Deutsche Telekom Security GmbH
Trust Center Certificate Practice Statement Public

Deutsche Telekom Security GmbH

Public

Version: 01.00

Valid from: 01.10.2021

Status: Final

Last Review: 23.09.2021

IMPRINT

Table 1: Document properties

Eigenschaft	Wert
Publisher	Deutsche Telekom Security Trust Center & ID-Solutions Untere Industriestraße 20, 57250 Netphen, Deutschland
Filename	Telekom Security CPS Public EN V0.91.docx
Valid from	01.10.2021
Title	Trust Center Certificate Practice Statement Public
Version	01.00
Last Review	23.09.2021
Status	Final
Contact	Telekom Security Leiter Trust Center Betrieb
Abstract	Telekom Security CPS Public

VERSION HISTORY

Table 2: Version history

Version	Date	Editor	Changes / Comments
0.9	01.08.2021	Telekom Security	Initial version structured according to RFC 3647
0.91	09.09.2021	Telekom Security	Correction of the Audit findings
01.00	24.09.2021	Telekom Security	Release

TABLE OF CONTENT

LIST OF TABLES

1 INTRODUCTION

1.1 Overview

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

This document is a Certificate Practice Statement (CPS) of the Telekom Security Trust Center. It describes, in the structure of RFC3647, the implementation of the requirements from the following sources to the Telekom Security PKI operation of the new generation and thus represents a supplement to the Telekom Security Root CPS. The sources are:

- Telekom Security CP (OID 1.3.6.1.4.1.7879.13.42)
- ETSI EN 319 401
- ETSI EN 319 411-1, ETSI EN 319 411-2
- Requirements published at http://www.cabforum.org:
  - "CA/Browser Forum Baseline Requirements" [BR]
  - "CA/Browser Forum EV Guidelines" [EVCG]
  - "CA/Browser Forum Network and Certificate System Security Requirements"
- Various Root Store Policies

Currently, only domain-validated TLS server certificates are offered in the scope of this.

In the event of a conflict between this CPS, the Telekom Security CP and the sources referenced above, the regulations from the Telekom Security CP and the sources referenced above 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)}

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

1.3 PKI participants

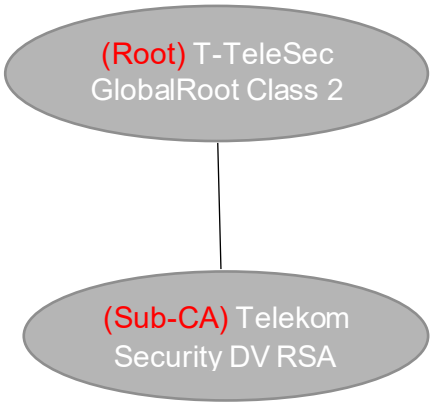
1.3.1 Certification Authorities

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

Table 3: Sub CA certificates within the scope of this CPS

Name	Key	Serial number	Validity period	Fingerprint
Telekom Security DV RSA CA 21	RSA 2048	2cf3c72f3f7d0f b31fc362d6b8 69558e	2021-04-21 to 2031-04-21	99cc84f820818cf 0eefe81ddf572ca ce4b3acb78

The intermediate certification authorities within the scope of this CPS are part of the following PKI hierarchy:



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 the sole registration authority for all certificates within the scope of this CPS.

1.3.3 Subscribers

Subscribers are all natural and legal persons applying for or owning subscriber certificates under the certification authorities named above.

1.3.4 Relying parties

Relying parties are persons or IT processes that trust certificates issued under this CPS 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

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

CA certificates are not used for use cases other than those listed in chapter 1.4.1.

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-Solutions

Untere Industriestraße 20

57250 Netphen, Germany

1.5.2 Contact person

Contact for this CPS is the Root/Compliance-Team of the Telekom Security Trust Center:

- Email: FMB_Trust_Center_Rootpogram@t-systems.com
- Internet: https://telesec.de/de/service/kontakt/anfragemitteilung/

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_Rootprogramm@t-systems.com

or, as far as possible, via the functions of the ACME protocol. 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/Compliance-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

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

This CPS will be reviewed by the Trust Center Root/Compliance-Team 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 made in section 2.2.

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 about all 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
- Certificate Practice Statements (CPS, including this document)
- PKI Disclosure Statements (PDS)
- All public Root CA certificates of Telekom Security that are still valid
- All Sub CA certificates that are still valid and were issued by Telekom Security's public Root CAs
- Audit attestations for the public Root CA certificates of Telekom Security (link to the Auditor's web pages)
- Service descriptions
- Terms and conditions

Both the CP and CPS Public 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 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

The corresponding URLs for each Root CA can be found on the Trust Center website.

All subscriber certificates for TLS server authentication are published in a sufficient number of CT Logs before their final issuance.

2.3 Time or frequency of publication

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 CPS are published in the Trust Center's repository and communicated to the CCADB after the release of a new version as fast as possible, 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 7.1.4.

3.1.2 Need for names to be meaningful

Each CA certificate is given a CommonName which clearly indicates the affiliation of that CA certificate with Deutsche Telekom Security GmbH (or DFN).

All certificates contain an IssuerName which is byte-by-byte identical to the SubjectDistinguishedName of the issuing CA certificate.

All TLS server certificates contain a SubjectAlternativeName with FQDNs that belong to this certificate.

3.1.3 Anonymity or pseudonymity of subscribers

Domain validated certificates do not contain any information regarding the owner of the certificate which generally preserves the anonymity of the subscriber.

3.1.4 Rules for interpreting various name forms

See section 7.1.2 and 7.1.4.

3.1.5 Uniqueness of names

All CA certificates issued under a specific (Root) CA certificate are assigned a unique CommonName and thus SubjectDistinguishedName.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Methods to prove possession of private key

A certificate request signed with the corresponding private key is necessary for issuance of a certificate.

3.2.2 Authentication of organization identity

Authentication of organisations is not necessary for the issuance of domain validated certificates.

Validation of an applicant's control over a corresponding domain is verified using the functions of the ACME protocol. These are:

1. (Method according to CABF Baseline Requirements chapter 3.2.2.4.7).
   DNS Change
   The applicant proves control of an FQDN by confirming the existence of a unique random value in a DNS TXT or CAA record for the requested FQDN prefixed with "_acme_challenge". This method is also used to validate wildcard certificates.
2. (Method according to CABF Baseline Requirements chapter 3.2.2.4.19)
   Agreed-Upon Change to Website – ACME
   The applicant proves control over an FQDN by using the ACME http challenge as defined in RFC 8555 chapter 8.3 and supplemented by the requirements of the Baseline Requirements.

For wildcard certificates, it is checked whether the wildcard character "*" (asterisk) is contained in the first label on the left of a "registry-controlled" label or "public suffix" (e.g. ".com", definition according to RFC 6454 Section). In such a case, the issuance of a certificate will be refused unless the applicant proves his legitimate control over the entire domain namespace.

3.2.3 Authentication of individual identity

Domain-validated certificates are not issued to individuals and therefore do not require an authentication of individual identity.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

Validation of authority for domain validated certificates is covered by the validation of domain control (see section 3.2.2) as well as taking into account existing CAA records (see section 4.2).

3.2.6 Criteria for interoperation

Telekom Security does not issue cross certificates..

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Certificate re-key of domain-validated certificates are handled as new certificate applications.

3.3.2 Identification and authentication for re-key after revocation

Certificate re-key of domain-validated certificates are handled as new certificate applications.

3.4 Identification and authentication for revocation request

The authentication of revocation requests regarding TLS server certificates is handled by the functions of the ACME protocol. Additionally, an identification of the certificate owner as authorized to request revocation is possible via ExternalAccoundingBinding and the private key associated with that account.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Certificate requests can generally be made by all natural and legal persons or their authorized representatives, provided that they registered a customer account.

4.1.2 Enrollment process and responsibilities

The enrollment process for subscriber certificates includes

- registration of an account on the ACME server and linking that account to their customer account (via ExternalAccountBinding-key),
- generation of a secure key pair,
- acceptance of the data privacy notice, the terms and conditions, the terms of use, the CPS and the service description,
- provision of a certificate request including the public key (e.g. via the ACME protocol)
- confirmation by the subscriber that the information provided in the certificate request are true and correct as well as that the key pair has been generated securely.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Identification and authentication in the context of certificate applications are performed according to section 3.2. Related manual activities are performed exclusively by qualified personnel in trusted roles of Telekom Security's Trust Center.

In addition, for TLS server certificates, all FQDN entries in the subjectAltName are checked against CAA entries in the DNS immediately before a certificate is issued. If no CAA resource record is stored or its issue or issuewild property contains "telesec.de", the issuance of the certificate is continued. "iodef" entries are evaluated but not followed up. Further entries of the CAA record are not supported.

For the identification of high-risk certificate requests, Telekom Security maintains a database with organisation names and domain names or IP addresses which, due to their attractiveness, have an increased risk of being the target of phishing, misuse or fraud attacks. Identified high-risk certificate requests are considered individually.

4.2.2 Approval or rejection of certificate applications

The Trust Center rejects applications for the issuance of certificates, if

- a validation according to section 4.2.1 cannot be fully completed,

- in the case of a High Risk Certificate Request, the risk of misuse cannot be sufficiently excluded,
- the request was made for an IP address from a reserved address space or for an internal server/host name,
- the key used does not meet the quality criteria or is compromised,
- the CAA check is negative,
- ICANN has not released the gTLD (the list of released and terminated gTLDs is updated regularly, but at the latest every 30 days via the ICANN website).

Telekom Security is also entitled to refuse certificate applications without giving reasons.

If all validation steps according to chapter 4.2.1 have been carried out successfully and none of the above points apply, the certificate issue will be approved.

In the event of a deferral or rejection of a request, the certificate applicant will be notified.

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 information contained in the certificates is protected during issuance by technical, organizational and personnel controls.

4.3.2 Notification to subscriber by the CA of issuance of certificate

After issuance of a certificate, the subscriber is informed and immediately provided with the certificate via the ACME protocol.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

See section 2.2.

4.4.3 Notification of certificate issuance by the CA to other entities

See section 2.2.

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.

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 stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

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 Sub-CA certificate is revoked if one or more of the following occur:

- The Subordinate CA requests revocation in writing.
- The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization.
- The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6.
- The CA obtains evidence that the Certificate was misused.
- The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with the CABF Baseline Requirements or the Telekom Security CP or applicable CPS.
- The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading.
- The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate.

- The Issuing CA's or Subordinate CA's right to issue Certificates under the CABF Baseline Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository.
- Revocation is required by the Telekom Security CP and/or applicable CPS.
- It is determined that the Sub-CA certificate was not issued in conformity with the Telekom Security CPS Root or the operator of the Sub-CA does not operate in conformity with this CPS,
- There are statutory provisions, judicial rulings or an instruction from a supervisory authority.

A subscriber certificate is revoked within a very short time (24 hours for TLS server certificates) 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 or IP address in the certificate should not be relied upon.

A subscriber certificate is, if possible, revoked within a very short time (24 hours for TLS server certificates), but at the latest within a medium time (5 days for TLS server certificates) 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 ore 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 or IP address 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 Baseline Requirements 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 the subscriber or a representative of the subscriber.

Additionally, revocation can be triggered or requested by every person, if the person is able to prove that a revocation reason according to section 4.9.1 exists.

4.9.3 Procedure for reovcation request

Revocation can be requested using the functions that are provided by the ACME protocol. This requires signing a revocation request with the private key associated with the certificate or the private key of the account associated with the certificate. Alternatively, a revocation request can be authorised by proving control over the domain specified in the certificate.

In addition, the Trust Center offers another interface for reporting misuse or problem reports regarding certificates (see Chapter 1.5.2). Telekom Security processes these reports and initiates the revocation of affected certificates if there is a corresponding reason for revocation. The person reporting the problem is informed about the receipt of the report and any resulting revocations of the affected certificates.

4.9.4 Revocation request grace period

If a revocation reason according to section 4.9.1 is determined, revocation is to be requested as timely as possible or the Trust Center is to be informed accordingly.

4.9.5 Time within which CA must process the revocation request

If there is an authorised 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

Relying parties are requested to request the status of certificates via the certificate status information services provided by Telekom Security before they fully trust a certificate issued by the Trust Center.

4.9.7 CRL issuance frequency

Certificate revocation lists (CRLs) for subscriber certificates are published within a few minutes after a revocation as well as regularly every 24 hours. The value within “nextUpdate” is 5 days after the “thisUpdate“-entry.

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 requested 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 advertisement available

No stipulation.

4.9.12 Special requirements re key compromise

Third parties that want to report a key compromise are requested to use the options of the ACME protocol as described in section 4.9.3 or the contact options described in section 1.5.2. For the later, 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 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, both 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) 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 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

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 all 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)
- processing of requests for CA certificates
- assessment of security incidents
- changes to CA system configurations
- changes to certificate profiles

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. 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 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 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,
- 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 life cycle of CA certificates and keys (e.g. key generation, storage, backup, recovery and destruction, issuance and revocation of CA certificates, and HSM lifecycle) as well as subscriber certificates (e.g. validation of application information as well as issuance, renewal and revocation of certificates) 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

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 being continuously logged. They 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 events listed in section 5.4.1.2 are logged continuously by all systems. They 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

Records of activities listed in section 5.4.1.1 are retained for 7 years after the end of validity or revocation date of the last certificate issued for the relevant public key and, in case of CA certificates, the destruction of the key.

Records of activities listed in section 5.4.1.2 are retained for at least 2 years after the date of the occurrence of a security-relevant event.

5.4.4 Protection of audit log

The records of the activities listed in section 5.4.1.1 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 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

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.

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

See section 5.7.1.

5.8 CA or RA termination

Telekom Security has a continuously updated termination plan.

In the event of termination, Telekom Security plans to inform all affected subscribers in good time so that they can migrate to another CA of Telekom Security or another operator and thus possible disruptions for end subscribers are avoided.

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 root store operators will be explicitly informed.

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

For terminating, the private keys of the 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 subscriber 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

Telekom Security does not generate keys for subscribers, but subscribers are informed about permitted algorithms for the generation of key pairs.

The prerequisite for the generation of CA keys is an approved application for the issuance of a CA certificate. The key pairs are generated within HSMs according to section 6.2.1 in the secure environment of the Trust Center and in scope of a key ceremony.

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

- 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"),
- separate storage of tokens to restore keys from backup ("n of m").

The ceremonies are supervised by a qualified internal auditor and, in case of Sub CAs for TLS server certificates a qualified external auditor of a conformity assessment body (see section 8.2). After correct performance of the ceremony, the respective auditor confirms this in the minutes of the ceremony.

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 connections secured by TLS.

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

RSA keys are only accepted with a minimum key length of 2048 bits and a length of the module divisible by 8.

EC keys are only accepted based on the elliptic curves NIST P-256 or NIST P-384.

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

Private CA keys are exclusively used for signing additional Sub CA or subscriber certificates, delegated OCSP-Signer certificates and revocation lists.

All subscriber 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.

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

Generation and usage of the private 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 CA keys are not stored outside the Telekom Security Trust Center.

6.2.4 Private key backup

Private CA keys 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 assigned to employees in different trusted roles and are stored separately secured from one another.

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 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

Private CA keys 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

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 at the end of the life cycle of the corresponding 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. Analogue to the generation of CA keys, the destruction of keys takes place in a ceremony in the presence of corresponding auditors (see Section 6.1.1) and takes into account all copies of the keys.

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 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

Certificates are archived as part of regular backup measures.

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.

Sub CA certificates are issued with a maximum validity period of 10 years.

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").

Key pairs can be reused for subsequent certificates as long as they are not compromised or otherwise unusable.

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 assigned 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

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

6.6.1 System development controls

Telekom Security maintains a regular and close exchange with the software supplier of the CA and OCSP systems, 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

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 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 usually 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 Time-stamping

All systems are regularly synchronized with reliable time information via the time server according to Section 5.5.

7 ZERTIFIKATS-, SPERRLISTEN- UND OCSP-PROFILE

7.1 Zertifikatsprofile

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 a random and, under the corresponding issuing CA, unique serial number with a length of 126 bit.

7.1.1 Version number

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

7.1.2 Certificate extensions

Sub CA certificates only contain the following certificate extensions:

- authorityKeyIdentifier: contains the value of the subjectKeyIdentifier of the corresponding issuing CA certificate
- subjectKeyIdentifier: contains the “keyIdentifier” according to RFC5280#4.2.1.1.
- keyUsage (critical): contains “keyCertSign”, “cRLSign”
- basicConstraints (critical):
  - „cA“: „true“
  - „pathLenConstraint“: according to RFC5280
- CertificatePolicies:
  - Sub CA certificates for the issuance of TLS server certificates contain the corresponding policy OID of the Baseline Requirements (see section 7.1.6).
- ExtendedKeyUsage:
  - Sub CA certificates for the issuance of TLS server certificates contain “id-kp-serverAuth” and, where appropriate, “id-kp-clientAuth”.
- cRLDistributionPoints: contains an http URL of the corresponding CRL
- authorityInfoAccess: contains an http URL of the corresponding OCSP responder (accessMethod 1.3.6.1.5.5.7.48.1 (ocsp)).
  - Sub CA certificates for the issuance of TLS server certificates also contain an http URL for a distribution point of the corresponding issuing CA certificate (accessMethod 1.3.6.1.5.5.7.48.2 (calssuers)).

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

Subscriber certificates only contain the following certificate extensions:

(DV TLS server certificates)

- authorityKeyIdentifier: contains the value of the subjectKeyIdentifier of the corresponding issuing CA certificate
- subjectKeyIdentifier: containts the “keyIdentifier” according to RFC5280#4.2.1.1
- keyUsage (critical): contains a value consistent with the extendedKeyUsage according to RFC5280 #4.2.1.12
- basicConstraints (critical):
  - „cA“: „false“
  - „pathLenConstraint“: not contained
- CertificatePolicies:
  - TLS server certificates contain the corresponding policy OID of the Baseline Requirements (see section 7.1.6).
- subjectAltName: contains at least one entry in the form of an FQDN or IP address
- extendedKeyUsage:
  - TLS server certificates contain “id-kp-serverAuth” and, where appropriate, “id-kp-clientAuth”.
- cRLDistributionPoints: contains an http URL of the corresponding CRL
- authorityInfoAccess: contains an http URL of the corresponding OCSP-Responder (accessMethod 1.3.6.1.5.5.7.48.1 (ocsp)) and an http URL for a distribution point of the corresponding issuing CA certificate (accessMethod 1.3.6.1.5.5.7.48.2 (calssuers)).

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)

7.1.4 Name forms

CA certificates only contain the following attributes:

- commonName
- organizationName
- countryName

Domain validated TLS server certificates only contain the following attribute:

- commonName (contains an FQDN listed in the SubjectAlternativeName)

7.1.5 Name constraints

Name constraints are not set.

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 Baseline Requirements [BR]:

- 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)

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 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 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), privilegeWithdrawn (9).

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 with value NULL 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

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

All CA certificates in the scope of this CPS are publicly disclosed on the website of the Trust Center as well as in the CCADB and various CT-Logs and are 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 and form an uninterrupted sequence.

In addition, all key generation and certificate issuance for Root CAs and for those Sub CAs being within the scope of [BR] are monitored by external auditors. Sub CA certificates for the DFN are only issued if there is evidence that the associated key generation was monitored by an external auditor and found to be compliant.

All activities at the offline CA are monitored by an internal auditor who ensures compliance with organisational and technical measures. Sub CA certificates for the Trust Center are only issued if the associated key generation has been monitored by at least one internal auditor and found to be compliant.

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.

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

All sub-CAs listed in chapter 1.3.1 including all associated processes, systems, infrastructures and organisational measures are part of the certifications according to the current versions of ETSI EN 319 411-1 or ETSI EN 319 411-2. The following policies are applied:

- Telekom Security DV RSA CA 21: DVCP

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 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

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:

- public
- internal
- confidential
- confidential (customer)

For the purposes of this CPS, confidential information is all information that is not classified as "public" 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 certificates. This includes, but is not limited to

- the information contained in certificates,
- 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 and mailing lists.

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.

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 permanent approval of operation under privacy law.

9.4.2 Information treated as private

All personal data processed by Telekom Security 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 or can be derivated from publicly available information. This includes, e.g., information in certificates.

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

Telekom Security assures reliable, trustworthy, non-discriminatory and legal operation of the service as well as compliance with the Telekom Security CP. Services offered to subscribers are also made available to persons with disabilities as far as that is possible. If existing measures are not sufficient, Telekom Security Trust Center also offers free support via telephone to people with disabilities to help them apply for, accept and revoke certificates.

Before concluding a contractual relationship with an end user, the end user shall be informed of the terms of use for the use of the certificates in accordance with Section 9.6.3.

Telekom Security assures the representations and warranties of a TSP in the Telekom Security CP section 9.6.1.

Acceptance of the contracts with the subscribers including the terms of use can, if legally enforceable, be made electronically and apply to several certificates.

9.6.2 RA representations and warranties

Telekom Security only relies on its own employees for registration activities and assures the representations and warranties of registration authorities 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 before issuing the certificates. These terms of use take into account the representations and warranties required in the Telekom Security CP chapter 9.6.3.

The terms of use are made permanently available to the subscribers in an integrated manner via the websites of the Trust Center and the service portals.

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 as well as in the terms and conditions.

9.8 Limitations of liability

Telekom Security 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 as well as terms and conditions and generally comply with applicable law.

9.9 Indemnities

Any claims for damages against Telekom Security are regulated in the internal and external agreements as well as the terms and conditions.

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 informs all subscribers 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

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.