individual will be personally identified by presenting official identification and acceptance for the transfer of the role, the responsibilities associated with it, and the resulting duties to ensure security will be obtained from that individual as well as Trust Center management.

Roles are only transferred to persons if this does not give rise to any conflicts of interest (see also section 5.2.4) and independence is maintained, i.e., that

- the areas of the Trust Center charged with issuing and revoking certificates are independent of other organizations in their decisions regarding the establishment, provision, maintenance, and suspension of services in accordance with applicable certificate policies and
- all employees entrusted with the issuing and revocation of certificates are free from financial or other pressures in the performance of their duties that could affect trust in the services provided by the Trust Center. This applies to all employees in trusted roles as well as senior managers and executives.

This structure, which ensures impartiality of operations, is documented in the Trust Center's ISMS Manual, among other documents.

Role holders are officially appointed to the trusted role by Trust Center management.

Role holders are advised that they may only act in the assigned role when performing tasks assigned to the role.

The assignment of required privileges is based on the "least privilege" principle, i.e., all privileges are limited to the minimum required.

After termination of employment of an employee in a trusted role, their access permissions are revoked within 24 hours.

5.2.4 Roles requiring separation of duties

The following roles are separated from each other:

- Management/Head of Trust Center
- IT Security Officer/Compliance Team/Internal Auditor
- RA/Validation specialist
- Administrator/CA operator

The named roles can only be applicants for certificates if these certificates are requested on behalf of their own organization.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The Trust Center management is stable and has many years of experience in the technical and organizational operation of the services offered by the Trust Center. In addition, through education, experience and training, they are well-versed in information security (including risk management, security procedures for personnel etc.) and PKI technologies.

Trust Center employees meet the requirement for sufficient expert knowledge to perform their activities correctly based on education, specific training, many years of experience or a combination of these. In addition, all Telekom Security employees and those of the Trust Center in particular are regularly informed about general security and privacy regulations, current threats and the specific requirements of the ISMS (e.g., by the ISMS or group-wide information events).

5.3.2 Background check procedures

All employees in trusted roles prove their trustworthiness by regularly submitting an official certificate of good conduct. Prior to an employment, relevant references, educational degrees etc. are reviewed to determine suitability for an occupation.

5.3.3 Training requirements

See section 5.3.1.

5.3.4 Retraining frequency and sequence

The Trust Center's employees are regularly (at least annually) sensitized with regard to information security and data privacy, and additionally on an ad hoc basis to current threats and security practices.

In addition, personnel in trusted roles receive regular technical training to maintain the necessary know-how.

5.3.5 Job rotation frequency and requirements

No stipulation.

5.3.6 Sanctions for unauthorized actions

Trust Center employees are accountable for their actions. Violations of requirements will have appropriate consequences under employment law, depending on the severity of the violation.

5.3.7 Independent contractor requirements

Not applicable since there is no external personnel in the context of PKI operation.

5.3.8 Documentation supplied to personnel

All role owners are provided with role descriptions which, in addition to the responsibilities and duties resulting from that role, at least specify the required

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

The information security guidelines and the security roles and responsibilities defined therein are described in corresponding Group documents and are available to all employees via the intranet.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The events required in Telekom Security CP chapter 5.4.1, i.e.

- all significant events of the certificate and key management systems as well as status services,
- all security-relevant events on the PKI and security systems,
- installation, update and uninstallation of software on the PKI systems
- Physical entries and exits to and from the security zones,

are logged continuously including a description of the event, the precise time and, if applicable, the identity of the trigger. The time of the logging systems is synchronized several times per day with a central and trusted source.

5.4.2 Frequency of processing log

Log data is evaluated as follows:

- Safety-relevant events are evaluated as described in Chap. 6.6.2.
- All other log data is only evaluated if necessary, e.g. for troubleshooting or analysis activities.

5.4.3 Retention period for archive

All logs mentioned in section 5.4.1 are retained for two years after their occurrence or two years until after expiration or revocation of the corresponding certificate or destruction of a CA key.

5.4.4 Protection of audit log

Technical and organizational measures have been established to ensure the confidentiality and integrity of the log data. The storage of log data is also monitored in internal audits.

5.4.5 Audit log backup procedures

Log data is backed up as part of regular system backups.

5.4.6 Audit collection system

All security-relevant events on PKI and security systems are immediately sent to a separate and tamper-proof log server via secure communication channels.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessment

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

All activities in section 5.4.1.1 are archived.

5.5.2 Retention period for archive

See section 5.4.3.

5.5.3 Protection of archive

See section 5.4.4.

5.5.4 Archive backup procedures

The electronic repositories for storing electronically signed applications and, if applicable, digitized minutes are set up with multiple redundancies and are backed up regularly.

5.5.5 Requirements for timestamping of records

See section 6.8.

5.5.6 Archive collection system

Only internal Archive collection systems are used.

5.5.7 Procedures to obtain and verify archive information

The archived data listed in section 5.5.1 is checked on demand (e.g., in the case of problem reports or in legal proceedings) and, if necessary, released as evidence or made available to internal or external auditors on request.

5.6 Key changeover

Before a sub-CA certificate expires, a new CA certificate is issued in good time in accordance with the current versions of the CP and CPS Root. The period between the publication of the

new CA certificate and the decommissioning of the old CA certificate is chosen to be sufficiently long so that there is no interruption in operation for end subscribers.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The emergency documentation of the Trust Center takes into account the requirements of the Telekom Security CP.

Trust Center employees have several options (technical interface, direct contact with ISMS, employee portal) for reporting (information security) incidents and are obligated to report incidents. Reports or alerts are followed up by qualified personnel according to the criticality in a reasonable time.

Security incidents with a significant impact on the trust service provided or on private data are, depending on the type and context of the incident, reported to the BSI, the Bundesnetzagentur or the data protection authority within 24 hours.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, Telekom Security also notifies the natural or legal person of the breach of security or loss of integrity without undue delay.

If an incident represents a violation of a Root Store Policy, the Trust Center Root/Compliance Team will promptly prepare an incident report, taking into account any specifications required by the root store operators. If necessary, the issuance of affected certificate types will be stopped until the cause has been eliminated or further damage can be ruled out.

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

Regular data backups of all relevant systems are carried out so that they can be restored if necessary. The data backups are kept geo-redundantly and are subject to the same security measures as critical systems.

5.7.3 Entity private key compromise procedures

The compromise, suspected compromise, or loss of a CA private key is treated as an emergency scenario and handled according to the processes defined in the emergency documentation.

In case of a compromised CA key the corresponding CA certificates are revoked and all affected subscribers to that CA as well as other instances with whom corresponding agreements have been made are informed.

5.7.4 Business continuity capabilities after a disaster

The continuation of business and the provision of the services and systems required for compliant continued operation are ensured by technical and organizational measures. In

addition to geo-redundant operation, these include emergency documentation and emergency management set up in accordance with Telekom Security CP chapter 5.7.1.

5.8 CA or RA termination

Before discontinuing operations, Telekom Security will evaluate whether the provision of the Trust Service for existing customers can be transferred to another Trust Service Provider. Prior to the transfer, appropriate agreements will be concluded with the acquiring Trust Service Provider.

If a transfer is not possible, secure termination will be ensured in accordance with a continuously updated termination plan.

All affected certificate holders, trusted root stores and subcontractors are informed in good time. For all other relying third parties, appropriate information will be provided on the Trust Center web pages.

Operation of the status services will be handed over to Deutsche Telekom AG, which acts as a Trust Service Provider (TSP) in accordance with the “Vertrauensdienstegesetz”, until the validity of all end user certificates expires. Likewise, the records archived in accordance with Section 5.5.1 shall be handed over to Deutsche Telekom AG for safekeeping until the specified retention period expires. Customer data and other data that does not need to be retained will be deleted.

All certificates not yet revoked at the time of the planned decommissioning will be revoked and the private keys of the sub-CAs will be destroyed.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

No keys are generated for end subscribers. However, the end participants are informed of the permissible key algorithms.

Key pairs for CAs are generated with HSMs according to chapter 6.2.1 in the secure environment of the Trust Center and as part of a key ceremony. Generation requires management approval. The trusted roles involved in the ceremony and their tasks before, during and after the key ceremony are described in a work instruction. This includes, among other things, the work steps for activating the HSMs using shared activation data, key generation and backup in a multi-person principle with different roles.

All ceremonies are monitored by a qualified internal auditor and, in the case of Sub CAs for the issuance of TLS server certificates, by a qualified external auditor of a conformity assessment body (see chapter 8.2). Successful performance of a ceremony is confirmed by the auditors in the protocols.

Key pairs for OCSP signers are generated in HSMs according to chapter 6.2.1 in the secure environment of the Trust Center.

Key pairs for RA employees are generated in appropriately certified smartcards.

6.1.2 Private key delivery to subscriber

Not applicable.

6.1.3 Public key delivery to certificate issuer

Public keys are provided by the subscriber via PKCS#10 and via secured communication channels.

6.1.4 CA public key delivery to relying parties

All CA certificates are published as described in Section 2.2. Additionally, all subscriber certificates are given to the respective subscriber including the corresponding Sub CA certificates of the trust chain.

6.1.5 Key sizes

Only RSA keys with a minimum length of 2048 bits and a modulo length divisible by 8 are generated (CA, RA) or accepted (end user). For key pairs used beyond 2025, a minimum length of 3072 bits applies.

Only EC keys that lie on the NIST P-256 or NIST P-384 curves are used and accepted.

6.1.6 Public key parameters generation and quality checking

For RSA keys, it is checked that the value of the exponent is an odd number greater than or equal to 3 and is in the range 2^{16} and 2^{256}-1, and that the modulus is an odd number that is not the power of a prime and has no factors less than 752.

EC keys are checked to be a normalized point that lies on the desired curve, is a multiple of the generator point, and is not the point at infinity of the curve.

6.1.7 Key usage purposes

All certificates contain a keyUsage and ExtendedKeyUsage with entries corresponding to section 7.1.2. These specify the intended and allowed usages of the corresponding keys.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

CA keys are generated and operated exclusively in HSMs that are certified according to FIPS 140-2 Level 3 and are also operated within that mode.

RA keys are generated and operated exclusively in certified and cryptographically secure SmartCards.

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

Private CA keys can only be generated, backed up and restored using the dual control principle, see Chapters 6.1.1, 6.2.4 and 6.2.8. Authentication tokens are used to import and export the keys to and from the backup HSMs and enforce the multi-person principle.

6.2.3 Private key escrow

Private CA keys are not stored outside the Telekom Security Trust Center.

6.2.4 Private key backup

As part of the key generation ceremony (see Section 6.1.1), the private CA keys are copied exclusively to backup HSMs, which are kept at a comparable security level to the HSMs in operation.

6.2.5 Private key archival

An archival of private CA keys is not supported.

6.2.6 Private key transfer into or from a cryptographic module

Private CA keys are only transferred for the purpose of backing up or restoring backup HSMs (see section 6.2.4). The work steps are performed as part of a key ceremony and under at least dual control.

6.2.7 Private key storage on cryptographic module

Private CA keys are generated, stored and used exclusively in HSMs.

Storage outside the operational HSM or backup HSM is not possible.

6.2.8 Method of activating private key

HSMs with private CA keys can only be activated using the dual control principle because the passwords for activation are divided between two people in different roles. Compliance with the dual control principle is monitored and logged by an auditor.

6.2.9 Method of deactivating private key

A deactivation of private CA keys is performed by persons in trusted roles using the functions provided by the HSMs.

6.2.10 Method of destroying private key

Private CA keys are destroyed when they are no longer needed or when the associated certificates have expired or been revoked.

Keys are destroyed in the same way as they are generated in a key ceremony (see chapter 6.1.1) and all copies of the keys are taken into account. Keys are destroyed using the HSMs' on-board resources.

When cryptographic modules are decommissioned at the end of their useful life or due to a defect, all private keys stored in these modules are destroyed as described above. 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.

6.2.11 Cryptographic module rating

See section 6.2.1.

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

All keys are only used as long as they are considered sufficiently secure in accordance with Chapters 6.1.5 and 6.1.6, including the algorithms used for certificate signing.

To ensure uninterrupted operation, a follow-up certificate is issued in good time before the expiry of a CA certificate or the end of the usability of the keys.

TLS server certificates are issued with a maximum validity period of 397 days.

The end of validity of any certificate does not exceed the end of validity of the issuing CA certificate ("shell model").

6.4 Activation data

6.4.1 Activation data generation and installation

When an HSM or a new partition of an HSM is put into operation, the passwords for activation are assigned in the multi-person principle in such a way that each person is only in possession of a fraction of the entire password.

6.4.2 Activation data protection

The activation data is always known only in parts to the relevant persons (see Section 6.4.1). In case of an emergency, the individual parts of the activation data are stored securely in different places to which no person has sole access.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The Trust Center uses only trustworthy systems that guarantee the technical security and reliability of the processes supported by the systems. All systems for certificate management as well as status and directory services are taken into account in the Trust Center's risk management and protected according to their criticality or damage potential.

All systems are hardened in accordance with Group-wide specifications or best practices, i.e., accounts, services, protocols, and ports that are not required are deactivated. In addition, systems are provided with integrity protection to guard against viruses, other malicious code, and the import of unauthorized software. Utilization and available resources are monitored to ensure uninterrupted operation. These and other security measures are described in a security concept.

The administration systems used to implement the security policies are used exclusively for this and no other purposes.

The required separation of trusted roles (see chapter 5.2.4) is technically supported by all necessary systems. In particular, the accounts of the trusted roles required for the operation of the critical systems (see chapter 5.2.1) are managed in such a way that access to the systems and data is restricted to the persons identified and authenticated for these roles (see chapter 5.2.3) with the minimum required authorizations. This includes the use of personalized accounts. All accounts are reviewed on a regular basis, at least every three months, and modified or deleted as needed within a reasonable time.

Accounts are protected with multi-factor authentication or strong passwords in accordance with current best practices, including adhering to the requirements of the CAB Forum Network Security Guidelines [NSG].

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

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

Group-wide processes have been established to ensure that security requirements for the development of PKI components are taken into account.

The Trust Center's development, test and production environments are operated on different hardware in different network segments and are therefore completely separate from one another.

6.6.2 Security management controls

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

All changes that affect the defined security level are approved in advance by the Trust Center management.

The integrity of the systems, including their relevant (configuration) settings, is continuously monitored for changes. In the event of changes that were not made on the basis of an authorized change, the resulting alerts are followed up by qualified personnel.

Systems log, to the extent possible, all security-related events. This includes monitoring systems for the following activities (including appropriate alerting functions):

- Security-relevant system events, which include:
  - successful and unsuccessful attempts to access the certificate systems
  - activities performed on the certificate and security systems
  - starting and shutting down of the logging functions
- Availability and usage of required services
- Changes to security profiles
- Installation, updating and removal of software on a certificate system
- System crashes, hardware failures, and other anomalies
- Firewall and router activities
- Ingress and egress into and out of certificate management system operations rooms
- The Trust Center's vulnerability management system is designed to ensure that
- Security patches are applied in a reasonable 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.

Telekom Security monitors the capacity requirements of the systems to ensure that adequate processing power and storage capacity are permanently available.

Data backups are tested regularly to ensure that they meet the requirements of the emergency plan. The data backup and restore functions are performed by the designated trusted roles.

6.6.3 Life cycle security controls

The usage of cryptographic keys and algorithms is based on continuously improved company-wide regulations and on the recommendations of established institutions like BSI or SOGIS.

6.7 Network security controls

The internal networks and systems are protected against unauthorized access and attacks with the help of multi-level firewalls, IDS and IPS, zoning and other protective measures. All network components are configured in such a way that only the minimum required protocols, services and accesses are available.

The segmentation of the network is based on a risk assessment taking into account the functional, logical and physical (including location) relationships between trusted systems and services.

All systems critical to CA operations are placed in secure or highly secure zones. Communications between systems within the security zones are protected by appropriately implemented and configured security procedures.

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

Firewalls are implemented between the zones, protecting systems and communications within the secure zones as well as communications with systems outside the zones. Connections are restricted to allow only those required for operation. Connections not required are explicitly prohibited or disabled.

The configurations of the systems are checked for compliance with these rules at regular intervals and as required.

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

Communication between all trusted as well as other systems is generally encrypted on multiple layers and is implemented for almost all systems, but at least for the trusted systems, via trusted channels that are logically distinct from other communication channels and ensure secure identification of their endpoints.

All external network connections are redundant.

The networks used to administer the systems are separated from the operational networks.

After each significant system or network change, an automated vulnerability check is performed within one week, but at least once per quarter, on public and private IP addresses identified by the Trust Center. Vulnerability testing will be performed and documented by individuals or organizations with the skills, tools, abilities, ethics, and independence necessary. The performance of a vulnerability assessment, indicating the qualifications of the person or organization performing the assessment, is controlled by the ISMS and documented along with the results.

Penetration tests are performed on the systems at the time of commissioning and at least once a year or after significant changes to the infrastructure or applications. Penetration testing will be performed and documented by individuals or organizations with the skills, tools, abilities, ethics, and independence necessary. The performance of the penetration tests, indicating the qualifications of the person or organization performing the tests, is controlled by the ISMS and documented along with the results.

Once a critical vulnerability has been identified, it is remediated within 48 hours unless there are good reasons not to remediate the vulnerability. If remediation is not possible within 48 hours, a plan for mitigating the vulnerability, including prioritization of activities, is prepared and processed within the timeframe specified therein. If it is decided not to fix a vulnerability, the justified decision is documented in the ISMS.

6.8 Timestamping

All systems are regularly synchronized with exact time information via a time server.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

The certificate profiles described below apply to all certificates issued as of the start of validity of this CPS. Certificates that have already been issued retain their validity unless explicit reference to their invalidity is made (legacy).

All certificate profiles comply with RFC5280 and the recommendations of ITU-T X.509.

All certificates are assigned, in regard to the corresponding issuing CA, a unique serial number, that has been generated by a cryptographically secure pseudo random number generator with an entropy of 126 bit.

7.1.1 Version number

All X.509 certificates are issued in version 3.

7.1.2 Certificate extensions

TLS server certificates contain the following certificate extensions:

- **authorityKeyIdentifier:** contains the subjectKeyIdentifier of the issuing CA
- **subjectKeyIdentifier:** contains „keyIdentifier“ according to RFC5280 #4.2.1.1.
- **keyUsage:** (critical) „digitalSignature“ and for RSA (optional) “keyEncipherment”
- **basicConstraints:** (critical)
  - **„cA“:** „false“
  - **„pathLenConstraint“:** not present
- **CertificatePolicies:** according to section 7.1.6
- **subjectAltName:** contains at least one FQDN
- **extendedKeyUsage:** „id-kp-serverAuth“ and (optional) „id-kp-clientAuth“
- **cRLDistributionPoints:** contains http-URL of corresponding CRL
- **authorityInfoAccess:** contains corresponding http-URLs for accessMethod 1.3.6.1.5.5.7.48.1 (ocsp) and accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers)

7.1.3 Algorithm object identifiers

Telekom Security only uses the following algorithms for signing certificates:

- sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)
- sha384WithRSAEncryption (OID 1.2.840.113549.1.1.12)
- sha512WithRSAEncryption (OID 1.2.840.113549.1.1.13)
- RSASSA-PSS (OID 1.2.840.113549.1.1.10)
  - MGF-1 with SHA-256 and a salt length of 32 bytes
  - MGF-1 with SHA-384 and a salt length of 48 bytes
  - MGF-1 with SHA-512 and a salt length of 64 bytes
- ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)
- ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3)

Certificates for RSA keys contain the OID 1.2.840.113549.1.1 (rsa-Encryption) in the subjectPublicKeyInfo.

Certificates for ECDSA keys contain the OID 1.2.840.10045.2.1 (ecPublicKey) and additionally the OID 1.2.840.10045.3.1.7 (prime256v1) or 1.3.1.32.0.34 (secp384r1) of the used curve in the subjectPublicKeyInfo.

The encodings specified in the Mozilla Root Store Policy [MOZ] are adhered to.

7.1.4 Name forms

Domain validated TLS server certificates contain the following attribute:

- **commonName:** contains exactly one of the FQDNs listed in subjectAltName

Organization validated TLS server certificates contain the following attributes:

- **commonName:** contains exactly one of the FQDNs listed in subjectAltName
- **organizationName:** as verified (common abbreviations are allowed for names longer than 64 characters)
- **country:** as verified and according to ISO-3166-1
- **localityName:** as verified
- **postalCode:** as verified
- (Optional) **stateOrProvinceName:** as verified and according to ISO-3166-2
- (Optional) **streetAddress:** as verified

7.1.5 Name constraints

Name constraints are not present.

7.1.6 Certificate policy object identifier

Sub CA and subscriber certificates contain at least one OID of a corresponding Certificate Policy. TLS server certificates and Sub CA certificates for the issuance of TLS server certificates contain one of the following OIDs of the [BR]:

- 2.23.140.1.2.1 (Domain Validation)
- 2.23.140.1.2.2 (Organizational Validation)

In end entity certificates, the qualifier „cPSuri“ contains a reference to the repository of the Telekom Security Trust Center, in which this CPS is published.

7.1.7 Usage of Policy Constraints extension

The extension policyConstraints is not present.

7.1.8 Policy qualifiers syntax and semantics

The policyQualifier contains the relevant information of section 7.1.2 in compliance with RFC5280.

7.1.9 Processing semantics for the critical Certificate Policies extension

The extension certificatePolicies is not marked critical, it is therefore up to the relying parties to evaluate this extension.

7.2 CRL profile

All revocation lists are issued according to the provisions of RFC5280 and are signed by the respective CA itself.

7.2.1 Version number

All revocation lists are issued as X.509 version 2.

7.2.2 CRL and CRL entry extensions

Certificate revocation lists contain the following CRL extensions:

- **AuthorityKeyIdentifier**
- **cRLNumber**
- **expiredCertsOnCRL**

The CRL entry extension **reasonCode** is applicable. The following CRLReasons are supported:

- unspecified (0)
- keyCompromise (1)
- affiliationChanged (3)
- superseded (4)
- cessationOfOperation (5)
- privilegeWithdrawn (9)

The CRLReason keyCompromise (1) takes precedence over all other revocation reasons. Should no revocation reason be known, i.e. the CRLReason unspecified (0) applies, then the CRL entry extension reasonCode is not present.

7.3 OCSP profile

All OCSP responses are issued according to RFC6960 and are signed by a delegated OCSP-signer, whose certificate is issued by the corresponding CA. All OCSP-signer certificates contain the extension **id-pkix-nocheck** and have a validity period of 1 month.

In OCSP responses for certificates that have been revoked, the revocationReason field within the RevokedInfo of the CertStatus is present. The CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1 Version number

All OCSP are operated in version 1 according to RFC6960.

7.3.2 OCSP extensions

The **revocationReason** extension is set analogously to the reasonCode of the revocation lists (see chapter 7.2.2).

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

Certification audits are carried out annually by external auditors in accordance with section 8.4. The audit periods directly follow each other and form an uninterrupted sequence.

In addition, all key generations and certificate issuances for Root CAs and for those Sub CAs being within the scope of [BR] are monitored by external auditors.

Internal auditors also carry out monthly internal audits, which randomly select at least 3% of the TLS server certificates issued since the last audit.

8.2 Identity/qualifications of assessor

External audits as described in section 8.1 are performed by qualified auditors who possesses the following qualifications and skills:

- The auditors are independent form the subject of the audit.
- The auditors are capable of performing assessments that fulfil the criteria of an Eligible Audit Scheme according to section 8.4.
- The auditors are proficient in examining PKI technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function.
- The auditors are bound by law, government regulation, or professional code of ethics
- The auditors maintain Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.
- The auditors are accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403 and are members of the Accredited Conformity Assessment Bodies' Council (ACAB'c).

Internal auditors performing the tasks described in section 8.1 have long-term experience and sufficient expert knowledge in the areas of auditing, PKI technologies and processes.

8.3 Assessor's relationship to assessed entity

The Trust Center only hires external auditors that are independent of the Deutsche Telekom AG and the audited subject.

For internal auditors the segregation of duties according to section 5.2.4 is adhered to.

8.4 Topics covered by assessment

The Trust Service Public Certificate Services Platform including all corresponding CAs is being audited according to ETSI EN 319 411-1 in the then current version. Applied policies are:

- LCP in association with DVCP and OVCP

8.5 Actions taken as a result of deficiency

Findings that are violating [BR], [MSRP], [MOZRP], [GGLRP] or [APLRP] are communicated to the respective Root Programs immediately.

In addition, all findings in general are fixed as fast as possible in accordance with the periods defined by the Trust Center ISMS as well as other internal regulations and, in case of external audits according to ETSI, in accordance with the following periods based on the classification of the finding:

- Recommendation: Within 12 months
- NC-B: Within 3 months
- NC-A: Certification-preventing, immediate correction is necessary

8.6 Communication of results

The audit attestations made by external auditors for all CAs are published in the “Common CA Database” (CCADB) in a timely manner and within three months at the latest. In case of delays of more than three months, the Trust Center will provide an explanatory letter signed by the external auditor.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The amount of fees to be paid for issuance, renewal and management of certificates is regulated in the corresponding service descriptions.

9.1.2 Certificate access fees

No fees are charged for access to certificates.

9.1.3 Revocation or status information access fees

No fees are charged for accessing revocation and status information.

9.1.4 Fees for other services

No other services are offered which are associated with the levying of fees.

9.1.5 Refund policy

The reimbursement of fees is based on the statutory provisions of German law and is specified in the General Terms and Conditions.

9.2 Financial responsibility

9.2.1 Insurance coverage

Telekom Security has business and property liability insurance coverage through Deutsche Telekom AG. It is ensured that the requirements arising with regard to insurance coverage are met.

9.2.2 Other assets

As a wholly owned subsidiary of Deutsche Telekom AG, Telekom Security has the financial stability and resources required to operate in conformity with the Telekom Security CP, including a planned termination according to Section 5.8. A control and profit and loss transfer agreement has been concluded for this purpose, which stipulates that Deutsche Telekom AG assumes all losses incurred by Telekom Security.

9.2.3 Insurance or warranty coverage for end-entities

Not applicable.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

All information in the context of the Trust Service is considered confidential information unless it has been explicitly classified as non-confidential information in accordance with Chapter 9.3.2.

9.3.2 Information not within the scope of confidential information

All information mentioned in chapter 2.2 as well as all information in issued and published certificates are classified as public.

9.3.3 Responsibility to protect confidential information

Telekom Security is subject to the Group-wide guidelines of Deutsch Telekom AG for the protection of confidential information. All Telekom Security employees are obligated to observe and comply with the Group guidelines on handling confidential information.

Contractors or third parties are also contractually obligated to comply with the Group guidelines.

9.4 Privacy of personal information

9.4.1 Privacy plan

To comply with all requirements of the German “Bundesdatenschutzgesetz” [BDSG], Deutsche Telekom AG has defined company-wide guidelines for handling personal data and, analogous to the handling of confidential information (see Section 9.3.1), has also defined corresponding protection classes for personal data.

Telekom Security only collects personal data that is required to provide the service and does not use this data for any other purposes.

To protect personal data, appropriate technical and organizational measures are taken in the operation of the PKI services, including the registration processes, with those measures being regularly checked as part of a binding company-wide procedure. Successful completion of this procedure is a prerequisite for approval of operation under privacy law.

9.4.2 Information treated as private

All personal information that has not been published in certificate content or otherwise is treated as confidential information and protected in accordance with the German Federal Data Protection Act.

9.4.3 Information not deemed as private

Personal information that is not considered confidential is all information that must be made public in order to provide services (e.g., certificate contents).

9.4.4 Responsibility to protect private information

All Telekom Security employees are required to observe and comply with the company-wide guidelines and legal regulations on handling personal information. Contractors or third parties are also contractually obligated to comply with the requirements.

9.4.5 Notice and consent to use private information

Information treated as private according to section 9.4.2 are only processed after notifying the affected persons and receiving their consent.

9.4.6 Disclosure pursuant to judicial or administrative process

Telekom Security discloses the information deemed to be private pursuant to Section 9.4.2 in the course of legal or administrative proceedings if disclosure is ordered by law or by a decision of a court or administrative authority or serves to enforce legal claims.

9.4.7 Other information disclosure circumstances

Not applicable.

9.5 Intellectual property rights

The statutory regulations apply.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Telekom Security assures the representations and warranties of CAs as required in the Telekom Security CP section 9.6.1. In particular, Telekom Security assures reliable, trustworthy, non-discriminatory and legal operation of the service as well as compliance with

the Telekom Security CP. As far as possible, the services and products offered to end users are also made accessible to people with disabilities. If measures are not sufficient, the Trust Center additionally offers free telephone support to assist people with disabilities in applying for, accepting and revoking certificates.

9.6.2 RA representations and warranties

Telekom Security assures the representations and warranties of RAs as required in the Telekom Security CP section 9.6.2.

9.6.3 Subscriber representations and warranties

Telekom Security specifies the terms of use for subscriber certificates to the subscribers and has their acceptance confirmed by the before issuing the certificates. These terms of use take into account the representations, warranties and information to be provided as required in the Telekom Security CP section 9.6.3.

9.6.4 Relying party representations and warranties

There are no contractual agreements with trusting third parties. However, recommendations to trusting third parties are included in the terms of use in order to verify the trustworthiness of a certificate for the respective use case.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimer of warranties

Any warranty exclusions are regulated in the terms and conditions.

9.8 Limitations of liability

Telekom Security shall be liable pursuant to Article 13 of EU Regulation 910/2014 ("eIDAS") for any damage caused intentionally or negligently to a natural or legal person.

Any limitations of liability are described in the Terms of Use and comply with applicable law.

9.9 Indemnities

Any claims for damages against Telekom Security are regulated in the terms and conditions.

9.10 Term and termination

9.10.1 Term

This CPS applies from the effective date indicated on the cover sheet to all newly issued and, if applicable, already existing certificates, as long as it is not revoked or replaced by a new version.

9.10.2 Termination

See section 9.10.1.

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 CPS is subject to review based on changing requirements or relevant changes in operations, but at least annually. To this end, the Trust Center Compliance Team will periodically review the underlying requirements of the requirements sources referenced in the CP Appendix B for new versions as well as track relevant forums and mailing lists.

Changes to this CPS, as well as the annual review, are listed in the change history of this document and a new version number is assigned, even if no substantive changes occurred during the annual review. The release of new versions is done according to chapter 1.5.4.

In case of changes that affect the terms of use, these will be adapted accordingly and made available in a new version.

9.12.2 Notification mechanism and period

New versions of this CPS shall be published in accordance with Chapter 2.

New versions of the terms and conditions that could affect the acceptance of the service by the subscribers are announced in good time to the subscribers and, where applicable, assessment bodies and supervisory or other regulatory authorities.

9.12.3 Circumstances under which OID must be changed

If there are changes to this CPS that affect applicability, a new OID will be assigned.

9.13 Dispute resolution provisions

In the event of disputes, the parties involved shall reach agreement, taking into account any agreements reached, regulations and applicable laws.

9.14 Governing law

German law applies.

9.15 Compliance with applicable law

Telekom Security assures to comply with applicable law.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If any provision of this CPS is or becomes invalid or unenforceable, this shall not affect the validity of the remaining provisions of this CPS.

9.16.4 Enforcement

No stipulation.

9.16.5 Force Majeure

Telekom Security shall not be liable if, due to force majeure, the contractual performance is significantly impeded, or the proper execution of the contract is temporarily impeded or impossible.

9.17 Other provisions

No stipulation.