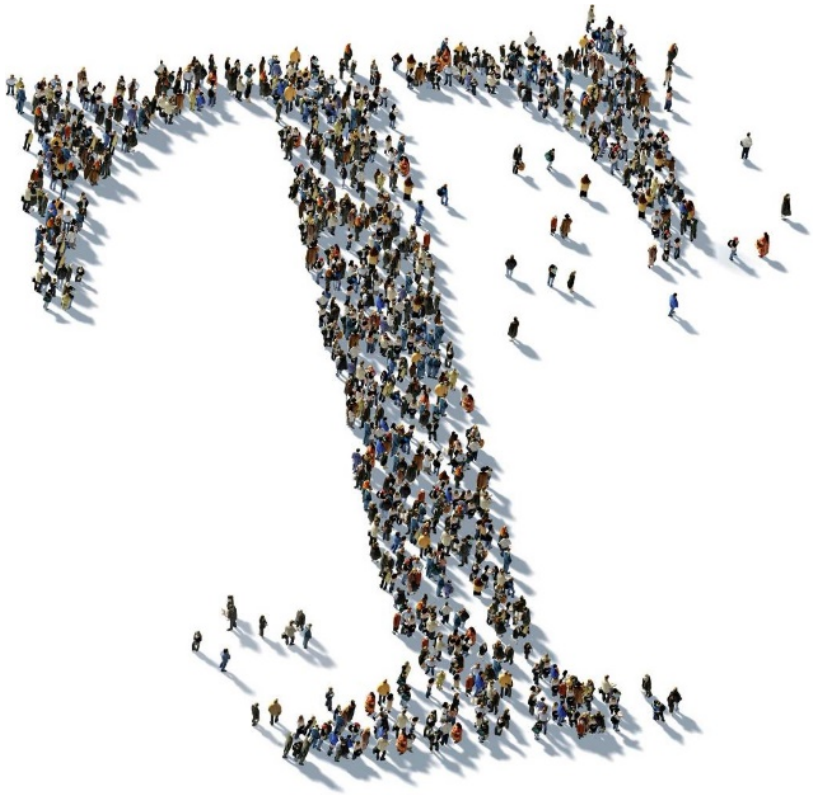
Deutsche Telekom Security GmbH
Root Certificate Practice Statement



Deutsche Telekom Security GmbH

Public

Version: 14.00

Valid: 30.04.2021

Status: release

Last review: 28.04.2021

IMPRINT

Table 1: Document properties

Property	Content
Issuer	Deutsche Telekom Security GmbH Trust Center & ID-Solutions Untere Industriestraße 20, 57250 Netphen, Germany
Filename	Telekom Security Root CPS EN V14.00.docx
Valid since	30.04.2021
Title	Root Certificate Practice Statement
Version	14.00
Last review	28.04.2021
Status	release
Contact	Telekom Security Leiter Trust Center Betrieb
Abstract	Root CPS

VERSION HISTORY

Table 2: Version history

Version	Date	Author	Changes
8.0	15.05.2018	T-Systems	Initial version after splitting CP & CPS document and changing the document structure conform to RFC 3647. A new version history has been started as older document versions base on a different document structure.
9.0	12.10.2018	T-Systems	Changes in sections 1.5.2, 4.9 and 5
10.0	10.10.2019	T-Systems	Update BR changes 1.5.7 to 1.6.6 Update EV changes 1.6.9 – 1.7.0
10.1 10.2	03.03.2020	T-Systems	Changes towards an accessible document template Changes according to Mozilla 2.7 requirements Changes according to BR 1.6.7 Changes according to EV 1.7.1
10.3	03.03.2020	T-Systems	Quality check
11.00	13.03.2020	T-Systems	Release of new version
11.01	05.06.2020	T-Systems	Changing T-System International GmbH to Deutsche Telekom Security GmbH
11.02	05.06.2020	T-Systems	Review
12.00	08.06.2020	T-Systems	Release
12.10	12.03.2021	Telekom Security	Adaption of new Telekom Security CP
12.11	12.03.2021	Telekom Security	Review
12.90	15.03.2021	Telekom Security	Formal QS
13.00	16.03.2021	Telekom Security	Release
13.10	28.04.2021	Telekom Security	Incorporation of MSRP 2.7.1 and diverse formal adjustments. Sections 4.9.12, 7.2.2, 7.3
13.11	28.04.2021	Telekom Security	Review
13.90	29.04.2021	Telekom Security	Formal QS
14.00	29.04.2021	Telekom Security	Release

TABLE OF CONTENT

LIST OF TABLES

1 INTRODUCTION

1.1 Overview

Deutsche Telekom Security GmbH (hereinafter referred to as Telekom Security) operates various Root Certificate Authorities (Root CAs) and Subordinate Certificate Authorities (Sub CAs) in its Trust Center for issuing certificates, both for customers and employees of Deutsche Telekom AG, as a Trust Service Provider (TSP).

This document is the Certificate Practice Statement (CPS) for the Root CAs of the Telekom Security Trust Center (in short: Root CPS). This CPS applies to all public Root CA certificates and supplements the CPS of the respective certification services issued below the public Root CAs.

The document describes, in the structure of RFC3647, the implementation of the requirements set in the Telekom Security CP with reference to the public Root CAs. In principle, the Telekom Security CP (OID 1.3.6.1.4.1.7879.13.42), the current version of the "CA/Browser-Forum Baseline Requirements" [BR] and the "CA/Browser-Forum EV-Guidelines" [EVCG] published at http://www.cabfourm.org as well as the ETSI EN 319 411-1 (in particular EVCP policy) and ETSI EN 319 411-2 are complied with. In the event of a conflict between this CPS, the Telekom Security CP and the referenced documents, the regulations from the referenced documents shall take precedence.

1.2 Document name and identification

This document is named „Telekom Security Root CPS“ and is identified by the OID 1.3.6.1.4.1.7879.13.39. 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 Root CPS (39)}

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

1.3 PKI participants

1.3.1 Certification authorities (CA)

The following Root CAs of Telekom Security are within the scope of this CPS:

Table 3: Root CA certificates in the scope of this CPS

Name	Key type	Serial number	Validity period	Fingerprint
T-TeleSec GlobalRoot Class 2	RSA 2048	01	2008-10-01 2033-10-01	590d2d7d884f40 2e617ea5623217 65cf17d894e9
T-TeleSec GlobalRoot Class 3	RSA 2048	01	2008-10-01 2033-10-01	55a6723ecbf2ecc dc3237470199d2 abe11e381d1

Telekom Security TLS ECC Root 2020	ECC 384	363a968cc95cb258cdd0015dc5e55700	2020-08-25 2045-08-25	c0f896c5a93b01062107da184248bce99d88d5ec
Telekom Security TLS RSA Root 2020	RSA 4096	0db6f3c9e660fb30b2119970a84b45b0	2020-08-25 2045-08-25	4513520839b22e20153c7b367a513ad2beaeda2a
Telekom Security ECC Root 2020	ECC 384	21b5a90c375f9871bf260a08f3f9c6f0	2020-08-25 2045-08-25	9bb84a99d51df08e1e3f9ab2a0629ca61b6ae00f
Telekom Security RSA Root 2020	RSA 4096	3db1afb04b9faa744a258f8189831579	2020-08-25 2045-08-25	c445da958e79728451c16245f548dbacc76fce07

1.3.2 Registration Authorities (RA)

The issuing of Root and Sub CA certificates is based on internal processes that ensure authenticity and integrity. The only registration authority is thus the Trust Center itself.

1.3.3 Subscribers

End-entity-certificates are not within the scope of this CPS.

1.3.4 Relying parties

Relying parties are persons or IT-processes that trust the certificates and use them for the verification of digital signatures.

Relying parties should check the revocation or status information according to section 4.9 before they trust a certificate.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The Root CAs are used exclusively for signing Sub CA certificates (incl. cross certificates) and OCSP signer certificates as well as for signing revocation lists.

1.4.2 Prohibited certificate uses

The Root CAs are not used for use cases other than those listed in Section 1.4.1.

1.5 Policy administration

1.5.1 Organization administering the document

Deutsche Telekom Security GmbH – Trust Center & ID-Solutions

Untere Industriestraße 20

57250 Netphen, Deutschland

1.5.2 Contact person

Contact person for this CPS is the Root Programm of the Trust Center.

- FMB_Trust_Center_Rootprogram@t-systems.com
- https://www.telesec.de/en/service/contact/request-information

Certificate misuse, key compromises, faulty or non-compliant certificates, other security-related certificate problems or suspicions of such incidents can be reported at

https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden/

or via

FMB_Trust_Center_Rootprogram@t-systems.com

This should include as much information as possible to enable verification of the problem. In the event of a compromise, this should include, for example, a CSR signed with the private key and the commonName “Key Compromise”.

1.5.3 Person determining CPS suitability for the policy

The Trust Center Root Programm 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

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

This CPS will be reviewed by the Trust Center Root Programm as required, e.g. due to changed requirements or relevant changes in operations, but at least once a year. Changes as well as the annual review are listed in the change history of this document. This also applies in the event that no substantive changes are made during the annual review. Each new version is approved by the Trust Center management, is given a new ascending version number and is published according to the specifications in section 2.2.

1.6 Definitions and acronyms

1.6.1 Definitions

See Telekom Security CP.

1.6.2 Acronyms

See Telekom Security CP.

1.6.3 References

See Telekom Security CP.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

As the Root TSP, Telekom Security operates a repository with information and documents for all Root and Sub CA certificates (see section 2.2) as well as certificate status services (see section 4.9 and 4.10).

2.2 Publication of certification information

Telekom Security publishes the following information or documents in the PKI repository on the Trust Center web pages (https://www.telesec.de/de/service/downloads/pki-repository/):

- Telekom Security CP
- Root CPS (this document)
- All still valid public Root CA certificates of Telekom Security
- All still valid Sub CA certificates issued by Telekom Security's public Root CAs
- The audit attestations for the public Root CA certificates of Telekom Security (link to the Auditor's web pages)

Both the CP and the Root CPS are compliant with RFC3647 and are published in German and English, both the valid version and all relevant superseded versions. The German and English versions of a document always have the same version number and are synchronized in terms of content. In case of dispute, however, the German version is authoritative.

In addition to publication in its own repository, Telekom Security publishes all required information on Root and Sub CA certificates in the "Common CA Database" (CCADB) in accordance with the CCADB policy (see https://www.ccadb.org).

The following test web pages are operated for all public Root CAs whose Sub CA certificates are used to issue TLS server certificates:

- a test web page with a valid TLS server certificate
- a test web page with an expired TLS server certificate
- a test web page with a revoked TLS server certificate

2.3 Time or frequency of publication

The information listed in section 2.2 is published as follows:

- The public Root CA certificates are published at the beginning of a Root inclusion in both the own repository and the CCADB.
- The Sub CAs below the public Root CAs are published in both the CCADB and the own repository within 7 days of their issuance and in any case before they are put into operation.
- The audit attestations are published or linked in both CCADB and own repository within 7 days of their issuance.

- The CP and Root CPS are published in the Trust Center's repository and communicated to the CCADB after the release of a new version, but no later than the start of the validity of a new version.

2.4 Access controls on repositories

Both the above-mentioned repository and the certificate status services are accessible from the Internet 24/7 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

See section 7.1.2 and section 7.1.4.

3.1.2 Need for names to be meaningful

Each Root and Sub CA certificate is given a CommonName which clearly indicates the affiliation of the CA with Deutsche Telekom Security GmbH or DFN.

3.1.3 Anonymity or pseudonymity of subscribers

Not applicable.

3.1.4 Rules for interpreting various name forms

See section 7.1.2 and section 7.1.4.

3.1.5 Uniqueness of names

Each Root CA certificate of Deutsche Telekom Security GmbH and all Sub CA certificates issued by a specific Root CA are assigned a unique CommonName and thus SubjectDistinguishedName.

3.1.6 Recognition, authentication, and role of trademarks

Not applicable.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The Root CA keys are generated as part of a root ceremony with multi-person principle under the supervision of an external auditor directly in connection with the generation of the corresponding Root CA certificate.

A CSR (Certificate Signing Request) signed with the private Key is required for the issuance of a Sub CA certificate.

3.2.2 Authentication of organization identity

An authentication of internal subscribers is not necessary.

The DFN has been authenticated upon conclusion of contract.

3.2.3 Authentication of individual identity

Internal subscribers are authenticated by the respective superior.

Applicants of the DFN are authenticated via an official identification document.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

Internal requests are approved by the authorized “Leiter VDA” (member of the management).

Applicants of DFN must present an authorization signed by a person authorized to represent DFN.

3.2.6 Criteria for interoperation

Telekom Security does not issue cross certificates for external organisations.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Not applicable.

3.3.2 Identification and authentication for re-key after revocation

Not applicable.

3.4 Identification and authentication for revocation requests

A revocation request signed by the operator of the Sub CA or the management of the Trust Center is required to revoke a CA certificate.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Eligible applicants for Root CA certificates are the representatives of the Trust Center Root Programm. The subject of the Root CA certificates is Deutsche Telekom Security GmbH.

Authorized applicants for Sub CA certificates are the operators of the respective certification services of Deutsche Telekom Security GmbH, Deutsche Telekom AG and representatives of DFN (Deutsches Forschungsnetz).

4.1.2 Enrollment process and responsibilities

The application for Root CA certificates is made by the Root Program in coordination with the management of the Trust Center, with the later also issuing the final approval.

To apply for a Sub CA certificate, the operators of the respective certification authority must submit

- a certificate request in PKCS#10 format (“Certificate Signing Request, CSR) and
- a signed application form

to the Trust Center Root Programm.

In the application form, the applicant confirms

- the correctness of the information provided and
- compliance with the requirements for generating the keys of a Sub CA

and provides, as a unique reference to the CSR, the CSR’s fingerprint.

Note: Certificate application forms in electronic form are accepted if they are signed with at least an advanced electronic signature of an authorized applicant.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Requests for issuance of Sub CA certificates are checked for completeness and whether they have been signed by an authenticated and authorized applicant in accordance with section 3.2.

4.2.2 Approval or rejection of certificate applications

Requests for the issuance of Sub CA certificates are checked by the Trust Center Root Programm for conformity with existing requirements. If necessary, additional required

documents (e.g., associated CPS) are requested. If all open questions are clarified and the check is successful, the request is forwarded by the Root Programm to the management of the Trust Center, which grants the final approval and thus release for certificate issuance.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Root and Sub CA certificates are issued at the so called Trust Center Offline CA in accordance with a defined ceremony. The following points, among others, are covered during that ceremony:

- Available application forms are checked for completeness and valid signatures.
- The CSR provided for the issuance of a Sub CA, as well as its fingerprint, will be compared and validated against the information provided in the application.
- At least a six-eye principle is adhered to, and even at least an eight-eye principle when generating Root CA keys and certificates.
- Knowledge of activation data is always distributed among two people in different trusted roles.

4.3.2 Notification to subscriber by the CA of issuance of certificate

After the issuance of a Root- or Sub CA certificate, the applicant is notified and the certificate is provided via the agreed method.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

After issuing a Sub CA certificate, the respective operator of the Sub CA has a maximum period of 7 days to check the new certificate for correctness and accept it. If the certificate is rejected or no feedback is received within the agreed period, the certificate will be revoked.

4.4.2 Publication of the certificate by the CA

See section 2.3.

4.4.3 Notification of certificate issuance by the CA to other entities

See section 2.3.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The keys of the Root and Sub CAs are used exclusively during the validity period of the corresponding Root and Sub CA certificates for the permitted purposes listed in Section 1.4.1 and only as long as they are not revoked. After the validity period expires or after revocation, the keys are destroyed.

4.5.2 Relying party public key and certificate usage

Relying parties are required to use the Root and Sub CA certificates to validate the entire certificate chain of an end-entity certificate.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

A renewal of CA certificates is not supported.

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

A re-key of CA certificates is not supported.

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-key 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

A modification of CA certificates is not supported.

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

Root CA certificates will not be revoked. If necessary, their trust is withdrawn by removing them from the root stores as well as the CCADB

A Sub CA certificate is revoked if

- a written revocation request has been submitted by the operator of the Sub CA, even without giving reasons,
- it is determined that the original certificate request was not authorized and cannot or should not be authorized retroactively,
- it is determined that the private key of the Sub CA has been compromised or disclosed to an unauthorized person or an organization that is not associated with the Sub CA or no longer meets the requirements (see Section 6.1.5 and 6.1.6),
- it is determined that the certificate has been misused,
- it is determined that the Sub CA certificate was not issued in compliance with this CP or that the operator of the Sub CA is not operating in compliance with this CP,
- it is determined that any information in the certificate is incorrect or misleading,

- the operation of the Root CA or the Sub CA is terminated and no arrangements have been made for the continuation of the revocation service,
- the right of the Root- or Sub CA to issue certificates in accordance with the requirements of this CP expires or is revoked or terminated and no arrangements have been made for the continued operation of the revocation services, and
- legal regulations, judicial rulings or an instruction from a supervisory authority exist.

Revoked certificates will not be reinstated.

4.9.2 Who can request revocation

Revocation of a Sub CA can only be requested by an authorized representative of the respective operator. If one of the reasons for revocation listed in Section 4.9.1 is determined by the Trust Center or made known to the Trust Center by a third party and verified by the Trust Center, revocation of the affected Sub CA certificate is initiated.

4.9.3 Procedure for revocation requests

The revocation of a Sub CA certificate can be requested by the operators of the certification authorities or by the management of the Trust Center with a legally signed revocation request.

Note: Certificate revocation requests in electronic form are accepted if they are signed by at least an advanced electronic signature of an authorized applicant.

In addition, the Trust Center also offers an interface for reporting problem messages about certificates (also from third parties) (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 about the receipt of the message and any resulting revocations of the affected certificates.

After a Sub CA certificate is revoked, the certificate holder is informed and the CCADB is updated by Telekom Security within 7 days or, in the case of a security incident, within 24 hours.

4.9.4 Revocation request grace period

The operator of a Sub CA is obligated to submit a revocation request without delay if 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 a reason for revocation in accordance with Section 4.9.1, a Sub CA certificate is generally revoked within a reasonable period of time, taking into account the circumstances (existing and emerging security risks, effort required, etc.). For Sub CAs issuing TLS server certificates under the baseline requirements, a maximum period of 7 days applies. This includes the publication of the revocation status in the certificate status services.

Exceptions are revocations that are requested for a later date. In this case, the desired date for revocation of the certificate listed in the revocation request is decisive.

4.9.6 Revocation checking requirements for third parties

Trusting third parties are required to query the status of certificates using the certificate status services offered by the Trust Center as described in Section 4.10 before trusting a certificate.

4.9.7 CRL issuance frequency

Revocation lists of Root CAs, which provide information about revoked Sub CAs (Certificate Authority Revocation List (CARL)), are updated within 24 hours after a Sub CA certificate has been revoked and regularly every 3 months.

4.9.8 Maximum latency for CRLs

Newly issued CARLs are published within 24 hours on the repositories.

4.9.9 Online revocation/status checking availability

In addition to the revocation lists mentioned above, online status information for all certificates is also provided via OCSP. The "Authority Information Access" certificate extension of each Sub CA certificate contains the URL of the relevant OCSP responder.

4.9.10 Online revocation checking requirements

Third parties are encouraged to consider the specifications for processing OCSP responses according to RFC6960 when checking a certificate status via OCSP.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

Parties that want to report a key compromise are requested to use the contact options described in Section 1.5.2. They have to provide sufficient information or references to information that is proof for a compromise, e.g. provide a CSR signed by the compromised private key with a commonName of "Compromised Key". The effected certificate itself should be referenced as well.

4.9.13 Circumstance for suspension

A suspension of Sub CA certificates is not supported.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspenion request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

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

4.10.1 Operational characteristics

All certificate status information (revocation lists and OCSP) are regularly time-synchronized (UTC) prior to the generation (also see section 5.4.1). Taking into account the different update periods of both methods, the status information provided by revocation lists and OCSP information is consistent after 24 hours at the latest.

4.10.1.1 Operational characteristics for the provision of OCSP-Responders

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

OCSP responses to the status of a Sub CA certificate have a validity of 5 days. They are retained for 120 minutes after a request and reused for further requests, provided the status of the requested certificate does not change during this time.

After a Sub CA certificate has been revoked, updated information can be retrieved from the OCSP responder within 24 hours.

4.10.1.2 Operational characteristics for the provision of CRLs

Revocation lists for Sub CA certificates (CARL) are issued every 3 months and have a validity period of 6 months.

Revoked certificates are not removed after their validity period ends.

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 6 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 leads to a revocation of certificates, the provisions described in section 4.9.1ff shall 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 practices

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 all other areas by additional enclosures and are audited and certified to "Trusted Site Infrastructure TSI V3.2 Dual Site".

Note: The so called Offline CA for the Root CAs is located at another secure site outside the data centers. However, the statements listed below also apply to the location of the Offline CA.

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. No media will be used for permanent or long-term storage or archiving.

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.

5.1.8 Off-site backup

No stipulation.

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, is responsible for vulnerability scans and penetration tests, manages the ISMS
- ISMS team member: supports the information security officer in his tasks

- Administrator: configures and maintains the IT infrastructure (networks, databases, servers, etc.)
- CA Operator: generates Root CA keys and certificates
- Internal auditor: audits certificates, processes, documentation, and ceremony compliance on a regular basis and in the event of inconsistencies
- Root Programm/Compliance Team (PKI): 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, processes applications for CA issuances

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 -critical activities for which dual control (or more) is required are:

- CA key generation, backup and recovery
- any activities on 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)
- processing of requests for CA certificates
- 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
- Administrator/CA operator

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.

5.3.3 Training requirements

See section 5.3.1.

5.3.4 Retraining frequency and sequence

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

5.3.5 Job rotation frequency and requirements

Job rotations are not applied.

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 the Root CA.

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,
- background checks and
- training and awareness measures.

5.4 Audit logging procedures

5.4.1 Types of events recorded

5.4.1.1 Activities of persons

All activities of Trust Center staff related to the Root and Sub CA certificate and key lifecycle (key generation, storage, backup, recovery and destruction, issuing and revocation of Root and CA certificates, and HSM lifecycle) are recorded.

5.4.1.2 Technical events

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

- all significant certificate and key management events
- all security events on the systems, including but not limited to changes in system security policies, system startup and shutdown, system crashes and hardware failures, clock synchronization events, firewall and router activity, and PKI system access attempts
- all OCSP requests for unassigned serial numbers

In addition, all (physical) entries and exits to/from the security zones are logged.

5.4.2 Frequency of processing log

The events listed in section 5.4.1.1 are logged in the respective ceremonies.

The events listed in section 5.4.1.2 are logged continuously by the systems (in the systems of the Offline CA only as long as they are in operating during a ceremony).

The records of the activities listed in section 5.4.1.1 are only evaluated on demand, e.g. in the event of problem reports, in legal proceedings or at the request of internal and external auditors.

The log data for the events listed in section 5.4.1.2 are evaluated as follows:

- Security-relevant events on the online systems are evaluated as described in section 6.6.2.
- All other log data is evaluated only when necessary, e.g., for troubleshooting or analysis activities.

5.4.3 Retention period for archive

The records of the activities listed in section 5.4.1.1 are retained for 7 years beyond the validity of the respective Root CA certificate. This also applies when a service is terminated.

5.4.4 Protection of audit log

The records of the activities listed in section 5.4.1.1 at the Offline CA are kept confidential and integrity-secured and protected against destruction and deletion. In the case of paper applications or minutes, this is done in the Trust Center's secure paper archive. In the case of electronic applications (signed PDF), this is done in secure and permanently available electronic repositories approved for this purpose.

Technical system events of the online systems according to section 5.4.1.2 are immediately sent to a separate and tamper-proof log appliance.

5.4.5 Audit log backup procedures

See section 5.4.4.

5.4.6 Audit collection system

Immediately after generation, any log data of technical events of the online systems are sent to a central and integrity-protected system (log appliance), which is specifically designed for the collection and backup of log data.

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 achived

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 time-stamping 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 as well as the records of the activities listed in section 5.4.1.1 are 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 changeober

See section 6.3.2.

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.

If an incident represents a violation of a Root Store Policy, the Trust Center Root Programm 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

See section 5.7.1.

5.7.3 Entity private key compromise procedures

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

5.7.4 Business continuity capabilities after a disaster

See section 5.7.1.

5.8 CA or RA termination

Telekom Security has a continuously updated termination plan.

In the event of termination of a Root CA's operation, Telekom Security plans to inform the operators of the affected Sub CAs in good time so that they in turn can inform their end customers in good time and migrate their services, including their end customers, to another Telekom Security Root CA or another operator before the Root CA's operation is ceased, if possible, and thus avoid possible disruptions for end subscribers.

A planned termination will be published on the Trust Center's web pages at an early stage so that third parties can inform themselves in good time. In addition, the affected rootts store operators will be explicitly informed.

All Sub CA, cross and end-entity certificates not yet revoked at the time of the planned termination of a Root CA are revoked before the Root CA is finally terminated.

For terminating, the private keys of the Root CA are deleted as described in section 6.2.10.

Operation of the status services will be handed over to Deutsche Telekom AG, which acts as the trust service provider in accordance with the German “Vertrauensdienstegesetz”, until the validity of all end user certificates expires. Likewise, the archived records will be handed over to Deutsche Telekom AG for safekeeping until the specified retention period expires.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Note: Since the Root CA does not generate keys for Sub CAs and end entities, the generation of such keys is not discussed here and instead reference is made to the CPSs of the respective operator, which describe the implementation of the relevant requirements from the Telekom Security CP. For information on how the Root TSP checks compliance with the requirements for generating the keys of a Sub CA, please refer to Section 4.3.

The keys of a Telekom Security Root CA are generated in an HSM in accordance with section 6.2.1 at the Offline CA in the secure environment of the Trust Center as part of a Root CA ceremony, in which the Root CA certificate is also generated immediately after the keys are generated. The prerequisite for the generation of the keys is thus that an approved application for the issuance of a Root CA certificate is available, see Section 4.1ff. on this subject.

The trusted roles involved in the ceremony and their tasks before, during and after the key ceremony are described in a work instruction. It also specifies which steps must be performed by different roles for key generation and backup in a multi-person process. These include

- starting the Offline CA and the HSM, including the integrity check of the system,
- the activation of the HSM by means of shared activation data,
- the backup of the keys to multiple backup HSMs using split tokens ("n of m"),
- the shutdown of the Offline CA and HSM including integrity protection of the system,
- separate storage of tokens to restore keys from backup ("n of m").

The root ceremonies are supervised by both a qualified internal auditor and a qualified external auditor of a conformity assessment body (see section 8.2). After correct performance of the ceremony, the internal auditor confirms this in the minutes of the ceremony. In addition, the conformity assessment body issues an audit attestation letter.

6.1.2 Private key delivery to subscriber

Not applicable since the private keys of Root CAs are operated exclusively in the HSM of the Offline CA in which they also have been generated. The only exception to this is a backup on backup HSMs and, if necessary, an import to a new HSM in the event of a defect.

6.1.3 Public key delivery to certificate issuer.

Not applicable since the Root CA generates its own keys.

6.1.4 CA public key delivery to relying parties

All Root and Sub CA certificates are published as described in Section 2.2.

6.1.5 Key sizes

For Root CAs, only RSA keys with a key length of 4096 bits and a length of the module divisible by 8 or EC keys of the curve secp384r1 (NIST P-384) are used.

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

The private keys of Root CAs are exclusively used for signing Sub CA certificates, cross certificates, delegated OCSP-Signer certificates and revocation lists.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

The Root 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.

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

The generation and use of the private Root CA keys in the HSM and the restoring of the keys from a backup HSM are only possible under the dual control principle, see Section 6.2.4 and 6.2.8. Authentication tokens are used to import and export the keys to and from the backup HSM, implementing the "n of m" principle.

6.2.3 Private key escrow

Private keys of the Root CAs are not stored outside the Telekom Security Trust Center.

6.2.4 Private key backup

The private keys of the Root CAs are copied exclusively to two backup HSMs, which are kept under a comparable security level, as part of the key generation ceremony (see section 6.1.1). Access to the backup HSMs for restoring the keys to an HSM is only possible via authentication

tokens based on the "n of m" principle. The tokens are issued to multiple employees in different trusted roles and are stored securely separately from one another.

6.2.5 Private key archival

An archival of private keys for Root CAs is not supported.

6.2.6 Private key transfer into or from a cryptographic module

The private keys of the Root CAs are saved in backup HSMs (see Section 6.2.4) and can only be restored into other compatible HSM via these backup HSMs.

6.2.7 Private key storage on cryptographic module

The private keys of the Root CAs are generated, stored and used exclusively in HSMs or backup HSMs (see Section 6.1.1, 6.2.4 and 6.2.6).

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

6.2.8 Method of activating private key

The HSMs with the private keys of the Root CAs 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

The HSMs with the private keys of the Root CAs are deactivated and shut down at the end of each root ceremony using the dual control principle. Compliance with the dual control principle is monitored and logged by an auditor.

6.2.10 Method of destroying private key

The private keys are destroyed at the end of the life cycle of the corresponding Root CA certificate, i.e., when the validity period expires or the service is put out of operation or terminated, and are not used any further. Like the generation of Root CA keys, the destruction of the keys takes place in a ceremony in the presence of the auditors (see Section 6.1.1) and takes into account all copies of the keys.

The keys are destroyed using the on-board means of FIPS 140-2 Level 3 certified HSMs.

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

Root CA certificates are issued with a validity period of 25 years. However, the keys are only used as long as the algorithms can be considered sufficiently secure. In addition, the keys are taken out of service prematurely if necessary due to other reasons (e.g., replacement of the Root CA certificate or termination of operation).

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

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 assigns only a part 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

Note: The certificate management system of the Root CA is operated as a pure Offline CA without any network connection to outside the system. However, the status services of the Root CA (revocation lists, OCSP) are available online. Accordingly, the following explanations

apply only conditionally to the Offline CA and in part only concern the systems of the status services available online.

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 and the status and directory services are taken into account in the Trust Center's risk management and are protected according to their criticality or potential for damage.

The required separation of trusted roles (see Section 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 section 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 section 5.2.3) with the minimum required authorizations. All accounts are reviewed on a regular basis, but at least every 3 months, and modified or deleted as necessary within a reasonable time.

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

The CA, certificate management, security and front-end systems and, if applicable, other internal systems to support operations are hardened by default in accordance with company-wide specifications or best practices, i.e., accounts, services, protocols and ports not required for the operation of the CAs are deactivated.

Telekom Security systems are provided with integrity protection to guard against viruses, malicious code and the import of unauthorized software, and are monitored in terms of utilization and available resources to ensure uninterrupted operation. These and other security measures for Trust Center systems are described in the security concepts.

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

The development, test and production environments of the Trust Center are operated on different hardware in different network segments and are therefore completely separate from each other.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

Note: The certificate management system of the Root CA is operated as a pure Offline CA without any network connection to outside the system. However, the status services of the Root CA (revocation lists, OCSP) are available online. Accordingly, the following explanations apply only conditionally to the Offline CA and in part only concern the systems of the status services available online.

6.6.1 System development controls

Telekom Security maintains a regular and close exchange with the software supplier of the Offline CA and has developed the OCSP systems for status information itself, so that consideration of the security requirements is ensured during system development for both certificate management and status services.

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 Trust Center's vulnerability management is regulated to ensure that

- security patches are applied within 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, and
- the reasons for not applying security patches are documented.

To the extent possible, the systems log all security-related events. This includes monitoring 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 logging functions,
- availability and use 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
- entries and exits to and from certificate management system operating rooms

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 alarm messages are followed up by qualified personnel.

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, SOGIS etc.

6.7 Network security controls

Note: The certificate management system of the Root CA is operated as a pure Offline CA without any network connection to outside the system. However, the status services of the Root CA (revocation lists, OCSP) are available online. Accordingly, the following explanations apply only conditionally to the Offline CA and in part only concern the systems of the status services available online.

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.

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

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.

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, significant changes to the infrastructure or applications, but at least once a year. 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 usually remediated within 4 days unless there are good reasons not to remediate the vulnerability. If remediation is not possible within 4 days, 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 Time-stamping

The time information of the Offline CA is checked at the beginning of each ceremony to ensure that the certificates and revocation lists are signed with the correct time information.

The systems of the OCSP responders are regularly synchronized with reliable time information via the time server according to Section 5.5 so that the OCSP responses are signed with the correct time information.

7 ZERTIFIKATS-, SPERRLISTEN- UND OCSP-PROFILE

7.1 Zertifikatsprofile

The certificate profiles described below apply to all Root and Sub CA 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 issued by a Root CA are assigned a unique, random serial umber with a length between 64 and 126 bit.

7.1.1 Version number

All X.509 certificates are issued in version 3 (with value “2”).

7.1.2 Certificate extensions

The Root CA certificates of Telekom Security only contain the following certificate extensions:

- subjectKeyIdentifier:
  The extension subjectKeyIdentifier contains the “keyIdentifier” according to RFC5280 #4.2.1.1 and is not marked critical.
- keyUsage:
  The extension keyUsage contains the values “keyCertSign” and “cRLSign” and is marked critical.
- basicConstraints:
  The extension basicConstraints contains the value of “cA”-Flag as “true”, does not contain a maximal pathlen and is marked critical.

The Sub CA certificates issued by Root CAs of Telekom Security contain the extensions described above. In addition, they contain the following certificate extensions:

- authorityKeyIdentifier:
  The extensions authorityKeyIdentifier contains the value of the subjectKeyIdentifier of the issuing Root CA certificate and is not marked critical.
- CertificatePolicies (optional, obligatory only for TLS):
  The extension certificatePolicies of Sub CA certificates used for issuance of TLS server certificates at least contains the corresponding Policy-OID of the Baseline Requirements [BR].
- ExtendedKeyUsage:
  The extension extendedKeyUsage is not marked as critical and contains the following values:
  - Sub CA certificates used for issuance of TLS server certificates only contain „id-kp-serverAuth” and optionally “id-kp-clientAuth”.
  - Sub CA certificates used for issuance of S/MIME certificates only contain „id-kp-emailProtection” and optionally “id-kp-clientAuth”.

- cRLDistributionPoints:
  The extension cRLDistributionPoints contains at least one http-URL pointing to the CARL of the Root CA that issued the Sub CA certificate. Additional URLs can be included if desired by the operator of the Sub CA.
- authorityInfoAccess:
  The extension authorityInfoAccess contains at least one http-URL pointing to the OCSP-Responder of the Root CA that issued the Sub CA certificate (accessMethod 1.3.6.1.5.5.7.48.1 (ocsp)).
  Sub CA certificates for issuance of TLS server certificates additionally contain a http-URL for a distribution point of the Root CA certificate (accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers)).
  Additional URLs can be included if desired by the operator of the Sub CA.
- subjectAltName (optional):
  If desired by the operator of the Sub CA, the extension subjectAltName contains a validated value.

The extension nameConstraints is not used because Telekom Security currently does not operate any technically constrained CAs.

7.1.3 Algorithm object identifiers

Telekom Security uses the following algorithms for signing Root and Sub CA 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)

7.1.4 Name forms

Telekom Security only includes the following attributes in the subjectDN of Root and Sub CA certificates:

- commonName
- organizationName
- countryName

If needed, OCSP-Signer certificates issued by a Root CA additionally contain the attribute serialNumber in the subjectDN.

7.1.5 Name constraints

Name constraints are not set in Root and Sub CA certificates.

7.1.6 Certificate policy object identifier

If applicable, the following OIDs of the Baseline Requirements [BR] are used:

- 2.23.140.1.2.1 (Domain Validation)
- 2.23.140.1.2.2 (Organizational Validation)
- 2.23.140.1.2.3 (Individual Validation)
- 2.23.140.1.1 (Extended Validation)

7.1.7 Usage of Policy Constraints extension

The extension policyConstraints is not used.

7.1.8 Policy qualifiers syntax and semantics

The policyQualifier contain 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, so it is up to the decision of the certificate users 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

All revocation lists for CA certificates contain the CRL extension AuthorityKeyIdentifier and cRLNumber as well as the CRL entry extension reasonCode. The CRLReason is not marked as critical and chosen to indicate the most appropriate reason for revocation. Supported values are: keyCompromise (1), cACompromise (2), affiliationChanged (3), superseded (4), cessationOfOperation (5). Other CRLReasons are not applied.

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 Root CA. All OCSP-signer certificates contain the extension id-pkix-nocheck with value NULL and have a validity period of 3 months.

In OCSP responses for CA 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 singleExtensions of an OCSP response does not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

All Root CA certificates in the scope of this CPS and all Sub CA certificates issued by those Root CAs are publicly disclosed and audited according to the following sections.

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 so that no gap in the auditing exists.

In addition, all key generation and certificate issuances for Root CAs are monitored by external auditors. Sub CA certificates for the DFN are issued only if there is evidence that the associated key generation has been monitored by an external auditor and found to be compliant.

All activities at the Offline CA are monitored by an internal auditor. Sub CA certificates for the Trust Center (not for the DFN) are only issued if there is evidence that the related key generation has been monitored by an internal auditor and found to be compliant.

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.

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 Root CAs including associated processes, systems, infrastructures and organisational measures are part of an assessment in accordance with the current versions of ETSI EN 319 411-1 and ETSI EN 319 411-2. The following policies apply:

- T-TeleSec GlobalRoot Class 2: LCP, NCP, NCP+, DVCP, OVCP
- T-TeleSec GlobalRoot Class 3: EVCP, QCP-w
- Telekom Security ECC Root 2020: LCP, NCP, NCP+, OVCP
- Telekom Security RSA Root 2020: LCP, NCP, NCP+, OVCP
- Telekom Security TLS ECC Root 2020: DVCP, OVCP, EVCP, IVCP, QCP-w
- Telekom Security TLS RSA Root 2020: DVCP, OVCP, EVCP, IVCP, QCP-w

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 Root and Sub CAs are published in the “Common CA Database” (CCADB) in a timely manner and within 3 months at the latest. In case of delays of more than 3 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 issuing or renewing CA certificates is regulated in the internal and external contracts.

9.1.2 Certificate access fees

No fees are charged for access to CA 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

The amount of fees to be paid for other services is regulated in the internal and external contracts.

9.1.5 Refund policy

The refunding is regulated in the internal and external contracts.

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

Telekom Security protects confidential business information according to their classification.

9.3.1 Scope of confidential information

Telekom Security is subject to the company-wide guidelines of Deutsch Telekom AG for the protection of confidential information. All information is classified according to the following protection classes:

- open
- internal
- confidential
- confidential (customer)

For the purposes of this CPS, confidential information is all information that is not classified as "open" according to the above classification. This is all information that is not explicitly listed as "non-confidential" in section 9.3.2.

9.3.2 Information not within the scope of confidential information

For the purposes of this CPS, non-confidential information is all published information relating to the Root and Sub CA certificates. This includes, but is not limited to

- the published and linked information in the Trust Center repository,
- the information published in the CCADB
- the information published by Telekom Security in "Bugzilla" (https://bugzilla.mozilla.org/) or other discussion forums.

9.3.3 Responsibility to protect confidential information

All Telekom Security employees are required to take into account and comply with the company-wide guidelines on handling confidential information. Training on the correct classification of information in accordance with the abovementioned protection classes and on the resulting measures is provided at the time of hiring and at regular intervals. Contractors or third parties are also contractually obligated to comply with the company-wide requirements.

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.

As the Root TSP, 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 Offline CA, including the registration processes, which are regularly checked as part of a binding company-wide procedure. Successful completion of this procedure is a prerequisite for permanent approval of operation under privacy law.

9.4.2 Information treated as private

All personal data processed by Telekom Security as the Root TSP is treated as private unless it is already publicly available via other channels and is thus not deemed as private information in accordance with Section 9.4.3.

9.4.3 Information not deemed as private

Information not deemed as private, that are processed by Telekom Security, are all information about the concerned persons that are publicly available, e.g. via websites of the operators of the Sub CAs, trade register excerpts etc. This includes commercial contacts resulting from communications, e.g. business addresses, mail addresses and phone numbers.

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. Training is provided at the time of hiring and at regular intervals. 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 cirucmstances

Not applicable.

9.5 Intellectual property rights

The statutory regulations apply.

9.6 Representations and warranties

9.6.1 CA representations and warranties

As the Root TSP, Telekom Security assures reliable, trustworthy, non-discriminatory and legal operation of the service as well as compliance with the Telekom Security CP.

In addition, Telekom Security as Root TSP assures to take appropriate precautions to ensure that also the operators of the Sub CAs operate their service in a reliable, trustworthy and non-discriminatory manner and maintain conformity to the Telekom Security CP.

As the Root TSP, Telekom Security informs the operators of Sub CAs in good time via the established communication channels about planned and decided changes.

9.6.2 RA representations and warranties

Telekom Security only relies on its own employees for registration activities in the context of the Root TSP, see section 9.6.1.

9.6.3 Subscriber representations and warranties

The operators applying for or holding Sub CA certificates from a public Telekom Root CA are obligated to

- to provide accurate and complete information,
- to use the key pair only in accordance with any restrictions communicated to the applicant,
- not to use the CA's private keys for any unauthorized purpose,
- to notify the Root TSP immediately if any of the following events occur during the validity period of a certificate,
- a private key has been lost, stolen, or possibly compromised,
- control of a private key has been lost, e.g., due to compromise of activation data or other reasons,
- inaccuracies or necessary changes to the certificate contents are discovered,
- after a private key has been compromised, immediately and permanently discontinue the use of that key,
- immediately revoke a certificate or have it revoked if there is a reason for revocation in accordance with Section 4.9.1,

- to immediately and permanently stop using the corresponding private key after revocation of a certificate,
- to immediately and permanently stop usingthe private CA key after the compromise of the issuing Root CA becomes known,
- to generate the keys using suitable algorithms and key lengths in accordance with Section 6.1.5,
- to keep the private key under control,
- to use the private key only within secure cryptographic modules,
- to generate the keys within the secure cryptographic module,
- to take all reasonable measures to ensure confidentiality and control over the private keys and activation data,
- verify the contents of the certificate for accuracy,
- to respond within a reasonable time to the Root TSP's instructions in the event of compromise of a key or certificate misuse,
- accept that the Root TSP is entitled to revoke a certificate immediately if there is a reason for revocation in accordance with Section 4.9.1, and
- to notify the Root TSP of any changes to the registration data.

In addition, Telekom Security, as the Root TSP, informs the operators of Sub CAs about the following aspects:

- the applicable policy according to ETSI EN 319 411-1 or -2
- information on what is considered acceptance of the certificate
- the period of time for which the records (see section 5.5.2) are kept
- the requirements for confidential third parties according to section 9.6.4
- whether and, if so, in what way the requirements of the Telekom Security CP are supplemented or further restricted
- any restrictions on the use of the service provided
- the limitations of liability of Telekom Security as Root TSP
- the applicable law
- the procedures for complaints and dispute resolution
- frequency and underlying audit schemes of audits according to sections 8.1 and 8.4
- contact information of the Root TSP
- statements on the availability of the services provided

9.6.4 Relying party representations and warranties

See section 4.5.2 and 4.9.6.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimer of warranties

Any warranty exclusions are regulated in the internal and external agreements.

9.8 Limitations of liability

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

Any limitations of liability are regulated in the internal and external agreements and generally comply with applicable law.

9.9 Indemnities

Any claims for damages by the operator of a Sub CA against Telekom Security as Root TSP is regulated in the internal and external agreements.

9.10 Term and terminiation

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

See section 9.10.1.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

Telekom Security as Root TSP informs the operators of the Sub CAs and, if applicable, assessment bodies and supervisory or other regulatory authorities about relevant changes, see also sections 1.5.4, 9.6.1 and 9.6.3.

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

Possible provisions between the operators of the Sub CAs and Telekom Security as Root-TSP are regulated in the internal and external contracts.

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

No stipulation.

9.17 Other provisions

No stipulation.