Deutsche Telekom Security GmbH
Certification Practice Statement Public

Version: 08.00

Valid from: 01.03.2025

Status: Released

Last Review: 18.02.2025

VERSION HISTORY

Table 1: Version history

Version	Date	Changes / Comments
01.00	24.09.2021	Initial version structured according to RFC 3647
02.00	15.03.2022	Include new CA certificate
03.00	13.08.2022	Integration of OV, general revision
04.00	10.01.2023	Integration of ▪ EV and QEVCP-w (supersedes CPS for Server.ID), ▪ S/MIME according to LCP and NCP (supersedes public parts of CPS cPKI and CPS Business.ID), ▪ Root CPS (supersedes Telekom Security CPS Root), general revision
05.00	20.06.2023	Integration of new CA certificates and new qualified Trust Service Provider for QWAC, deprecation of BR method 3.2.2.4.2, general review
06.00	01.09.2023	Integration SMIME BR, Addition of new CA certificates
07.00	18.03.2024	Integration of Trust Service „Client.ID”
08.00	01.03.2025	Extension of SMIME validation methods, update of CA list and minor adjustments / updates to various parts

TABLE OF CONTENT

LIST OF TABLES

1 INTRODUCTION

1.1 Overview

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

Deutsche Telekom AG is accredited as qualified Trust Service Provider according to [eIDAS] for the issuance of certificates for qualified signatures (QES). Deutsche Telekom Security GmbH and T-Systems International GmbH are accredited as qualified Trust Service Providers according to [eIDAS] for the issuance of qualified website authentication certificates (QWAC).

This document is the Certification Practice Statement (CPS) for issuing public certificates by the Trust Services "Business.ID", "Server.ID" and "cPKI" (Corporate PKI of Deutsche Telekom). It describes in the structure of [RFC3647] the compliance and the implementation of the requirements of

- Telekom Security CP (OID 1.3.6.1.4.1.7879.13.42) [TSCP],
- ETSI EN 319 401,
- ETSI EN 319 411-1,
- ETSI EN 319 411-2,
- the current versions of the following CA/Browser Forum documents, published at https://www.cabforum.org:
  - "CA/Browser Forum Baseline Requirements" [BR],
  - "CA/Browser Forum EV Guidelines" [EVCG],
  - "CA/Browser Forum Network and Certificate System Security Requirements" [NCSSR],
  - “CA/Browser Forum S/MIME Baseline Requirements” [SBR],
- various Root Store policies (Mozilla [MOZRP], Microsoft [MSRP], Google [GCRP], Apple [APLRP] etc.).

Applicable policies, depending on the Trust Services, are

- DVCP, OVCP, EVCP and QEVCP-w for TLS certificates issued by Server.ID,
- OV for TLS certificates issued by Business.ID,
- NCP for S/MIME certificates issued by Business.ID and Client.ID,
- LCP for S/MIME certificates issued by cPKI and Client.ID.

The Terms of Use Public [TOUP] apply.

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

Note: The statements made in this document generally apply to all certificates within the scope of this CPS. Some statements that only apply to specific certificate types are indicated by specifying the certificate type ([TLS] or [SMIME]) or the applicable policy ([DVCP], [OVCP], [EVCP], [QEVCP-w], [LCP] or [NCP]) in square brackets.

1.2 Document name and identification

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

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

1.3 PKI participants

1.3.1 Certification Authorities

The CA certificates listed in the following tables are within the scope of this CPS.

Note: The Root CAs created since 2020 will be used to set up dedicated PKI hierarchies for TLS and S/MIME (not yet active).

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

commonName	Issued	Fingerprint (SHA1)
Telekom Security TLS RSA Root 2023	2023-03-28	EFC65CADBB59ADB6EFE84DA22311B35624B71B3B1EA0DA8B6655174EC8978646
Telekom Security SMIME RSA Root 2023	2023-03-28	78A656344F947E9CC0F734D9053D32F6742086B6B9CD2CAE4FAE1A2E4EFDE048
Telekom Security SMIME ECC Root 2021	2021-03-18	3AE6DF7E0D637A65A8C81612EC6F9A142F85A16834C10280D88E707028518755
Telekom Security TLS ECC Root 2020	2020-08-25	578AF4DED0853F4E5998DB4AEAF9CBEA8D945F60B620A38D1A3C13B2BC7BA8E1
T-TeleSec GlobalRoot Class 3	2008-10-01	FD73DAD31C644FF1B43BEF0CCDDA96710B9CD9875ECA7E31707AF3E96D522BBD
T-TeleSec GlobalRoot Class 2	2008-10-01	91E2F5788D5810EBA7BA58737DE1548A8ECACD014598BC0B143E041B17052552

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

commonName	Issued	Fingerprint (SHA1)
Sub CA certificates under Telekom Security TLS RSA Root 2023		
Telekom Security EV RSA CA 25	2025-02-27	C9A5C1A8848C3FE895EA32DBAA4BEDEBCDABF6833469E6EA9CB90E156EF1F09D
Telekom Security EV RSA CA 23	2023-03-28	9A6FC4AB4DB1EA6F6663507EDC1D008F091AE88FAB6F3AE56A84A4090529EF58
Sub CA certificates under Telekom Security SMIME RSA Root 2023		
Telekom Security SMIME RSA CA 24	2024-02-13	0E2CFE3B15D2A754BD86DDDA077AC4A3DF961A9FA6B59278DD72098024D04567
Telekom Security SMIME RSA CA 23	2023-03-28	EB48699C89C702DAC2C05F483396489BBBF71AA0ACAC0F52596A5DE97CEBD913
Sub CA certificates under Telekom Security SMIME ECC Root 2021		
Telekom Security SMIME ECC CA 24	2024-02-13	F33B1859C34A063E941DC7D8F3F5378833C4770D48B7454EE1CDCD9A8194935A
Telekom Security SMIME ECC CA 23	2023-03-28	EA45DD36FD0CA91706080F68F7213D55E658249A20C81AFDD34E80CC5EC3E349
Sub CA certificates under Telekom Security TLS ECC Root 2021		
Telekom Security EV ECC CA 24	2024-11-26	708E9E96AD5CE5C9B1F79137423FA98A81FFB087879B7BBE3DA71425742E2EEC
Telekom Security OV ECC CA 24	2024-11-26	679C0CD9D0C4E893E0073250322304F0E7741067E0C92DB42B90FFB94144BBFB
Telekom Security DV ECC CA 24	2024-11-26	688C275E88EBB382EED0AC7D8FAD62A8D0C7D0731D63A9CA31A67B6B1525E228

Telekom Security EV ECC CA 21	2021-04-21	D7A8A9947C31806C1B4625F82FCBCCA7CC2090E58DB215B8E4D88BA9C60D3166
Sub CA certificates under T-TeleSec GlobalRoot Class 3 (used for [EVCP] and [QEVCP-w])		
Telekom Security EV RSA CA 23A	2023-06-20	82FBE865DA22D1F25ADF94BBD809D3F516125849E792DB7BB18452304C2ECC43
Telekom Security ServerID EV Class 3 CA	2022-08-02	5092CE0E3F70F2FD9561C34623B546F7D333EF1B633C147D1290E28DE986A230
Telekom Security EV RSA CA 22	2022-06-21	86DB1D597419BC0FDDF2A6129DE46AF537752683A49CB9435C855F53637CFE13
TeleSec ServerPass Extended Validation Class 3 CA	2014-02-11	8A0ADDAE4F2CF9D2C24D7A49EED5C86C8B1DF1C85BA73DE5C477CB14FA0D13E9
Sub CA certificates under T-TeleSec GlobalRoot Class 2 (used for [DVCP], [OVCP], [LCP] and [NCP])		
Telekom Security SMIME CA 25	2025-02-27	BE096522370C4BABCA86876B3060A94FC3D157613C3500606A9E5691DA7D11E7
Deutsche Telekom AG secure email CA E05	2023-08-09	1AB8A68FCBBA644D5C6D2627FE6D943CE4FD3E58619B3B087F3CF4EFA838C46A
Telekom Security BusinessID SMIME CA 2023	2023-06-20	6F25BD0E9E7492D15375089EB97C1C0747537336BB0FA82543BD2A485BE61A00
Deutsche Telekom AG secure email CA E04	2023-06-20	651656EDA8A9765470C57B3692A4FF62D9B05AB5CE1179E866B70F4DAFD754FD
Telekom Security ServerID OV Class 2 CA	2022-08-02	944ACE961DB316BEB694E01C302C46FED40DC0291729E7DAF58550C3CB55E791
TeleSec Business TLS-CA 2022	2022-06-21	A3F2A10A366AFF774CBB4E6EC4C8A8EF707C03E932B4C46E5078767AACF1ED60
Telekom Security OV RSA CA 22	2022-06-21	D5D9445EEAA5576081DDF2E6C0904091BBC79BA10915E5215C8A2A7D87915FFD
Telekom Security DV RSA CA 22	2022-02-22	938E52642501DD16E23D8AEBFB97EB3C3B2562F50C324144C390946B29684A7E
TeleSec Business TLS-CA 21	2021-11-17	F00E616B59ED06E6CC9717D039F7A1A70CB3D08E0B6AD74653670CCE448C61F3
TeleSec Business CA 21	2021-11-17	06B58F124B45E9417708F60CDDAEB6F39B72206FE4BD40EE2E20E628DDFDD33D
TeleSec Business TLS-CA 2021	2021-11-17	A712E2126EA4CAC6A5EE860D2F3E0CE03CDFD232A9E7911B7CFE2C4B12A228FA
TeleSec Business CA 2021	2021-11-17	7732599AAF35853E0351E49F8057BBF5321777E83603C38570065056A56FA68B
Telekom Security DV RSA CA 21	2021-04-21	956FF9CC914874D9CAF9655BCCB696C1BE49A25BF928D5C41C0F5395A135D8B8
Deutsche Telekom AG secure email CA E03	2020-07-09	38CBC81860C904BDF18046CD0FB7754E44D569398DD14FBF09F72AA20FC35CCF
TeleSec ServerPass Class 2 CA	2014-02-11	AC1EC556318E3EA70F8F04E03A0F2633BFE73992359A810145FFDF1A427396EE
TeleSec Business CA 1	2012-11-29	44EBF0123E27FF1DB0497BD2DAE18155B2A414E6BCD9C6C8FB8F48398449B9E9

1.3.2 Registration Authorities

Depending on the Trust Service, subscribers are registered

- by the Trust Center itself (Server.ID),
- by external / Enterprise RAs (Business.ID) or

- by an internal Enterprise RA of the Deutsche Telekom Group (cPKI).

An RA employee MUST NOT validate a request for a certificate in which he himself is the subject.

External RAs are bound by contract and restricted as far as possible by means of technical measures, including restrictions to pre-validated certificate contents. However, the validation of the control of domains (including mail domains for [SMIME]) and IP addresses is not delegated to external RAs.

[EVCP], [QEVCP-w] Also the validation of certificate applications is not delegated.

1.3.3 Subscribers

Note: Due to the partially different use of terms in the referenced documents, the terms as used in this document are described below.

Subscribers within the meaning of this CPS are organizations or natural persons identified in association with an organization that obtain certificates from the Trust Services named above and that are legally bound by acceptance of the Terms of Use.

Organizations in the context of this CPS are legal persons or organizational units identified in association with a legal person. Organizations may be:

- Private organization: A non-governmental legal person whose existence was created by a filing with or an act of the Incorporating Agency or equivalent body
- Government Entity: A government-operated legal person, agency, department, or another related organizational unit
- Non-Commercial Entity: International organization created under a charter, agreement, convention, or equivalent instrument signed by or on behalf of more than one government of a country
- Business Entity: Organization that is not one of the previously mentioned organization types.

[EV], [QEVCP-w] Only private and public organizations of the DACH region (Germany, Austria, Switzerland) are accepted as subscribers.

Subject of a certificate in the context of this CPS is the user of the private key named in the certificate in the attributes of the "Subject Distinguished Name" or the "subjectAltName" extension. Subjects can be

- natural persons in association with an organization,
- organizations,
- devices.[1] operated by or on behalf of an organization.

Applicant in the context of this CPS is the person who submits the application to the Trust Service. This is always a natural person who is either

- the subscriber and/or the subject itself,
- an authorized representative of the subscriber (in the case of an organization) or
- another person authorized by the subscriber.

[EVCP] In addition to the applicant, the following roles are implemented:

- Contract Signer: A natural person who is explicitly authorized to represent the subscriber and to sign certificate applications on its behalf.
- Certificate Approver: A natural person who is explicitly authorized to represent the subscriber and to approve certificate applications on its behalf.

Note: One person may be entrusted with more than one of the listed roles and the roles may be filled by more than one person.

[1] "devices" hereinafter also subsumes systems, functions and IT processes, unless explicitly stated otherwise

1.3.4 Relying parties

Relying parties are persons, systems or IT processes that rely on the certificates issued under this CPS.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Subscriber certificates may only be used for the following applications:

- [DVCP], [OVCP]: TLS server and client authentication of TLS servers.
- [EVCP], [QEVCP-w]: TLS server authentication of web servers.
- [SMIME]: Encryption and/or signature of emails, files or other data, as well as client authentication, if applicable.

The application must comply with the key usages defined in the certificates in the keyUsage and extendedKeyUsage attributes.

TLS server certificates may only be installed on servers that are accessible under the domain names or IP addresses listed in the subjectAltName. EV certificates may only be installed on web servers.

1.4.2 Prohibited certificate uses

The use of certificates contrary to the scenarios mentioned in Section 1.4.1 is not permitted.

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, etc.

1.5 Policy administration

1.5.1 Organization administering the document

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

1.5.2 Contact person

The contact for this CPS is the Trust Center's PKI Compliance Management, which can be reached via email under TrustCenter-Roots@telekom.de.

Certificate misuse, key compromises, faulty or non-compliant certificates, other security-relevant certificate problems or suspicions of such incidents can be sent to this email address. Regarding the reporting of key compromises, the instructions according to Section 4.9.12 have to be considered.

1.5.3 Person determining CPS suitability for the policy

The Trust Center's PKI Compliance Management is responsible for determining the conformance of this CPS to [TSCP]. For contact see Section 1.5.2.

1.5.4 CPS approval procedures

Each version of this CPS is being released by the Trust Center management after compliance with the [TSCP] has been determined and shall remain valid for newly issued certificates as well as for existing certificates until it is revoked or replaced by a new version.

1.6 Definitions and acronyms

For definitions, acronyms and references see [TSCP#1.6]. In addition, the following documents are referenced in this CPS:

[TSCP] Deutsche Telekom Security GmbH, Trust Center Certificate Policy
[TOUP] Deutsche Telekom Security GmbH, Terms of Use Public
[TOUC] Deutsche Telekom Security GmbH, Terms of Use cPKI (Corporate PKI Deutsche Telekom)

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Telekom Security operates a repository with information and documents (see Section 2.2) as well as certificate status services (see in particular Sections 4.9 and 4.10). In addition, various (LDAP) directories are provided for dedicated purposes.

2.2 Publication of certification information

Telekom Security operates a PKI repository (https://www.telesec.de/de/service/downloads/pki-repository/) in which current as well as superseded versions of the following information and documents are published:

- Telekom Security CP [TSCP]
- Certification Practice Statements (CPS, includes this document as well as the replaced CPSs)
- Terms of Use Public [TOUP]
- General Terms and Conditions (GTC)
- PKI Disclosure Statements (PDS)
- all CAs within the scope of this CPS
- Audit Attestations for Telekom Security Root CA certificates (link to the auditor's official web pages)
- Service descriptions

This CPS is published in German and English. The German and English versions always have the same version number and are synchronized in terms of content.

All required information on CA certificates is maintained in the "Common CA Database" (CCADB) in accordance with the CCADB policy [CCADB] (see https://www.ccadb.org).

For all Root CAs under which TLS server certificates are issued, test web pages are operated with one valid, one expired and one revoked TLS server certificate. For EV-enabled Root CAs, these are EV certificates. The links to the test web pages of each Root CA can be found on the Trust Center website (https://telesec.de/en/root-program/informations-about-ca-certificates/root-certificates/).

All TLS server certificates are published in the form of "pre-certificates" in a sufficient number of CTLogs before they are finally issued.

2.3 Time or frequency of publication

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

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

Audit Attestations are published or linked in both CCADB and the repository within 7 days of their issuance.

2.4 Access controls on repositories

The information listed in Section 2.2 is publicly available in a read-only manner. 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

All certificates contain the name of the subject in the form of a Distinguished Name (subjectDN) according to [X500] and, in the case of subscriber certificates, in the form of a subjectAltName. See Section 7.1.4 for details.

3.1.2 Need for names to be meaningful

All CA certificates are given a commonName which unambiguously reflects the affiliation to the organization.

The attributes givenName, surname, organizationName, organizationUnitName and organizationIdentifier represent the natural or legal person according to the identification documents. Common abbreviations are allowed.

[SMIME] For natural persons with several given names, at least one given name is included. For natural persons with only a single legal name, the name is included in surname.

3.1.3 Anonymity or pseudonymity of subscribers

[SMIME] The use of pseudonyms is permitted. Pseudonyms are chosen in such a way that confusion with existing names of natural persons or organizations is avoided.

The true identity of a pseudonymized identity is known to the responsible RA and to Telekom Security as CA.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

Certificates issued under a CA are unique with regard to the assignment of subjectDN and subscriber. A subjectDN is therefore not assigned to different subscribers. If the contents of the subjectDN of several subscribers match, additional identifiers are added to make the subjectDN unique.

Domain validated certificates are exempt from this rule. In this case, a subjectDN can be assigned to a new subscriber if the latter has proven control over the domain.

3.1.6 Recognition, authentication, and role of trademarks

Trademarks, tradenames and DBAs are not supported.

3.2 Initial identity validation

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

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

The following sections describe the applied methods themselves. Which methods are used in the context of a policy is described in Section 4.2.1.

3.2.1 Methods to prove possession of private key

If the key material is generated by the requester, proof of possession requires a PKCS#10 request signed with the private key,.

3.2.2 Authentication of organization identity

The following methods are used to validate the organizational identity according to Section 4.2.1.

QGIS - Qualified Government Information Source: The legal, physical and operational existence and identity of an organization are validated via government-managed sources that are deemed reliable for identification. Examples of QGIS are commercial registers, public corporations, and the Federal Central Tax Office. The information provided by the applicant is used for an automated or manual search in the relevant registers. The sources used for the validation ("Incorporation or Registration Agency") are published in the repository (https://telesec.de/de/service/downloads/pki-repository/) under "Validation Resources".

QIIS - Qualified Independent Information Source: The legal, physical and operational existence and identity of an organization are validated via privately managed sources that are classified as reliable for identification purposes. These sources are evaluated for their reliability before they are classified as QIIS by Telekom Security. Examples of QIIS are business reporting agencies such as Dun&Bradstreet or GLEIF. The information provided by the applicant is used for an automated or manual comparison with the QIIS databases.

Attestation: The applicant proves the legal, physical and operational existence and identity of an organization by presenting a letter of attestation issued by a notary (Verified Professional Letter (VPL) according to [EVCG]) or by presenting an official attestation from a public authority. A prerequisite for the acceptance of a notarial attestation is, that the notary is listed in an appropriately recognized notary directory.

Onsite: Applying organizations are identified during an onsite visit by CA or RA staff.

OrgDB: Enterprise RAs of applying organizations can obtain relevant internal organizational certificate data, e.g., device identifiers, names of organizational units, etc., from a reliable internal database or comparable data source. The data source must be appropriately protected and maintained to ensure the accuracy of the data.

3.2.3 Authentication of individual identity

The following methods are used to validate the identity of natural persons according to Section 4.2.1.

PersIdent: Natural persons are personally identified by a RA (internal/external) on the basis of an official identification document.

PostIdent: Natural persons are identified by means of an official identification document via the "PostIdent" service of Deutsche Post.

eID: Natural persons are identified by means of an electronic identification in accordance with [eIDAS#24].

Attestation: Natural persons are identified by means of a VPL or by official attestation from a public authority.

[SMIME] **HR-DB:** Enterprise RAs of applying organizations may use relevant certificate data for employees from a reliable internal database or comparable data source, provided that personal or comparable identification has taken place as part of the standard processes in accordance with the preceding procedures. The data source must be appropriately protected and maintained to ensure the accuracy of the data.

3.2.4 Non-verified subscriber information

Only information validated according to the described methods is included in a certificate.

3.2.5 Validation of authority

Depending on the applicable policy, the authenticity of a certificate application and, if applicable, the authorization of an applicant to request certificates on behalf of another natural person or organization are validated.

[OVCP] The authenticity of a certificate application is validated via a verified method of communication (mail, telephone, fax, email, etc.) with the organization to be included in the certificate, whereby the selected method of communication is based on a source described in section 3.2.2. Organizations can specify in writing the natural persons, that are authorized to apply for certificates. In this case only applications from the specified persons are accepted. Upon a written request of an organization, Telekom Security provides a list of the persons, specified for this organization. For Enterprise RAs, the applicant is identified during the setup process and, if he or she is not authorized to represent the organization, a power of attorney signed by an authorized representative is requested.

[EVCP], [QEVCP-w] The authorization of the contract signer and the certificate approver are validated via a corresponding power of attorney if they are not authorized to represent the company themselves. Identification of the contract signer is performed using one of the methods described in Section 3.2.3. The authenticity of a certificate request is validated via a verified method of communication (mail, telephone, fax, email, etc.) with the contract signer or certificate approver. The method of communication is validated via the sources described in section 3.2.2.

[SMIME] For Enterprise RAs, the applicant is identified during the setup process and, if the applicant is not authorized to represent the company, a power of attorney signed by an authorized representative is requested.

3.2.6 Criteria for interoperation

If necessary and reasonable, Telekom Security cross-certifies its own Root CAs, e.g., issuing a cross certificate from a known and trusted Root CA certificate to a new Root CA certificate, which is not yet known and/or trusted in all applications. All cross certificates are published in the CCADB.

3.2.7 Validation of control over a domain or IP address

The following methods are used to validate control over a domain:

- **Constructed email to domain contact (method [BR#3.2.2.4.4])**
  Sending a random value to "admin", "administrator", "webmaster", "hostmaster", or "postmaster" of the domain and receiving a confirming response using the random value.
- **DNS Change (method [BR#3.2.2.4.7])**
  Providing a uniquely specified random value in the DNS TXT record of the domain that is prefixed by a specified label.
- **Validating Applicant as a Domain Contact (Method [BR#3.2.2.4.12])**
  Validation of the applicant as a domain contact. This method is only used for domains of the Deutsche Telekom AG group.
- **Agreed-Upon Change to Website v2 (Method [BR#3.2.2.4.18])**
  Providing a uniquely specified random value in a file in the "/.well-known/pki-validation" directory.
- **Agreed-Upon Change to Website - ACME (method [BR#3.2.2.4.19])**
  Use of the ACME HTTP Challenge as defined in RFC 8555 Section 8.3 and supplemented by the requirements of [BR].

For wildcard certificates, the requirements of [BR#3.2.2.6] are met based on the ICANN domains of the Public Suffix List. The methods listed above, with the exception of [BR#3.2.2.4.18] and [BR#3.2.2.4.19], are also used for validating wildcard domains.

For methods [BR#3.2.2.4.7], [BR#3.2.2.4.18], [BR#3.2.2.4.19] and according to the requirements for MPIC ([BR#3.2.2.9]), the domain validation is performed via three different network perspectives. The validation is considered positively completed if it is positively completed by the primary and at least one other network perspective.

The following methods are used to validate control over an IP address.

- **Agreed-upon change to website (method [BR#3.2.2.5.1])**
  Providing a uniquely specified random value in a file in the "/.well-known/pki-validation" directory.
- **Email, Fax, SMS, or Postal Mail to IP Address Contact (method according to [BR#3.2.2.5.2])**
  Sending a random value by email, fax, SMS, or postal mail and receiving a confirming response using the random value.
- **Reverse Address Lookup (method [BR#3.2.2.5.3])**
  The applicant's control is proven by the control over a domain name determined by reverse-IP lookup.
- **Phone Contact with IP Address Contact (method [BR#3.2.2.5.5])**
  Calling the phone number of the IP address contact and receiving a response that confirms the request for validation of the IP address.

3.2.8 Validation of control over a mail address

The following methods are used to validate control over email addresses:

- **Validating authority over mailbox via domain (method [SBR#3.2.2.1])**
  The subscriber proves control over an email address by proving control over the entire mail domain based on one of the methods listed in Section 3.2.7 for controlling a domain.
- **Validating control over mailbox via email (method [SBR#3.2.2.2])**
  An individual and limited token is sent via email to the email address to be validated and the subscriber must use this token in the service portal.
- **Validating applicant as operator of associated mail server(s) (method [SBR#3.2.2.3])**
  Confirming control of the SMTP FQDN using one of the methods listed in section 3.2.7 for controlling a domain.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Depending on the Trust Service and taking into account the validity period of validations and evidence in accordance with Section 4.2.1, identification and authentication for Re-Key is based on the successful authentication of the applicant by logging into the corresponding customer account, by specifying a secret service password or on the basis of the existing certificate and private key ([SMIME]), provided that these are still valid.

3.3.2 Identification and authentication for re-key after revocation

Re-Key is not supported for revoked certificates.

3.4 Identification and authentication for revocation request

Subscribers can authorize revocation of their own certificates after successful authentication at the portals and interfaces provided.

In addition, the relevant RA (e.g., Enterprise RA) and the CA itself have the option to revoke in accordance with this CPS.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Entities with which business is not permitted due to legal or internal regulations are excluded from being valid applicants.

[EVCP] Only private and public organizations from the DACH-region are valid applicants.

4.1.2 Enrollment process and responsibilities

Applicants can submit certificate applications via the service portals and interfaces (e.g., ACME, CMP) provided. Depending on the certificate type, the application process includes the following (in a potentially different order):

- Provision of contact information
- Generation of a key pair in accordance with the applicable requirements of this CPS or the Terms of Use by the subscriber or, if permitted, by the CA
- Provision of the attributes to be included in the certificate by the applicant, including a certificate signing request (CSR, e.g., PKCS#10) if necessary
- Acceptance of the Terms of Use, Privacy Policy, General Terms and Conditions
- Provision of additional evidence, if necessary

Upon requesting a certificate, at least the mail address is required as contact data, if not already provided upon registration of the customer account.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Certificate applications are checked for completeness, accuracy and authenticity. Manual activities associated with identification and authentication are performed exclusively by personnel in trusted roles.

Domains, IP addresses, mail domains: All FQDNs, IP addresses and email addresses to be included in a certificate are validated according to the methods described in Section 3.2.7 and Section 3.2.8. The validation of domains (including mail domains) or IP addresses and the validation of EV certificate applications in general are performed by the CA itself and not delegated to external RAs. However, if a domain (Authorization Domain Name) has been validated accordingly, an Enterprise RA can validate certificate requests for subdomains or email addresses under the already validated domain on its own authority.

Organization: All organization data to be included in a certificate or necessary for unique identification, i.e., organization name, street name and number, location, postal code, state or province, country, and, if applicable, organization type, parents, subsidiaries or affiliates, status of the organization, as well as a nationally recognized identity number or date of incorporation are validated using the QGIS, QIIS, Attestation, or Onsite methods described in Section 3.2.2, although the QIIS method is not used to validate organizational data in the context of [EV] or [QEVCP-w]. Internal organizational information such as organizational entity names (relevant for [SMIME] only) and device identifiers associated with an organization can be obtained or validated from an Enterprise RA using the OrgDB method as described in Section 3.2.2.

Natural person: All natural persons that are included as a subject of a certificate or that have to be validated as part of the application process in accordance with the applied policy are identified using the methods described in Section 3.2.3. The identification includes at least the attributes necessary for unique identification, in particular the full name.

Internal organizational information about employees such as employee identifiers or email addresses (does not include the general validation of the domain portion) can be obtained or validated from an Enterprise RA using the HR-DB method according to Section 3.2.3.

Authorization and authenticity: The validation of the authorization of an applicant to act on behalf of an organization in a specific role or to request certificates for that organization as well as the authenticity of the respective applications are validated according to Section 3.2.5.

Prior Validations and evidence can be reused, provided that they are not older than the following deadlines:

- Control over (email) domain or IP address: 398 days
- Control over mailbox (validated via email): 30 days
- Validation of identity and authorization according to Section 3.2: 825 days
  (398 days for [EV], [QEVCP-w])

4.2.2 Approval or rejection of certificate applications

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

[EVCP], [QEVCP-w] Subsequently obtained information is confirmed by the Certificate Approver or Contract Signer. In addition, each application is cross-checked by another RA employee who was not involved in the previous application validation (four-eyes principle).

Certificate applications will be rejected if the corresponding key

- was demonstrably generated by means of a faulty method,
- can be compromised via a known or proven method (includes Debian Weak Keys, ROCA),
- is known to be compromised,
- [TLS] has previously been generated by the CA itself,
- does not meet the quality criteria according to Section 6.1.5 and Section 6.1.6.

For all certificates, the CAA records in the DNS are checked for all FQDN entries contained in the request at the start of an application and immediately before a certificate is issued. The CAA check is, according to the requirements for MPIC ([BR#3.2.2.9]), performed via three different network perspectives. The validation is considered positively completed if it is positively completed by the primary and at least one other network perspective. A certificate application is rejected if there is an entry in [TLS] "issue" or "issuewild" or in [SMIME] “issuemail” and none of the entries contains "telesec.de". Further entries of the CAA record are not supported. The CAA check is valid for 8 hours. If the query of a CAA record fails, the issuance of the certificate can still proceed, provided that

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

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

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

[EVCP] Wildcard EV certificates are denied. EV certificates for IP addresses are denied.

If all validation steps according to Section 4.2.1 have been successfully performed and none of the validation steps mentioned in this section result in a rejection, the certificate issuance is approved.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Telekom Security ensures that the integrity and authenticity of the data to be included in a certificate are protected by technical, organizational and personnel measures during issuance of certificates. In particular, it is ensured that all activities that trigger the issuance of a certificate originate from authorized RAs.

Issuance of Root and CA certificates requires management approval and is performed in the secure Offline-CA environment of the Trust Center as part of a certificate ceremony. The trusted roles involved in the ceremony and their tasks before, during and after the ceremony are described in a work instruction. This includes, among other things, the work steps for activating the Offline-CA and the HSMs in a multi-person principle with different roles. A certificate ceremony follows a defined protocol, is documented therein and is monitored by a qualified internal auditor as well as a qualified external auditor of a conformity assessment body (see Section 8.2). The successful performance of a ceremony is confirmed by the auditors in the protocol.

[TLS] All certificates are published as "pre-certificates" in a sufficient number of CT log servers (Certificate Transparency according to [RFC6962]) and checked by several lint tools before issuance. The Signed Certificate Timestamps (SCTs) are included in the final certificate.

All certificates are linted by several linting tools.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Subscribers are informed of the issuance of a certificate by email and/or the issued certificates are provided via the Trust Service specific interfaces.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Applicants commit to check the certificate upon receipt and, in the event of incorrect information in the certificate, to report immediately to Telekom Security. If no such report is made before the certificate is used, the certificate is deemed accepted.

4.4.2 Publication of the certificate by the CA

Applicants receive the certificates issued to them via the respective interfaces. In addition, publication in public or protected directories is supported by agreement with enterprise customers.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation, except for TLS server certificates, which are published in several CT log servers before they are issued. See Section 2.2 or 4.3.1 for more information.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The conditions for the usage of private keys and certificates by the subscriber are described in the Terms of Use and include, among other things, the protection of the private key and the use of the certificate in accordance with the intended purposes. Subscribers are obligated to comply with the Terms of Use by accepting them.

4.5.2 Relying party public key and certificate usage

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

The Terms of Use contain recommendations and information for Relying parties.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

The prerequisite for renewal is that the existing key has not been compromised or otherwise become unusable and the certificate has not been revoked due to a security incident.

[SMIME] The issuance of follow-up certificates with the same content and the same key depends on the key media.

4.6.2 Who may request renewal

According to Section 4.1.1.

4.6.3 Processing certificate renewal requests

Renewal requests are processed in the same way as new applications, whereby validations that have already been carried out and are still valid are reused (see Section 4.2.1) so that issuance takes place automatically, if possible.

4.6.4 Notification of new certificate issuance to subscriber

According to Section 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

According to Section 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

According to Section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

According to Section 4.4.3.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

If a private key is to be replaced, has been lost, or other reasons exist that require a key change, then a follow-up certificate with a new key but otherwise unchanged content can be requested. The prerequisite is that the existing certificate is not revoked.

[SMIME] Re-keying is only possible for certificates that are not based on a smartcard.

4.7.2 Who may request certification of a new public key

According to Section 4.1.1.

4.7.3 Processing certificate re-keying requests

Re-keying Requests are processed in the same way as new applications, whereby validations that have already been carried out and are still valid can be reused (see Section 4.2.1) so that issuance takes place automatically if possible.

4.7.4 Notification of new certificate issuance to subscriber

According to Section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

According to Section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

According to Section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

According to Section 4.4.3.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

A request for a new certificate must be submitted to modify certificate data. A dedicated process for certificate modification is not offered.

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

- 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 has been compromised or disclosed to an unauthorized person or organization 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 has not been issued or operated in compliance with this CPS,
- it is determined that 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 CA or the Sub CA to issue certificates in accordance with the requirements of this CPS expires or is revoked or terminated and no arrangements have been made for the continued operation of the revocation services,
- statutory provisions, judicial rulings or an instruction from a supervisory authority exist.

Furthermore, a Sub CA certificate is revoked, if the operator of the Sub CA applies for revocation, even without giving a reason. In this case a written revocation request, signed by Trust Center's Management (in the case of a Sub CA certificate of Telekom Security), resp. signed by an authorized person of DFN (in the case of a Sub CA certificate of DFN) is required.

A subscriber certificate is revoked if

- an authorized revocation request, even without giving reasons, has been received from the subscriber or, if applicable, from the respective RA
- relevant information in the certificate is not or no longer correct.
- no authorization of the certificate exists (anymore), this includes:
    - an information from the subscriber is available that the original application was not authorized and cannot or should not be authorized retroactively
    - [TLS] control over a FQDN or IP address specified in the certificate can no longer be trusted
    - [TLS] the use of a FQDN or IP address specified in the certificate is no longer allowed
    - [SMIME] the use of an email address specified in the certificate is no longer permitted
    - [SMIME] control over an email address or authorization over a domain can no longer be trusted
- a key weakness or compromise is demonstrated, this includes:
    - It is proven to Telekom Security that the private key has been compromised or given to an unauthorized person
    - It is proven to Telekom Security that a weak private key is used, which can be easily computed based on the public key (e.g., "debian weak key") or generated using a flawed method or other methods are known to compromise the private key
    - the private key no longer meets the requirements according to sections 6.1.5 and 6.1.6
- a violation of the CP, CPS or the Terms of Use is proven, this includes
    - the certificate has not been issued in accordance with the relevant CPS
    - the certificate has been misused
    - the subscriber has been suspended or revoked, if applicable
    - [TLS] a wildcard certificate has been used to authenticate a fraudulently misleading Sub-FQDN

In addition, all affected certificates are revoked if

- Telekom Security ceases operation and has not taken precautions for continuing operation of the revocation services,
- Telekom Security loses the authorization to issue certain certificate types and has not taken precautions for continuing operation of the revocation services or
- the private key of a CA has been compromised.

Revoked certificates do not get unrevoked.

Revocation reasons are set according to [TSCP].

4.9.2 Who can request revocation

The revocation of a certificate can be initiated by the CA, the responsible Enterprise RA, the subscriber or an authorized representative of the subscriber.

In addition, the revocation of a certificate can be triggered by other parties if it can be proven to Telekom Security that one of the revocation reasons listed in Section 4.9.1 exists. For more information, see Section 1.5.2 and Section 4.9.12.

4.9.3 Procedure for revocation request

Subscribers or their authorized representatives or, if applicable, responsible Enterprise RAs can authorize revocation of their certificates around the clock via the functions of their customer account or, after providing an individual revocation password for each certificate, via the support interfaces provided.

Telekom Security also offers an email interface that can be used to report certificate misuse and problem reports (see Section 1.5.2). Telekom Security processes these messages 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 report and any resulting revocations of the affected certificates.

4.9.4 Revocation request grace period

Subscribers are obligated via the Terms of Use to submit a revocation request without delay as soon as a revocation reason is identified in accordance with Section 4.9.1.

4.9.5 Time within which CA must process the revocation request

Sub CA certificates are revoked within seven days after receipt of an authorized revocation request. This period includes the time to handover the revocation status to the certificate status services. After revocation of a Sub CA certificate, the corresponding entry in the CCADB is updated. If the revocation of the Sub CA certificate is required due to a security incident, the CCADB is updated within 24 hours, otherwise within 7 days at the latest.

Subscriber certificates are revoked as soon as possible, but not later than within 24 hours after receipt of an authorized revocation request. This period includes the time to handover the revocation status to the certificate status services. This does not apply to revocations requested for a later date, e.g., due to a planned termination.

For revocations that are not based on authorized revocation requests but on other reasons for revocation listed in section 4.9.1 the following revocation deadlines apply:

- Subscriber certificates are revoked within 24 hours if a key weakness or compromise or a missing authorization of a certificate is proven to Telekom Security or Telekom Security loses its authorization to issue certificates according to [BR].
- Subscriber certificates are revoked as soon as possible but at the latest within 5 days if a violation of the CP, CPS or Terms of Use is proven to Telekom Security.

However, Telekom Security will, in justified cases, revoke certificates on a date specified by a relevant Root Store operator that deviates from the above deadlines.

Upon receipt of a problem report regarding a certificate, the facts and circumstances are investigated within 24 hours and initial feedback is provided to the subscriber and the reporting person regarding the findings available to date. The results of the analysis are then discussed with the subscriber and, if applicable, the reporting party and a decision is made as to whether revocation is necessary. If a revocation is necessary, taking into account the time specifications from Section 4.9.1 and taking into account the following aspects, the time of revocation is determined:

- Nature of the alleged problem (scope, context, severity, magnitude, risk of harm)
- Consequences of revocation (direct and collateral impact on subscribers and relying parties)
- Number of certificate problem reports received about a particular certificate or subscriber
- Entity making the complaint
- Relevant legislation

4.9.6 Revocation checking requirement for relying parties

Relying parties are required to check the status of certificates using the certificate status services provided in accordance with Section 4.10 before trusting a certificate.

4.9.7 CRL issuance frequency

Revocation lists containing information on revoked CA certificates (Certification Authority Revocation List (CARL)) are updated every 6 months at the latest and if required.

Revocation lists containing information on revoked subscriber certificates (Certificate Revocation List (CRL)) are updated regularly every 24 hours and if required.

4.9.8 Maximum latency for CRLs

Newly created CARLs and CRLs are published to the directories immediately after generation.

4.9.9 On-line revocation/status checking availability

Online status information is provided for all certificates via OCSP. The URL of the relevant OCSP responder is listed in the corresponding extension of each certificate.

4.9.10 On-line revocation checking requirements

Relying parties are encouraged to consider the specifications in [RFC6960] when checking a certificate status via OCSP.

4.9.11 Other forms of revocation advertisement available

No stipulation.

4.9.12 Special requirements related to key compromise

Subscribers can report a key compromise via the interfaces provided to them (see also Section 4.9.3).

In addition, any party can report a key compromise via the email address mentioned in Section 1.5.2. Corresponding reports should include a CSR that was created and signed with the compromised private key. The commonName in the CSR should contain an appropriately unambiguous description that indicates that the key has been compromised (e.g., "Compromised Key"). The certificate itself or at least a reference to it should also be included.

4.9.13 Circumstances for suspension

Suspension is only supported for S/MIME certificates issued to Deutsche Telekom AG employees. Suspension is performed in case of

- temporary unavailability of subscribers’ smart card,
- longer planned absences of an employee,
- suspicion of unauthorized use of subscribers’ smart card,

- timely planned leaving of an employee from the company (will be subsequently converted into revocation).

In such a case, the revocation reason is set to certificateHold.

4.9.14 Who can request suspension

Suspensions can be requested by the subscriber, RA or CA.

4.9.15 Procedure for suspension request

The suspension of certificates is triggered by automated processes or ordered by authorized persons after appropriate authentication and subsequently performed.

4.9.16 Limits on suspension period

The suspension period is limited to a maximum of 30 days for some suspension reasons (e.g., loss of a smart card) before the certificate is automatically revoked. Otherwise, there is no general limit.

4.10 Certificate status services

At least over the entire validity period of a certificate, both revocation lists signed by the CA and OCSP responses signed by a delegated OCSP Signer are provided.

[TLS] This also applies to pre-certificates.

4.10.1 Operational characteristics

All certificate status services are time-synchronized several times a day, but at the latest every 24 hours.

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

4.10.1.1 Operational characteristics for the provisioning of OCSP

OCSP responders are operated in conformity with [RFC6960].

Requests for certificates with unknown certificate serial numbers are answered with the status "unknown" and are logged.

OCSP responses are generated on demand and are given a value in the nextUpdate field that is 5 days after the thisUpdate value but are reused for a maximum of 2 hours for further requests.

4.10.1.2 Operational characteristics for the provisioning of CRLs

The value of the nextUpdate field of a CARL is at most 6 months after the value of the thisUpdate field.

The value of the nextUpdate field of a CRL is at most 5 days after the value of the thisUpdate field.

Depending on the Trust Service, revoked certificates are either still included in at least the next regular revocation list after they expire or they are not removed from revocation lists after they expire.

[QEVCP-w] Revoked certificates are not removed from revocation lists after they expire.

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 remediate disruptions as soon as possible.

Sufficient capacity is available so that the response time of the status services does not exceed 10 seconds under normal operating conditions.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

If a certificate revocation should be linked to the termination, the provisions described in Section 4.9.1 shall apply.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

[SMIME] The keys for end entity encryption certificates of the cPKI are stored in encrypted form for backup purposes. The encryption key is stored in an HSM.

Access or recovery is restricted to the certificate owners themselves and to their expressly authorized representatives. The authorization of orders for the recovery of encryption keys is only carried out after prior authentication and authorization check of the applicant.

Key recovery to third parties without the consent of the certificate owner is subject to the approval of the departments responsible for IT security, data protection and staff representation within the Group in accordance with group policies. This requires the consent of all the aforementioned bodies.

4.12.2 Session key encapsulation and recovery policy and practice

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The Trust Center of Telekom Security is within the scope of a security policy, approved by Group 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 [TSCP#5]. In particular, risk management comprises a risk analysis including likelihood of occurrence and impact of damage as well as appropriate risk treatment including a 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 assets, media and information are protected against loss, theft, damage or compromise by physical measures according to their criticality. These measures are set out in internal security concepts and other documents.

5.1.1 Site location and construction

The Trust Center infrastructure is located in data centers (including twin-core data center, geo-redundant) within Germany. The locations have been selected considering environmental conditions such as susceptibility to natural disasters and other sources of danger, based on a corresponding risk analysis. The construction and infrastructure of the buildings are designed for the secure operation of critical systems and meet the requirements for a high security zone.

The Trust Center’s premises are separated from other areas by additional enclosures and audited and certified according to "Trusted Site Infrastructure V3.2 Dual Site".

5.1.2 Physical access

The data centers have extensive physical security measures, including security personnel, secured entrances, burglar alarm systems, and multi-level access systems. In particular, the Trust Center’s premises are accessible only to authorized persons in trusted roles and visitors are permitted only when accompanied by such a person.

Access rights are reviewed regularly and as needed and adjusted if necessary.

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 backed up 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 premises themselves are protected against water ingress or water damage by further measures.

5.1.5 Fire prevention and protection

The data centers are protected against fire damage with structural measures appropriate to their criticality and in compliance with applicable fire protection regulations.

5.1.6 Media storage

Media is stored exclusively in the Trust Center's premises, protected from fire, water and unauthorized access.

5.1.7 Waste disposal

Confidential documents and data carriers are disposed of securely exclusively via certified disposal companies. In addition, all data carriers are erased using certified processes before they are disposed of. Data carriers are 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 Trust Center: has the overall responsibility for the Trust Center services provided
- Head of VDA: Contact for authorities in the context of qualified certificates according to eIDAS
- Solution Manager: is responsible for and manages a Trust Service
- Trust Center Information Security Officer: is responsible for the general implementation of ISMS processes
- RA employee (validation specialist): validates certificate requests, initiates issuance or manual revocation of certificates
- Administrator: installs, configures, and maintains the IT infrastructure
- Internal auditor: reviews certificates, processes, documentation and verifies the conformity of key ceremonies and root ceremonies on a regular basis and in the event of discrepancies
- Compliance Manager: regularly reviews the requirements underlying the Trust Services, coordinates these with the Solution Managers and coordinates the necessary audits by external auditors.

5.2.2 Number of persons required per task

For all roles listed in Section 5.2.1 at least one deputy is appointed.

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

The security-relevant and -critical activities for which at least dual control is required are:

- Generation, backup and recovery of CA keys

- Any activities at the Offline CA:
    - Issuance of certificates and revocation lists
    - Certificate revocation
    - Changes to the configuration
- Any access to the Offline HSMs (incl. backup HSMs)
- Validations of EV certificate applications
- Assessment of security incidents
- Activities within the scope of change management

5.2.3 Identification and authentication for each role

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

Prior to the delegation of a trusted role (or already at the time of hiring as an employee), the person is identified by presenting official identification and acceptance is obtained from this person as well as from the management of the Trust Center for the delegation of the role, the associated responsibility and the resulting duties to ensure security.

Roles are only transferred to persons as long as this does not lead to any conflicts of interest (see also Section 5.2.4) and independence is preserved, i.e., that

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

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

Persons accepting a role are officially appointed to the trusted role by Trust Center management and advised that they may only act in the assigned role when performing tasks assigned to the role.

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

Upon termination or change of employment relationship of an employee in a trusted role, its access rights are revoked within 24 hours.

5.2.4 Roles requiring separation of duties

The following roles are separated from each other so that an employee may only occupy the roles listed under one bullet point at a time:

- Head of Trust Center and/or Head of TSP
- Trust Center Information security officer and/or internal auditor
- Registration staff/Validation Specialist
- Administrator

Persons in the named roles can only be applicants for certificates if these certificates are requested on behalf of the person itself or Telekom Security’s Trust Center.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The management of the Trust Center is stable and has many years of experience with regard to the technical and organizational operation of the Trust Services offered. Furthermore, through training and experience, it is familiar in the areas of information security (incl. risk management, security procedures for personnel, etc.) and PKI technologies.

Employees meet the requirements in regard to sufficient expert knowledge to perform their activities correctly due to 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 data protection 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 have been identified by presenting an official identification document and demonstrate their trustworthiness by regularly submitting an official certificate of good conduct. Prior to initial employment, relevant degrees and references are also checked to determine suitability for the job.

5.3.3 Training requirements

All employees involved in registration activities are trained and tested on the following topics:

- Public Key Infrastructures
- Common threats to the information review process, including phishing and social engineering
- Authentication and validation policies and procedures in accordance with [TSCP], this CPS as well as [BR] and [EVCG], if applicable

Evidence of these trainings is kept and it is documented that each employee entrusted with registration activities has the required know-how before taking on the activities.

5.3.4 Retraining frequency and sequence

Employees are regularly (at least annually) made aware of information security and data protection and additionally on an ad hoc basis to current threats and security practices.

In addition, personnel in trusted roles receive regular training to maintain the required expertise.

5.3.5 Job rotation frequency and requirements

No stipulation.

5.3.6 Sanctions for unauthorized actions

Employees are accountable for their actions. Violations of instructions have disciplinary consequences according to the severity of the violation.

5.3.7 Independent contractor requirements

Independent contractors, namely external RAs or Enterprise RAs are contractually obligated to also comply with the processes and measures set forth herein, as applicable.

5.3.8 Documentation supplied to personnel

Role descriptions are available to all role owners which, in addition to the responsibilities and duties arising from the role, contain at least the necessary

- (minimum) permissions,
- separation of duties,
- dual control activities,
- training and awareness-raising measures

In addition, relevant manuals for systems and processes as well as FAQs are provided.

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

5.4 Audit logging procedures

5.4.1 Types of events recorded

The following events (as listed in detail in [TSCP#5.4.1]) are logged continuously including a description of the event, the precise time and, if applicable, the identity of the trigger:

- All essential certificate lifecycle events of the certificate and key management systems as well as the status services
- All security-related events on the PKI and security systems
- Installation, update and removal of software on/from the PKI systems
- Physical entrances and exits to and from the security zones

The time of the logging systems is synchronized with a central and trusted source several times a day (see Section 6.8).

5.4.2 Frequency of processing log

Log data is evaluated as follows:

- Security relevant events are evaluated as described in Section 6.6.2.
- All other log data is evaluated, when necessary, e.g., for troubleshooting or analysis activities.

5.4.3 Retention period for archive

All certificate lifecycle log data is retained until two years after the expiration of the associated certificates and, for CA certificates, two years after the deletion of the CA keys.

All other log data is retained for two years after its occurrence.

5.4.4 Protection of audit log

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

Log data is provided, when necessary, e.g., in legal proceedings or at the request of internal or external auditors.

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system

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

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessment

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

The following records are archived as detailed in [TSCP#5.5.1] with date, time, and, if applicable, identity of the person acting:

- Application/certificate history and, if applicable, life cycle of keys
- Evidence in the context of issuance, renewal, revocation of certificates (registration information) [TLS] This includes the method according to [BR#3.2.2.4] and [BR#3.2.2.5] used to validate control over domains and IP addresses as well as the version of the [BR] on which the validation was based
- All published CP, CPS and Terms of Use
- Official certification documents and audit reports
- Relevant documentation related to the security of the systems

5.5.2 Retention period for archive

All records mentioned in Section 5.5.1, with the exception of the documentation related to the security of the systems, are kept for seven years. For records relating to the certificate history, this period begins with the expiration of the certificates and, in the case of CA certificates, with the deletion of the CA keys.

Relevant documentation related to the security of the systems is kept for two years.

5.5.3 Protection of archive

Technical and organizational measures have been implemented to ensure and monitor the availability, integrity and confidentiality of records during retention.

Access to electronically stored information as well as paper archives is restricted to authorized Trust Center personnel.

5.5.4 Archive backup procedures

The electronic storages have multiple redundancies and are regularly backed up.

5.5.5 Requirements for timestamping of records

See Section 6.8.

5.5.6 Archive collection system (internal or external)

Only internal archiving systems are used.

5.5.7 Procedures to obtain and verify archive information

The archived data listed in Section 5.5.1 is evaluated and made available, if necessary, e.g., in the event of problem reports or legal proceedings or upon request of internal or external auditors.

Access to the information has to be requested from one of the following roles:

- Head of Trust Center
- Head of VDA
- Trust Center Information Security Officer
- Solution Manager of the corresponding Solution

After approval of the request, the information is provided via the authorized personnel (see chapter 5.5.3).

5.6 Key changeover

Before a CA certificate expires, a new CA certificate is issued in good time. The period between the publication of the new CA certificate and the taking out of service of the expiring CA certificate is chosen to be sufficiently long, so that subscribers do not experience any interruption in their operations. The newly issued CA certificates are distributed in the same way as existing CA certificates, as described in Section 2.2.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The Trust Center's emergency documentation addresses all requirements of [TSCP#5.7.1] and is disclosed to auditors as required.

Employees have several options (technical interface, direct contact with the ISMS, employee portals) for reporting (information security) incidents and are obligated to do so. Reports and alarms are followed up by qualified personnel within a reasonable period of time, depending on the criticality.

Security incidents with a significant impact on a Trust Service or on private data are reported to the appropriate authorities within 24 hours, depending on the nature and context of the incident.

Natural persons or organizations who use Telekom Security's Trust Services and are potentially negatively affected by a security incident will be informed immediately about the security incident.

If an incident represents a violation of a Root Store policy, the Trust Center PKI Compliance Management promptly prepares an incident report taking into account the relevant requirements. If necessary, the issuance of affected certificate types is stopped until the problem is solved or further damage can be excluded.

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

Regular data backups of all relevant systems are performed so that they can be restored if necessary. The data backups are kept in a geo-redundant manner 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 private CA key is treated as an emergency scenario and handled according to the processes defined in the emergency documentation. The affected keys are no longer used until final clarification.

In the event that a CA key is compromised, revocation of the CA certificate as well as all affected subscriber certificates is initiated and all affected subscribers, Root Stores and other entities with which corresponding agreements have been concluded are informed.

5.7.4 Business continuity capabilities after a disaster

Business continuity resp. the provision of the services and systems required for compliant continuation of operation are ensured by technical and organizational measures. In addition to geo-redundant operation, these include emergency documentation and emergency management set up in accordance with [TSCP#5.7.1]. In the event of an emergency, operations are reinstated within the period specified in the emergency documentation after all causes have been eliminated by appropriate mitigation measures.

5.8 CA or RA termination

If continuation of a Trust Service is not possible, secure termination is ensured in accordance with a continuously updated termination plan that minimizes potential disruption to subscribers and relying parties.

All affected subscribers, Root Stores and subcontractors will be informed in good time of any planned termination. In addition, corresponding information will be made available on the Trust Center's web pages.

Operation of the status services will be handed over to Deutsche Telekom AG or T-Systems International GmbH, which act as qualified TSPs in accordance with [eIDAS] and the German “Vertrauensdienstegesetz” (Trust Services Act), until the validity of all subscriber certificates expires. Likewise, the records archived in accordance with Section 5.5.1 are handed over to Deutsche Telekom AG or T-Systems International GmbH for safekeeping until the specified retention period expires. Customer data and other data, that does not need to be retained, is deleted.

All certificates not yet revoked at the time of the planned termination will be revoked and the private keys of the affected CAs will be destroyed.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA and OCSP-Signer key pair generation

Generation of CA and OCSP-Signer keys requires management approval and is performed in the secure environment of the Trust Center as part 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. This includes, among other things, the work steps for activating the HSMs, key generation and backup in a multi-person principle with different roles. Key generation is always performed on the HSMs according to Section 6.2.1, that are also intended for subsequent operation, i.e., CA and OCSP-Signer key pairs are not generated by the issuing (Root-) CA.

All ceremonies for CA keys follow a specified protocol, are documented therein and are monitored by a qualified internal auditor and by a qualified external auditor of a conformity assessment body (see Section 8.2). The successful performance of a ceremony is confirmed by the auditors in the protocol.

CA key pairs are generated anew for each new CA.

6.1.1.2 RA key pair generation

RA key pairs are generated in smartcards according to Section 6.2.1.

6.1.1.3 Subscriber key pair generation

[TLS] Key pairs are generated by the subscriber itself.

[SMIME] Key pairs are generated by the subscriber or by the CA.

The CA generates key pairs for end-entities in certified cryptographic modules (HSM or smartcard) and protects the keys in terms of confidentiality and integrity.

Subscribers who generate their own keys are informed about the permitted key algorithms and parameters.

6.1.2 Private key delivery to subscriber

Private keys for subscriber certificates are provided to subscribers in PIN-protected smartcards or in the form of password-protected PKCS#12 files via secure channels. Corresponding passwords or PINs are transmitted to the subscribers via separate secure channels.

6.1.3 Public key delivery to certificate issuer

Public keys are handed over by applicants using PKCS#10 requests over secure communication channels.

6.1.4 CA public key delivery to relying parties

All CA certificates are published as described in Section 2.2.

6.1.5 Key sizes

Only RSA keys with a minimum length of 2048 bits and a modulo length divisible by 8 are generated or accepted.

Only EC keys based on the NIST P-256 or NIST P-384 curves are generated or accepted.

6.1.6 Public key parameters generation and quality checking

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

For EC keys it is checked that the point is a normalized point on the desired curve, that it is a multiple of the generator point, and is not the point at infinitely.

6.1.7 Key usage purposes

All certificates contain a keyUsage and extendedKeyUsage extension according to Section 7.1.2, which specifies the permitted use of the keys associated with the certificate according to [RFC5280].

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

- its own Root CA certificate,
- Sub CA certificates,
- OCSP signer certificates and
- revocation lists (CARLs).

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

- subscriber certificates,
- OCSP signer certificates and
- revocation lists (CRLs).

The usage of OCSP signer's private keys is limited to the signing of

- OCSP responses.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

All HSMs used are certified according to FIPS 140-2 Level 3 and are operated in the corresponding FIPS mode. The manufacturer-specific mechanisms are used to protect the HSMs during operation, transport and storage.

All smartcards used are evaluated according to CC EAL4+.

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

Generation, backup, recovery and deletion of private CA keys are only possible under dual control, see Section 6.1.1, 6.2.4 and 6.2.8. Authentication tokens are used when importing and exporting keys to and from the backup HSMs, which enforce a multi-person control.

6.2.3 Private key escrow

Escrow of private keys is not supported.

6.2.4 Private key backup

Private CA keys are backed up exclusively under dual control and as part of a key ceremony to backup HSMs, which are kept at a comparable security level to the HSMs in operation.

With regard to the subscriber keys, only the private keys for encryption certificates of Deutsche Telekom AG employees are backed up. The keys are protected by means of encryption keys, which are themselves stored in HSMs.

6.2.5 Private key archival

An archival of private keys is not supported.

6.2.6 Private key transfer into or from a cryptographic module

Private CA keys are only transferred encrypted to or from backup HSMs for the purpose of backup or recovery (see Section 6.2.4). The work steps are performed as part of a key ceremony and at least under dual control.

It is not possible to transfer private RA or subscriber keys to or from smartcards, with the exception of private keys for encryption certificates of Deutsche Telekom AG employees (see Section 6.2.4), which can only be imported to smartcards, but not exported from smartcards.

6.2.7 Private key storage on cryptographic module

The keys stored in the cryptographic modules are stored securely using the functions provided by the cryptographic modules.

6.2.8 Method of activating private key

An activation of private CA keys is performed by persons in trusted roles using the functions provided by the HSM.

For initial activation, the smartcards of the subscribers must be changed from the "Zero PIN" state to the operating state by setting a PIN of at least six digits. In the operating state, the PIN must be entered for each use of the private key.

6.2.9 Method of deactivating private key

Deactivation of private CA keys is performed by persons in trusted roles using the functions provided by the HSM.

6.2.10 Method of destroying private key

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

The destruction of keys is performed analogue to the generation in a key ceremony (see Section 6.1.1) and considers all copies of the keys. The keys are destroyed with the functions provided by the HSM.

If cryptographic modules are decommissioned at the end of their lifecycle 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

The public keys are archived as part of the archiving of certificates according to Section 5.5.2.

6.3.2 Certificate operational periods and key pair usage periods

The validity date of a certificate does not exceed the validity date of the issuing CA certificate.

The following maximum certificate validity periods apply:

▪ Root CA certificates	25 years
▪ Sub CA certificates	10 years
▪ [TLS] Subscriber certificates	397 days
▪ [SMIME] Subscriber certificates	825 days (legacy certificates: up to 1185 days)

6.4 Activation data

6.4.1 Activation data generation and installation

The activation data of the HSM is generated and installed during commissioning of the HSM in in a four-eyes principle as part of a defined change process, using the functions provided by the HSM.

[SMIME] The PINs and PUKs for subscriber keys on smartcards are either generated by a secure random number generator of the CA and installed as part of the smartcard personalization process or are assigned by the subscriber after receiving the smartcard in “Zero PIN”-state and verifying its integrity.

6.4.2 Activation data protection

The activation data of the HSM is known only to persons in trusted roles. The group of persons with knowledge is restricted to the minimum required. With regard to the HSM for Root CAs, the activation data is only known in part to the respective persons, so that no single person can gain sole access.

Subscribers must protect the PINs and PUKs for smartcards on their own responsibility in accordance with the Terms of Use.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Only trustworthy systems are used 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 and dimensioned according to their criticality or damage potential.

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

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

The required segregation 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 permissions. This includes the use of personalized accounts. All accounts are reviewed regularly, but at least every three months, and changed or deleted as necessary within a reasonable period of time.

All accounts are protected with multi-factor authentication or strong passwords, complying with the requirements of [TSCP#6.5.1].

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

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

Only software from reputable manufacturers, that observe the usual security measures for the development of IT security systems and have many years of experience, is used. Release planning and documentation are carried out in accordance with the release management specifications. New versions of software (planned updates) or bug fixes (short-term bug fixes) are only transferred to the effective system after extensive testing in a test environment.

The Trust Center's development, test and production environments are operated on different hardware in different network segments and are therefore completely separated from each other.

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. Changes that affect the defined security level are approved in advance by management and, if necessary, by the ISMS.

The integrity of the systems is continuously monitored for changes. In the event of modifications that have not been made on the basis of an authorized change, the resulting alarms are investigated by qualified personnel.

Systems log all security relevant events mentioned in Section 5.4.1.

Security patches will be applied within a reasonable time, but within 6 months at the latest, unless they introduce additional vulnerabilities or instabilities that outweigh the benefit of the patch. The reasons for not applying security patches are documented.

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

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

Networks and systems are protected against unauthorized access and attacks using multi-layer firewalls, IDS and IPS, segmentation, and other protective measures. 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.

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.

Networks used to administer systems are separated from operational networks.

All systems critical to CA operation are located in secure or high secure zones. The same minimum-security requirements apply to all systems within a zone. The certificate management system and the associated HSMs of the Root CAs are operated on a pure Offline CA in a high secure zone, i.e., in a physically isolated network with no network connection to other networks.

The communication is generally encrypted on several layers and is realized for almost all systems, but at least for the trusted systems, via trusted channels that ensure secure identification of their endpoints.

All external network connections are redundant.

After significant system or network changes, a vulnerability check is usually performed on public and private IP addresses within one week, but at least once per calendar quarter.

Penetration tests are performed when the infrastructure or applications are put into operation or significant changes are made, but at least once a year.

Vulnerability scans and penetration tests are performed by individuals or organizations that have the skills, tools, abilities, ethics, and independence necessary for reliable testing and documentation. The performance is documented together with the results.

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

6.8 Timestamping

All systems are regularly synchronized (several times a day) with exact time information via a time server and the Network Time Protocol (NTP), so that the timestamps on logs and records are reliable.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

Note: The certificate profiles described in this section reflect current practice. Older certificates, in particular certificates from before the validity of this CPS, may show minor deviations. However, these certificates retain their validity unless explicit reference is made to their invalidity.

All certificate profiles comply with [RFC5280] and [X.509].

All certificates receive a unique serial number under the respective CA, generated by a cryptographically secure pseudo-random number generator and with an entropy of at least 126 bits.

The validity period of each certificate begins with issuing or, if applicable, later, but validity is never backdated.

7.1.1 Version number

All X. 509 certificates are issued in version 3.

7.1.2 Certificate extensions

7.1.2.1 Root CA certificates

Only the following certificate extensions are set:

- **authorityKeyIdentifier** (optional): contains "keyIdentifier" according to [RFC5280 #4.2.1.1].
- **subjectKeyIdentifier**: contains "keyIdentifier" according to [RFC5280 #4.2.1.2].
- **keyUsage** (critical): contains "keyCertSign" and "cRLSign".
- **basicConstraints** (critical): The "cA" flag is set to "true". The "pathLenConstraint" is not set.

7.1.2.2 Sub CA certificates

Only the following certificate extensions are set:

- **authorityKeyIdentifier**: contains "keyIdentifier" according to [RFC5280 #4.2.1.1].
- **subjectKeyIdentifier**: contains "keyIdentifier" according to [RFC5280 #4.2.1.2].
- **keyUsage** (critical): contains "keyCertSign" and "cRLSign".
- **certificatePolicies**: contains those policy OIDs according to Section 7.1.6 which may be issued under the respective Sub CA. Alternatively, the policy OID "anyPolicy" (2.5.29.32.0) is set to make no such restriction. However, Sub CA certificates are used in any case to issue only one certificate type ([TLS] or [SMIME]). The qualifier cPSuri is optionally set and contains a corresponding http URL to a CPS or repository.
- **basicConstraints** (critical): The "cA" flag is set to "true". The "pathLenConstraint" is set with “0”.
- **extendedKeyUsage**:
  - [TLS] Sub CA certificates contain "id-kp-serverAuth" and optionally "id-kp-clientAuth".
  - [SMIME] Sub CA certificates contain "id-kp-emailProtection" and optionally "id-kp-clientAuth".
- **cRLDistributionPoints**: contains at least one http URL to the issuing CA's CRL. In some cases, additional entries for LDAP are provided.
- **authorityInfoAccess**: contains a corresponding http URL for accessMethod 1.3.6.1.5.5.7.48.1 (ocsp) and accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers). In some cases, additional entries for LDAP are provided.

7.1.2.3 Subscriber certificates

Only the following certificate extensions are set:

- **authorityKeyIdentifier**: contains "keyIdentifier" according to RFC5280 #4.2.1.1.
- **subjectKeyIdentifier**: contains "keyIdentifier" according to RFC5280 #4.2.1.2.
- **keyUsage** (critical):
    - [TLS] contains "digitalSignature" and optionally "keyEncipherment" (only RSA keys) or "keyAgreement" (only ECC keys).
    - [SMIME] contains a combination of the values "digitalSignature", "keyEncipherment" and "dataEncipherment" according to [RFC5280] that corresponds to the respective purpose.
- **certificatePolicies**: according to Section 7.1.6. The qualifier cPSuri is set and contains a corresponding http URL to a CPS or a repository.
- **subjectAlternativeName**: according to Section 7.1.4.
- **basicConstraints** (critical): the extension is set optionally. If it is set, the "cA" flag is set to false and the "pathLenConstraint" is not set.
- **extendedKeyUsage**:
    - [TLS] contains "id-kp-serverAuth" and optionally "id-kp-clientAuth".
    - [SMIME] contains "id-kp-emailProtection" and optionally "id-kp-clientAuth".
- **cRLDistributionPoints**: contains at least one http URL to the issuing CA's CRL.
    - [SMIME] Optionally contains further entries for LDAP.
- **authorityInfoAccess**: contains a corresponding http URL to accessMethod 1.3.6.1.5.5.7.48.1 (ocsp) and accessMethod 1.3.6.1.5.5.7.48.2 (caIssuers).
    - [SMIME] Optionally contains further entries for LDAP.
- **cabfOrganizationIdentifier**: [EVCP], [QEVCP-w] Content and syntax according to [EVCG#7.1.2.2].
- **signedCertificateTimestampList**: [TLS] Contains SCTs from different CT logs according to the specifications of the relevant Root Stores regarding the number of SCTs and recognized CT log servers of different operators.
- **qcStatements**: [QEVCP-w] According to ETSI EN 319 412-5.
- **Microsoft-specific extensions**: [SMIME] Optionally contains the Microsoft-specific certificate extensions
    - certificateTemplate
    - applicationCertPolicies

7.1.3 Algorithm object identifiers

Only the following algorithms to sign certificates, CARLs, CRLs and OCSP responses are used:

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

Certificates for RSA keys contain the OID 1.2.840.113549.1.1.1 (rsaEncryption) in the subjectPublicKeyInfo.

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

The encodings comply with [BR#7.1.3] and [MOZRP#5.1].

7.1.4 Name forms

In general,

- the name of the issuer ("Issuer DN") is set identically (byte-for-byte) to the "Subject DN" of the issuing CA certificate in all certificates,
- the attributes commonName, organizationIdentifier, organizationName, countryName are set at most once,
- all attributes use the same language encoding,
- [TLS] the order of the attributes follows [BR#7.1.4.2],
- attributes do not consist of metadata (e.g., spaces, "n/a" or "-") only.

7.1.4.1 Root CA certificates

Only the following attributes are set:

- **countryName**: always contains the value "DE".
- **organizationName**: contains the organization name of Deutsche Telekom AG or an affiliate.
- **commonName**: contains a uniquely assigned name that reflects the affiliation with Deutsche Telekom AG or an affiliate.
-

In legacy certificates, additional attributes may be set, e.g., organizationUnitName.

7.1.4.2 Sub CA certificates

Only the following attributes are set.

- **countryName**: always contains the value "DE".
- **organizationName**: contains the organization name of Deutsche Telekom AG or an affiliate.
- **commonName**: contains a name uniquely assigned under the respective Root CA, which reflects the affiliation with Deutsche Telekom AG or an affiliate.

In legacy certificates, additional attributes may be set, e.g., organizationalUnitName.

7.1.4.3 Subscriber certificates

All subscriber certificates contain a subjectAltName and a subjectDN according to Section 3.1. Only the following contents are set for the certificate types specified in each case.

subjectAltName

- [TLS] Contains at least one entry of type dNSName or iPAddress according to validation. No internal names (definition according to [BR]), reserved IP addresses or .onion domains are included. FQDNs consist of P labels or Non-Reserved LDH labels.
- [SMIME] Contains at least one email address as RFC822 name according to validation. In addition, additional names (e.g., UPN) are set if necessary.

subjectDN

- **countryName**
  [OVCP], [EVCP], [QEVCP-w], [SMIME] Contains the ISO-3166-1 country code (two characters) according to validation. When using pseudonyms (SMIME only), the value "DE" (country of domicile of Telekom Security) is set as an alternative.
- **stateOrProvinceName + localityName**

[OVCP], [EVCP], [SMIME] At least one of the attributes is set according to validation.
[QEVCP-w] The attribute localityName is set.

- **streetAddress + postalCode**
  [OVCP], [EVCP], [QEVCP-w], [SMIME] The attributes are set optionally and according to validation.
- **organizationName**
  [OVCP], [EVCP], [QEVCP-w], [SMIME] Contains the organization name validated according to Section 3.2.2. If necessary, common abbreviations may be used and the legal form may be omitted, provided that the uniqueness of the organization is maintained.
- **same + givenName**
  [SMIME] Contain the respective first and last name for natural persons according to validation unless a pseudonym is set. Names with only one name component are listed in the surname.
- **organizationalUnitName**
  [SMIME] The attribute is set optionally and contains additional validated information, e.g., via the method OrgDB as described in Section 3.2.2.
- **commonName**
  - [TLS] Contains exactly one FQDN or IP address listed in the subjectAltName.
  - [SMIME] Contains the name of the natural person, organization or an email, group, function, system or pseudonym.
- **emailAddress**
  [SMIME] Is optionally set and contains an email address listed in the subjectAltName.
- **Pseudonym**
  [SMIME] The attribute is set optionally and in consideration of Section 3.1.3. If it is set, the givenName and surname attributes are not set.
- **businessCategory**
  [EVCP], [QEVCP-w] According to [TSCP#7.1.4] resp. [EVCG#7.1.4.2.3].
- **jurisdictionOfIncorporationCountryName, -StateOrProvinceName, -LocalityName**
  [EVCP], [QEVCP-w] According to [TSCP#7.1.4] resp. [EVCG#7.1.4.2.4].
- **serialNumber**
  - [EVCP], [QEVCP-w] According to [TSCP#7.1.4] resp. [EVCG#7.1.4.2.5].
  - [SMIME] The attribute is optionally set to distinguish different entities with otherwise identical subjectDN, if necessary.
- **organizationIdentifier**
  [SMIME] Contains a value according to [TSCP#7.1.4] for legal persons or organizational entities related to legal persons.

7.1.5 Name constraints

Name constraints are not supported.

7.1.6 Certificate policy object identifier

[TLS] The respective policy OIDs according to [BR] resp. [EVCG] are set. Depending on the Trust Service these are optionally supplemented by the respective policy OIDs according to ETSI and/or the specific OIDs

- 1.3.6.1.4.1.7879.13.23.1 (for OV)
- 1.3.6.1.4.1.7879.13.24.1 (for EV)

of Telekom Security.

[QEVCP-w] For qualified website certificates, the corresponding policy OID according to ETSI is also set.

[SMIME] The respective policy OIDs according to ETSI ([LCP], [NCP]) or, for internally issued certificates, the specific OID 1.3.6.1.4.1.7879.13.26 of Telekom Security are set.

7.1.7 Usage of Policy Constraints extension

The extension policyConstraints is not set.

7.1.8 Policy qualifiers syntax and semantics

If policy qualifiers are set, they contain a CPS pointer (CPSuri) that points to the applicable CPS.

7.1.9 Processing semantics for the critical Certificate Policies extension

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

7.2 CRL profile

All revocation lists are issued in accordance with the requirements of [RFC5280] and 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

Revocation lists contain the following CRL extensions:

- AuthorityKeyIdentifier
- cRLNumber
- [EV] expiredCertsOnCRL

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

- keyCompromise (1)
- affiliationChanged (3)
- superseded (4)
- cessationOfOperation (5)
- [SMIME] certificateHold (6) (only for Deutsche Telekom AG)
- privilegeWithdrawn (7)

The CRLReason keyCompromise (1) takes precedence over all other revocation reasons, and revocation reasons may be subsequently changed to keyCompromise if a compromise of the key subsequently becomes known.

If no revocation reason is known for a TLS certificate, i.e., CRLReason unspecified (0) applies, the CRL entry extension reasonCode is not set.

7.3 OCSP profile

All OCSP responses are issued according to the requirements of [RFC6960] and are signed by a delegated OCSP-Signer. The OCSP-Signer certificates are issued by the respective CA with a short validity period and contain the id-pkix-ocsp-nocheck extension.

OCSP responses for revoked certificates contain the revocation reason in the revocationReason attribute within the RevokedInfo. The specifications made in Section 7.2.2 apply with regard to the revocation reasons.

7.3.1 Version number

All OCSP responders are operated in version 1 according to [RFC6960].

7.3.2 OCSP extensions

OCSP signers providing information for qualified certificates use ArchiveCutOff. Other extensions are not set.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

Audits are carried out by external auditors on an annual basis and in accordance with Section 8.4. The audit periods directly follow each other, don't exceed one year and form an unbroken sequence, starting from the CA key pair generation up to destruction of the keys and the withdrawal of trust ("Cradle-to-grave").

In addition, all key generations and certificate issuances for all CAs within the scope of this CPS are monitored and attested by external auditors.

Monthly self-audits are performed by internal auditors, which randomly sample at least one certificate (TLS) or 30 certificates (SMIME) and at least 3% of the certificates issued since the last audit (6% for [EVCP]).

The practices of external RAs are randomly audited in an annual basis.

8.2 Identity/qualifications of assessor

External audits according to Section 8.1 are performed by qualified auditors with the following qualifications and skills:

- The auditors are independent of the subject of the audit.
- The auditors are capable of performing audits that meet the criteria set forth in appropriate audit schemes in accordance with Section 8.4.
- The auditors are proficient in auditing PKI technology, information security tools and techniques, information technology and security auditing, and in the third-party attestation function.
- The auditors are bound by law, government regulations, or professional code of ethics.
- The auditors maintain Professional Liability/Errors and Omissions insurance with policy limits of at least one million US dollars in coverage.
- The conformity assessment body is accredited by "DAkkS" (German Accreditation Body) according to ISO 17065 using the requirements specified in ETSI EN 319 403 and is a member of the "ACAB'c" (Accredited Conformity Assessment Bodies' Council).

Internal auditors performing the tasks listed in Sections 8.1 have many years of experience and sufficient expertise in the areas of auditing, PKI technologies and processes.

8.3 Assessor's relationship to assessed entity

Only external auditors who are independent of Deutsche Telekom AG and the subject of the audit are commissioned.

For internal auditors, the segregation of roles according to Section 5.2.4 is taken into account.

8.4 Topics covered by assessment

Telekom Security's Trust Services within the scope of this CPS, including all associated CAs, are audited in accordance with ETSI EN 319 411-1 and ETSI EN 319 411-2. Trust Services for SMIME are additionally audited according to TS 119 411-6.

Depending on the Trust Service, the ETSI policies NCP, LCP, DVCP, OVCP, EVCP or QEVCP-w apply.

For qualified Trust Services, the audit additionally includes the conformity assessment according to [eIDAS].

8.5 Actions taken as a result of deficiency

If deficiencies are identified that constitute violations of the [BR], [EVCG], [MSRP], [MOZRP], [GCRP], or [APLRP], they will be reported to the respective Root Store according to their requirements as soon as possible.

In addition, any deficiencies identified are corrected as soon as possible. Internal Group deadlines and, in the case of audits in accordance with ETSI, the deadlines specified for each finding are adhered to.

8.6 Communication of results

Audit attestations of all CAs prepared by external auditors in accordance with [CCADB#5.1] will be published in the "Common CA Database" (CCADB) without delay, but at the latest within 3 months after the end of the audit. If the deadline of 3 months cannot be met, Telekom Security will provide an explanatory letter signed by the external auditor.

Conformity assessment reports for qualified services are submitted to the “Bundesamt für Sicherheit in der Informationstechnik” (BSI, German Federal Office for Information Security) within three days of receipt.

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 and contracts.

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 charging of fees.

9.1.5 Refund policy

The refund of fees is based on the statutory provisions of German law and is specified in the General Terms and Conditions or other contractual agreements.

9.2 Financial responsibility

9.2.1 Insurance coverage

Telekom Security has sufficient business and property liability insurance coverage through Deutsche Telekom AG in accordance with [TSCP#9.2.1].

9.2.2 Other assets

As a one-hundred percent subsidiary of Deutsche Telekom AG, Telekom Security has the financial stability and resources required to operate in compliance with the [TSCP], including a planned termination in accordance with Section 5.8.

9.2.3 Insurance or warranty coverage for end-entities

Not applicable.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

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

9.3.2 Information not within the scope of confidential information

All information mentioned in Section 2.2 as well as all information in published certificates are classified as public.

9.3.3 Responsibility to protect confidential information

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

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

9.4 Privacy of personal information

9.4.1 Privacy plan

To comply with all requirements of the General Data Privacy Regulation [GDPR], Deutsche Telekom AG has defined Group-wide guidelines for handling private data and corresponding protection classes have been defined for private data.

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

Appropriate technical and organizational measures are taken to protect private data against unauthorized processing and loss and to maintain its integrity and confidentiality. These measures are set out in a regularly revised privacy plan.

9.4.2 Information treated as private

All personal information that has not been published as certificate content or otherwise is treated as private.

9.4.3 Information not deemed as private

All personal information that must be made public in order to provide services (e.g., certificate contents) are not deemed as private.

9.4.4 Responsibility to protect private information

All Telekom Security employees are obligated to observe and comply with the Group's guidelines and legal regulations on handling private information. Contractors or third parties are also contractually obligated to comply with the requirements.

9.4.5 Notice and consent to use private information

Information considered to be private according to Section 9.4.2 will only be processed after informing and consent of the affected person.

9.4.6 Disclosure pursuant to judicial or administrative process

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

9.4.7 Other information disclosure circumstances

Not applicable.

9.5 Intellectual property rights

The legal provisions apply.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Telekom Security assures the representations and warranties required in [TSCP#9.6.1]. In particular, Telekom Security assures of reliable, trustworthy, non-discriminatory and legal operation of the Trust Services as well as compliance with [TSCP]. The Trust Services are also be made accessible to people with disabilities as far as possible. If existing measures are not sufficient, Telekom Security additionally offers free telephone support to assist people with disabilities in applying for, accepting and revoking certificates.

9.6.2 RA representations and warranties

Telekom Security ensures the representations and warranties of the RAs required in [TSCP#9.6.2].

External RAs are contractually bound to comply with the representations and warranties required in [TSCP#9.6.2] and are regularly audited for compliance (see Section 8.1). However, the overall responsibility remains with Telekom Security.

9.6.3 Subscriber representations and warranties

Subscribers’ representations and warranties as well as the information to be provided are defined in [TOUP] resp. [TOUC], which have to be accepted by the subscribers when applying for a certificate. [TOUP] and [TOUC] take into account all requirements from [TSCP#9.6.3].

9.6.4 Relying party representations and warranties

There are no contractual agreements with relying parties. However, [TOUP], [TOUC] as well as the PDS contain recommendations for third parties to verify the trustworthiness of a certificate for the respective use case.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimer of warranties

Any disclaimer of warranties is regulated in the GTC or other applicable contractual agreements.

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.

Corresponding contractual agreements have been made with delegated third parties in regard to liability, but overall responsibility remains with Telekom Security.

Any limitations of liability under applicable law are regulated in the GTC or other applicable contractual agreements.

9.9 Indemnities

Any claims for damages against Telekom Security are regulated in the GTC or other applicable contractual agreements.

9.10 Term and termination

9.10.1 Term

This CPS is valid from the validity date indicated on the cover page until it is replaced by a new version (maximum one year, see Section 9.12).

9.10.2 Termination

The validity of this document terminates when a new version comes into force.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

This CPS is subject to review based on changed requirements or relevant changes in operations, but at least annually. For this purpose, the Trust Center's PKI Compliance Management regularly reviews the underlying requirements of the sources referenced in the [TSCP#Appendix B] for new versions and follows relevant forums and mailing lists.

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

In the event of changes that affect the Terms of Use, they will be adjusted accordingly and provided in a new version.

9.12.2 Notification mechanism and period

New versions of this CPS are published in accordance with Section 2.

New versions of the Terms of Use that could affect the acceptance of a service by subscribers or relying parties shall be disclosed in a timely manner to subscribers, relying parties and, where applicable, conformity assessment bodies and supervisory or other regulatory authorities.

9.12.3 Circumstances under which OID must be changed

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

9.13 Dispute resolution provisions

In the event of disputes, the parties shall reach an agreement taking into account contracts, 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.