Deutsche Telekom PKS – Certificate Practice Statement (CPS)

Certification Practice Statement for the Telekom Security GmbH Public Key Service

Deutsche Telekom Security GmbH

Telekom Security

Public

Version: 07.00

Valid from: 01.07.2020

Status: release

Last review: 10.06.2020

PUBLICATION DETAILS

Table 1 – Publication details

Details	Characteristic
Published by	Deutsche Telekom Security GmbH Bonner Talweg 100 53113 Bonn Deutschland
File name	telekom security-pks-cps_v07.00_eng.docx
Valid from	01.07.2020
Title	T-Systems PKI - Certificate Policy
Version	07.00
Last review	10.06.2020
Status	Freigabe
Author	Telekom Security
Contents reviewed by	Telekom Security
Approved by	Telekom Security
Organizational unit involved	Telekom Security
Contact	Telekom Security
Brief description	Certification Practice Statement

CHANGE HISTORY

Table 2 – Change history

Version	Last revised	Edited by	Changes/Comments
1.0	January 14, 2005	T-Systems	Original version in English
1.1	January 21, 2005	Jog	Editorial changes
1.2	June 17, 2005	Jog	Revision
1.3	August 10, 2005	SB	Translation into German
1.33	September 7, 2005	Jog, SB	Revision
2.0	September 20, 2007	PS	Qual. and Advanced Certificates for Netkey3.0 (RSA2048)
2.1	September 21, 2007	PS	Comments and notes by DD, TH, and JK regarding Quality Assurance added
3.0	April 19, 2013	TH	Adapted in line with updated ETSI TS 102 042 requirements
3.1	May 19, 2014	JS	Adjustments online revocation and amendments in accordance with ETSI audit
3.2	April 21, 2015	TH	2015 review
3.3	April 8, 2016	TH, LK, JS	2016 review
3.3	April 8, 2016	DD	Approval
3.4	August 1, 2017	LK, TH JS	Review, revision for eIDAS
3.5	August 1, 2018	JS	Review, revision after last audit
4.0	January 1, 2020	JS	Revision for remote electronic signature
5.0	March 1, 2020	T-Systems	Structuring according to RFC 3647
6.0	May 28 2020	T-Systems	Approval
07.00	July 01 2020	Telekom Security	Approval

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

This document is the **Certification Practice Statement (CPS)** for the **TeleSec Public Key Service ® (PKS)**. Hereinafter it will be referred to as "**PKS CPS**." The PKS CPS is used exclusively for issuing qualified Public Key certificates as well as advanced certificates in the context of the PKS. As far as qualified certificates are concerned, this PKS CPS applies both to certificates on a chip card as well as to the remote electronic signature certificates stored at the TSP. If a differentiation is required in some places, this will be highlighted accordingly in the text.

Note:

The term "advanced certificates" in the context of the PKS should be construed as certificates for issuing advanced signatures, for encryption, and for authentication.

1.1 Overview

Deutsche Telekom AG's Trust Center (Telekom Trust Center) is operated by the Telekom Group unit Deutsche Telekom Security GmbH. The Telekom Trust Center has been certified in accordance with ISO 9002 since 1996 and ISO 9001:2000 since January 2001.

Deutsche Telekom AG has been operating a Trust Center since 1994, which – in 1998 – became the first Trust Center in Germany to obtain approval for issuing certificates for digital signatures in accordance with the German Digital Signature Act (Signaturgesetz – SigG) at the time. This approval saw the start of the Public Key Service (PKS) in early 1999, the Trust Center was continually expanded and, since July 1, 2016, has been compliant with the European Regulation on electronic identification and trust services (eIDAS).

Since starting operation, the Telekom Trust Center has issued more than 200 million certificates. The services offered by the Telekom Trust Center include the TeleSec Public Key Service (PKS), which covers the process of issuing qualified certificates in accordance with EU regulation eIDAS.

The PKS CPS describes the operational workflows and security measures adopted by the Telekom Trust Center in its capacity as a Certification Authority (CA) and Registration Authority (RA). This document is intended to round out the General Terms & Conditions (GT&C) for using the services of Deutsche Telekom Security GmbH's PKS. The latest version of the PKS CPS reflects the current status of the Trust Center's certification activities and applies exclusively to the TeleSec PKS.

The unit specified in section 1.5.1 is responsible for ensuring that the described workflows, activities, systems, roles, and security measures are also implemented even if they are outsourced.

The PKS CPS covers the following aspects in detail:

- Importance and use of qualified Public Key certificates
- Importance and use of advanced certificates
- Certificate issuance
- Renewal of certificates (re-certification)
- Follow-up orders for certificates
- Certificate management
- Liability
- Security precautions

1.1.1 PKI service TeleSec Public Key Service (PKS)

With the PKS, the customer is provided with a certificate and a key pair for electronic signature. This qualified certificate is subject to the regulations of the eIDAS Regulation of the European Union and the German Trust Service Act. A qualified PKS certificate enables a subscriber to prove that they have electronically signed an electronic document with their (private) signature key, which is stored on a qualified signature creation device (QSCD). In addition, the subscriber can prove the authenticity or genuineness of the signed document. The associated qualified signature is regarded as being equivalent to a handwritten signature.

Customers can extend qualified signature certificates with attributes to restrict the use of the corresponding signature key or disclose additional information (e.g., power of representation).

1.1.2 Complying with the baseline requirements of the CA/Browser Forum

The following regulation applies only to the advanced certificates of the Public Key Service. The Telekom Security Trust Center ensures that the "T-TeleSec GlobalRoot Class 2" root CAs with the corresponding sub-CAs meet and comply with the requirements and regulations of the respective currently published version of the [CAB-BR] (http://www.cabforum.org/documents.html). In the event that this document and the [CAB-BR] contradict one another, the regulations in the [CAB-BR] have priority.

1.2 Document name and ID

Table 3 – Document information

Name:	Certification Practice Statement for the TeleSec Public Key Service ® (PKS CPS)
Version:	07.00
Date	2020
Object identifier	1.3.6.1.4.1.7879.13.27

1.3 PKI participants

1.3.1 Certification authorities

1.3.1.1 Qualified certificates

The TeleSec Public Key Service for qualified certificates is structured in a two-level certification hierarchy:

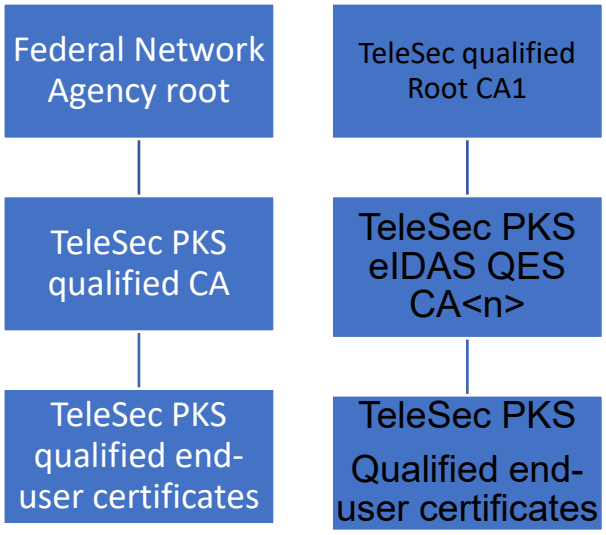

Figure 1 - Certification hierarchy of qualified certificates

The above graphic illustrates the certification hierarchy, taking examples of selected certificates. The left part shows the certificate hierarchy used for qualified certificates, which were issued in accordance with the requirements of the German Digital Signature Act (before August 1, 2017). The right part applies to certificates in accordance with the Trust Services Act (Vertrauensdienstegesetz, VDG) and the eIDAS Regulation (after August 1, 2017).

At present, the following CA certificates are used: TeleSec PKS eIDAS QES CA1 for signing end-user certificates on signature cards and TeleSec PKS eIDAS QES CA2 for signing end-user certificates on the remote electronic signature server.

These CA certificates are only used for the signing of OCSP signers and end-user certificates

The CA and service certificates during the validity of SigG were issued by the Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railway (BNetzA) as the responsible supervisory authority.

The root certificates and the CA and service certificates for use after August 1, 2017 are issued by Deutsche Telekom Security GmbH. In order to acquire the status of a qualified trust service, certificates are included and published in the European Union's Trust List after confirmation of eIDAS conformity.

In accordance with the eIDAS Regulation, the PKS CA only issues qualified certificates. The certification path of PKS certificates can be audited right through to a root certificate. The PKS CA is operated in the high-security area of the Telekom Trust Center.

Only certified QSCDs are used as key tools for end-user certificates. The keys are generated on the respective device itself by evaluated key generators. The certification validity of the QSCD used is checked regularly and on demand in the context of internal and external audits. Before expiry of a certification, the use of another certified QSCD is planned and implemented in good time.

End-user certificates are provided for the user and relying parties via LDAP, provided the user has not objected to their publication.

Certificates for technical tests can be obtained from the test environment by agreement with the TSP. These are clearly marked as test certificates.

The provisions of EU Regulation No. 910/2014 (eIDAS) apply to qualified certificates.

1.3.1.2 Non-qualified certificates

The issuance of non-qualified certificates in addition to a qualified certificate is optional. These are sometimes also referred to as advanced certificates. Customers who belong to specific closed user groups may possibly not receive non-qualified certificates. This depends on the agreements reached with the head of the user group. It is not possible to create non-qualified certificates retrospectively.

The TeleSec Public Key Service for non-qualified certificates uses a two-level certification hierarchy:

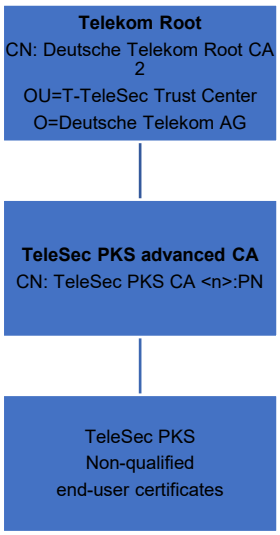

Figure 2 – Certification hierarchy for non-qualified certificates

The Public Key of the Telekom Root CA2 is contained in a self-signed certificate (root certificate). All subscribers to the TeleSec Public Key Service receive this certificate and can thus monitor the authenticity and validity of all the certificates issued under this root certificate within the TeleSec Public Key Service.

The TeleSec PKS CA certifies certificates for end users of the TeleSec Public Key Service exclusively. These certificates are subject to the requirements of ETSI TS 102 042, Policy NCP+.

1.3.2 Registration authorities

TeleSec PKS affiliated offices operate several registration authorities who accept PKS orders and perform reliable identification of principals. The trustworthiness and dependability of registration authorities is audited and confirmed by recognized inspection authorities in accordance with the requirements of the eIDAS Regulation. Identification is accessible to everyone by using Deutsche Post AG's “PostIdent" procedure or the "Notarident" service, which is available from any notary. There are also various registration authorities that are, however, only responsible for specific user groups. Identification using the "BehördenIdent" procedure is also available to employees of municipalities, state and federal authorities in Germany.

Telekom Security' registration authorities have the following tasks in particular:

- Accepting requests and checking identification documents
- Checking documents for authenticity and completeness
- Verifying identities

They are obliged to abide by the relevant applicable legal principles and data privacy provisions through appropriate contracts.

1.3.3 Certificate owner

Certificate owners are natural persons who apply for and/or receive a PKS certificate after having been successfully identified and authenticated.

1.3.4 Relying parties

Relying parties are natural persons or subjects who rely on the trustworthiness of issued certificates. For use and verification of the certificates by third parties, e.g., encryption or signature checking, the certificates and revocation information are available for retrieval in the directories.

1.3.5 Other entities involved

1.3.5.1 Identity checkers

Identity checkers are notaries in the case of "Notarident," employees of Deutsche Post in the case of the "PostIdent" procedure or employees of authorities in the case of the "BehördenIdent" procedure.

1.3.6 End entity

In the context of the PKS PublickEy Service, end entities are understood to be all certificate users to which a certificate can be issued that do not themselves represent a role of a certification authority.

1.4 Certificate usage

1.4.1 General principles

In the event of loss of a chip card or misuse of the certificate, the certificate owner must arrange revocation immediately. This also applies if misuse is suspected or it is suspected that the key material used has been compromised. Affected certificates shall no longer be used. The certificates must only be used within the permitted and legally valid framework. This applies particularly to the relevant country-specific import and export provisions.

1.4.2 CA certificates

The CA certificates are published in a ZIP file on the homepage.

1.4.3 Qualified certificates

TeleSec PKS Public Key Service qualified certificates are used for qualified signatures in the meaning of the eIDAS Regulation.

Qualified user certificates to which this CPS apply correspond to the QCP-n-qcsd policy.

1.4.4 Advanced certificates

TeleSec PKS advanced certificates are used for authentication, encryption, and for advanced signatures. The processes and the level of security for ordering, producing, and delivering advanced PKS certificates are identical to those for qualified certificates. Only the root hierarchy differs. In addition, no OCSP service is offered for advanced certificates.

1.4.5 Validity model

Two different validity models are used to check the validity of a signature or a certificate. The German Digital Signature Act stipulates that the chain model applies to all end-user certificates that are issued by July 2017.

The chain model states that every certificate must have been valid at the point in time when it was used. This means

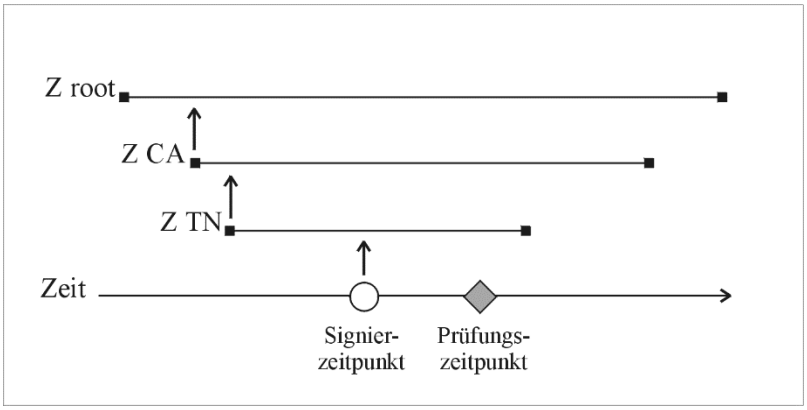

Fig. 3 – Chain model

that, at the time a document was signed, the signing certificate must have been valid. Its signer certificate must have been valid when it signed the issued certificate and so on. The figure below illustrates this.

The shell model has applied to end-user certificates since the eIDAS-compliant certification hierarchy was first implemented on August 1, 2017.

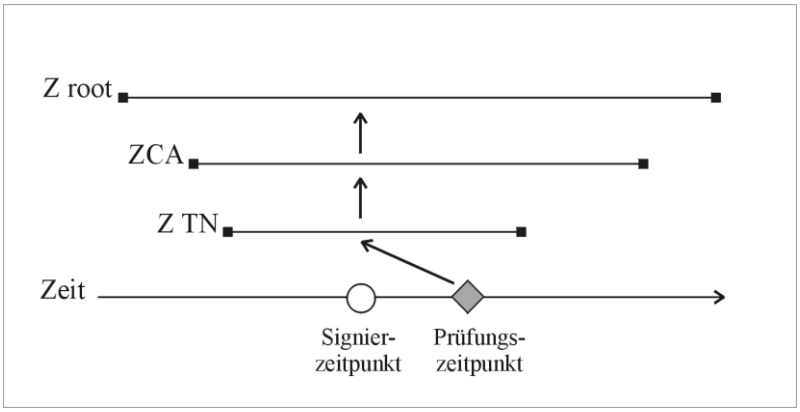

Figure 4 – Shell model

The shell model states that all certificates must have been valid at the time of the signature that was to be verified. This means that, at the time a document was signed, all the certificates in the certification hierarchy must have been valid.

1.5 Policy administration

1.5.1 Responsibility for the document

This CP/CPS is published by:

Deutsche Telekom Security GmbH
Deutsche Telekom Security GmbH
Bonner Talweg 100
53113 Bonn

Germany

The Trust Service is represented externally by the head of VDA and his deputy.

1.5.2 Contact information

Address:
Deutsche Telekom Security GmbH

Untere Industriestrasse 20, 57250 Netphen, Germany
Postfach 1465 57238 Bonn, Germany

Telephone: +49 1805 268 204 [1]

Revocation hotline:

From Germany	116 116
From abroad	+49 30 4050 4050

Email: telesec_support@t-systems.com

WWW: https://www.telesec.de

All relevant documents regarding the PKS can be found in the Public Key Service/Download area via the above-mentioned URL.

1.5.3 Department that decides whether this CPS is compatible with the CP

Section 1.5.1 names the organization that is responsible for ensuring that this CP/CPS, or the documents that supplement or are subordinate to this document, are compatible with the Certificate Policy (CP).

1.5.4 CPS approval procedures

This document is handled as per the quality assurance and release process defined in the operating guidelines of the Trust Center. This provides for quality assurance in the case of adaptations, with subsequent release by the head of the Trust Center.

This CPS undergoes annual review, regardless of any other amendments. The annual review must be noted in the change history of the CPS. This shall also apply even if no changes are made to contents.

1.6 Acronyms and definitions

BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railways)
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)

[1] 14 cents/minute from the German fixed network, max. 42 cents per minute from mobile networks

CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List, Revocation List
Common PKI	Joint specification by TeleTrust and the T7 Group for electronic signatures, encryption, and public key infrastructures
eIDAS	EU Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
ETSI	European Telecommunications Standards Institutes
FIPS	Federal Information Processing Standards is the name for publicly announced USA standards
HSM	Hardware Security Module
LDAP	Lightweight Directory Access Protocol
LRA	Local RA
OCSP	Online Certificate Status Protocol
PKS	Public Key Service
QCSD	Signature creation unit for qualified signatures in accordance with the eIDAS Regulation.
RA	Registration authority
Relying party	Denotes the persons or organizations that rely on a certificate or a digital signature.
RS	Registration authority
SigG	Signaturgesetz (German Digital Signature Act)
SigV	Signaturverordnung (German Digital Signature Regulation)
Subscriber	Certificate recipient
TSP	
VDG	Vertrauensdienstegesetz (Trust Service Act)
Certificate recipient	Denotes a person who is the subject matter of a certificate and to whom a certificate has been issued.

2 RESPONSIBILITIES FOR PUBLICATIONS AND STORAGE

2.1 Storage

Certificates and revocation lists are retrieved using LDAPv3, and OCSP responders are accessed by http. Access to the OCSP responder by end entities, relying parties or registration authorities is not subject to any access restriction. For each read access, the LDAP server allows a maximum of 100 data records to be requested.

The integrity and authenticity of revocation lists and OCSP information are ensured by signing with trustworthy signers.

The certificate status service is available 24/7. The response time of the

OCSP responder is less than one second under normal operating conditions.

2.2 Publication of certification information

TeleSec PKS publishes the following information at http://www.telesec.de/signaturkarte:

- Information on filling in a PKS order
- Technical description of directory service (LDAP, OCSP responder)
- Certificate profiles
- Information about the revocation service

The certificate owner and framework agreement partner are also notified in the case of

- revocation of a root instance key or a CA key
- a root instance key or a CA key that has been compromised or is suspected of being compromised
- security-relevant amendments to the CPS.

This information is published on the trust service provider's website. In addition, in the event of security-critical incidents, the subscriber is notified directly in writing or by email.

2.3 Updating the information (point in time, frequency)

Newly issued certificates, CRLs, policies, and any other information is provided promptly. The following publication frequencies apply:

- Immediately after activation, certificates are submitted to the directory service. Certificates are published in the directory service for at least one year after their validity expires.
- Revocation lists are updated at least once every six hours.
- Policies are updated as required.

2.4 Access to the storage and directory services

The directory service for TeleSec's PKS can be contacted at the following addresses (24/7 in accordance with the requirements of the eIDAS Regulation):

- https://www.telesec.de/signaturkarte/ → Directory service

- http://pks.telesec.de/ocspr
- ldap://pks-ldap.telesec.de

All certificates that have been issued and **released for retrieval** can be retrieved online in the Public Key Directory. In addition, the OCSP service makes it possible to **verify the status of all** issued qualified certificates (revoked/not revoked).

A certificate revocation list (CRL), but no OCSP service, is offered for non-qualified certificates for signing, encryption, and authentication. Only OCSP is offered for checking the status of qualified certificates.

3 IDENTIFICATION AND AUTHENTICATION

This section describes the mechanisms that are used in the identification and authentication process before a certificate is issued:

- The principal is personally identified in the RA/LRA.
- The received order forms are checked to ensure they are complete and plausible.
- The authenticity of the documents is checked.
- If registration in an RA/LRA has been performed, the registration employee's authorization is checked by CA personnel.
- After identification by the PostIdent procedure, the authenticity of the PostIdent form is checked by CA personnel.

3.1 Naming conventions

Issued Public Key certificates contain the name of the certificate owner. The name of the certificate owner is stored in the subject field and may have the following attributes:

- countryName (mandatory)
- organizationName (optional)
- organizationalUnitName (optional)
- commonName (mandatory)
- serialNumber (mandatory)
- pseudonym (mandatory to a limited degree, see below)
- email (certificate extension)

The ISO-8859-1 character set is supported.

Email addresses may only be included in a certificate if the certificate owner has confirmed to have access to the specified email inbox.

If the principal wants a pseudonym as a name, the pseudonym attribute is also entered in the certificate. A pseudonym is always entered in the two attributes commonName and pseudonym. In doing so, the pseudonym is given the ending ":PN".

At the principal's request, an email address, or other data of the principal (e.g., organization affiliation, etc.) is entered in the certificate in addition to the name or pseudonym.

3.1.1 Informative value of names

A name must uniquely identify the certificate owner and be in a form that is intelligible to humans. In addition, the following conventions apply when giving a name:

- The spelling of a name must correspond to the spelling in the identification document. The spelling must not be changed by special characters such as umlauts.
- If the same name exists more than once, it will be made unique by adding a numbered suffix (serialNumber).
- If a name is too long for an entry in the certificate the Trust Center will truncate it.

3.1.2 Pseudonymity/anonymity

It is possible to issue a pseudonymized certificate if explicitly requested by the principal. In this case, the principal may select a pseudonym that will be included in the certificate; pseudonyms are marked with the suffix ":PN". If the same pseudonym exists more than once, it will be made unique by adding a number. The choice of pseudonyms is subject to various name restrictions (excluded are, for example, names such as “Telekom CA,” political slogans and names that suggest authorizations that the certificate owner does not have).

The certification service provider transmits the identity of a signature key owner, encryption key owner, and authentication key owner with a pseudonym to the responsible departments if this is necessary in order to prosecute crimes or offenses, avert dangers to public security or order, or to fulfill the statutory requirements of the federal and state-based authorities for the protection of the Constitution, the Federal Intelligence Service, the German Military Counterintelligence Service, or the financial authorities or where courts have requested this in the context of pending proceedings in accordance with the relevant applicable provisions.

3.1.3 Recognition, authentication, and role of trademarks

Not applicable, as certificates are only issued for natural persons, with the name of the person in the subject DN.

3.2 Identity check for new application

The principal personally proves their identity in the RA/LRA or in a post office of Deutsche Post by presenting their identity card, passport, or an equivalent document (in the case of foreign principals).

The type of identification document as well as the ID number and the validity dates of the identification document are specified on the application form and stored in the database. A copy of the identification document must be attached to the application and is stored in the Trust Center's archive.

The applicant's name, registered address, and date and place of birth are recorded as identification data, thus ensuring precise identification.

If an application for a certificate contains details regarding third parties, work-related or other indications (e.g., affiliation to an organization, power of representation, professional license), the principal must provide proof of the third party's consent or authorization to this in the form of appropriate documents.

3.2.1 Identification and authentication for follow-up orders

The certificate owner is notified in good time before the validity of their certificates expire. New certificates are issued to them if they apply for certificates before the validity of their existing certificates expire. Follow-up orders can be placed only once by providing a qualified signature using the certificate that is still valid. Therefore, no further follow-up certificate can be issued on the basis of a follow-up certificate.

3.3 Identification and authentication for key renewal (re-key) orders

Key renewal is not supported.

Identification and authentication for revocation orders

Persons and institutions that are authorized for revocations (see Section 4.9) may request the revocation of certificates online, by telephone, or by sending an informal letter.

A written revocation is authenticated by comparing the signature on the letter with the signature on the original application form.

A certificate can be revoked immediately online or by calling the revocation hotline, which operates 24/7. The Tele PIN of the certificate is needed in both cases. The Tele PIN is defined by the ordering system and notified to the principal during the order process. The Tele PIN is used to authenticate the certificate owner.

Following generation of the certificate, institutions authorized to perform revocations (e.g., professional chambers) will obtain a Tele PIN for revocation.

A similar process is used for revocation of TSP certificates. Revocation of a CA certificate can be requested by authorized persons either by means of a signed email 24/7 or in writing. If the conditions for the revocation are met (authorization and reason), the revocation is carried out and the revoked certificate is included in the revocation information.

The authorized person or institution will be notified that the revocation has been carried out. The documents belonging to the process are archived in accordance with the requirements.

4 OPERATIONAL REQUIREMENTS IN THE LIFE CYCLE OF CERTIFICATES

4.1 Certificate application

In the context of the TeleSec Public Key Service, orders must be submitted in written form. The order must include the principal's handwritten signature. The necessary forms can be found on the TeleSec Public Key Service web pages.

The order must be supplemented by copies of the official document that was used for identification purposes, and – if the order contains details regarding third parties, work-related or other indications (e.g., affiliation to an organization, power of representation, professional license) – other documents that prove that the principal is authorized to use such details.

4.1.1 Placing an order for a qualified certificate

Besides a completely and legibly filled-in order form, a copy of the identification document (e.g., ID card) is required to order a qualified certificate. A list of other accepted documents can be found in the explanations regarding the PKS order form.

4.1.2 Placing an order for non-qualified certificates

Orders for non-qualified certificates are placed together with orders for a signature card for qualified signatures. It is not possible to place individual orders for non-qualified certificates without having a qualified certificate.

Non-qualified certificates for remote electronic signature are not offered.

4.2 Processing certification requests

An order for a qualified certificate is placed as follows:

- Fill in the requisite forms using the online forms that are available on the website http://www.telesec.de. Forms that are filled in by hand will not be accepted. The same applies to handwritten amendments on printed forms.
- Enclose copies of the identification documents.
- If necessary, enclose copies of other documents and forms (e.g., signed by the originator of a power of representation, etc.).
- If the principal wants to include an organization entry in their certificates, proof is required that they are allowed to make such an entry.
- All forms shall be duly signed.
- Personal identification of the principal in a Deutsche Telekom AG RA/LRA, using the PostIdent procedure, the BehördenIdent procedure, or via a notary.
- All forms (order forms, documents authenticated by notaries, confirmations of attributes by third parties, etc.) must be printed out and only the original, or qualified electronically signed copies for follow-up orders, must be provided by the certificate owner. Handwritten amendments are not permitted in order

to prevent manipulation. For the same reason, order forms that do not reach the Trust Center in a sealed envelope are rejected.

Documents are then sent to the Telekom Trust Center in order to produce the qualified certificate. At the Telekom Trust Center, the authenticity of orders is checked on the basis of the processes defined in the security concept. These processes are inspected at regular intervals by a conformity assessment body that is recognized in accordance with the eIDAS.

All order documents for the orders produced before July 31, 2017 are archived in the Trust Center, in accordance with the requirements of the German Digital Signature Act, for 30 years after the last certificate that was issued on the basis of an order expires. Order documents for orders produced starting August 1, 2017 are archived in the Trust Center in accordance with the provisions of the Trust Service Act. For follow-up orders, the retention period for the certificate with the longest archiving period applies.

Due to the archiving of these documents, orders for non-qualified certificates are also archived.

The purely digital transmission of a new order for creation of qualified certificates is not offered.

4.3 Issuance of certificates

Certificates are not issued until all the necessary documents are complete and available in the required form (original, no faxes). Issued certificates are assigned to the relevant orders and persons in the Trust Center's customer database.

4.3.1 Issuance of qualified certificates

The certificate is generated after successful checking of the order. Secure, unambiguous assignment to the order documents in the archive is ensured based on the data stored in the database. The certificate issued is stored on the certificate owner's personal chip card and in the Trust Center's customer database.

Remote electronic signature certificates are stored in the TSP's HSM. Only the certificate owner can use the certificate.

4.3.2 Issuance of non-qualified certificates

Non-qualified certificates are created in parallel to qualified certificates. The checking, generation, and delivery procedures are identical. Non-qualified certificates are not offered in the remote electronic signature service.

4.4 Certificate acceptance

Qualified certificates are not regarded as valid in accordance with the eIDAS Regulation until they have been activated in the Telekom Trust Center's directory service.

Advanced certificates are regarded as valid from the time they are issued. If a certificate owner returns their confirmation of receipt and requests revocation in it, certificates are revoked.

The principal can transfer the confirmation of receipt online (by using a web form) or by post. Additional attachments are required (copy of personal ID or copy of order documents) in order to process a confirmation of receipt that is received by post.

4.4.1 Acceptance by the certificate owner

4.4.1.1 Signature card

After a qualified certificate has been delivered, the certificate owner must acknowledge receipt and confirm the correctness of the certificate to the Telekom Trust Center. Confirmation of receipt ensures that the certificate owner received the chip card without there being any manipulation. The certificate is only activated once its receipt has been confirmed and the customer has confirmed correct receipt of the chip card, its integrity and that the content of the certificate is correct. The certificate owner should ensure that the content of the certificate is correct before issuing the confirmation of receipt.

The chip card has an integrated protection mechanism. This procedure, patented as the NullPIN procedure, protects a chip card against misuse by a third party while the card is in transit. The NullPIN is a special transit PIN (for instance "00000"), which is preset by the Trust Center but does not make it possible to use the security functions of the chip card. After initial activation, the PIN can no longer be reset to the NullPIN status. This makes it possible to detect security-critical manipulation of a received chip card.

4.4.1.2 Remote electronic signature

After a qualified certificate has been generated, the certificate owner must confirm the correctness of the certificate to the Telekom Trust Center. The confirmation of receipt ensures that the certificate was produced with the correct content. The certificate is only activated once its receipt has been confirmed by the customer.

4.4.1.3 Certificate transparency

Public Key Service supports Certificate Transparency (CT). You can find more information at: https://www.certificate-transparency.org

4.5 Use of the key pair and the certificates

4.5.1 Use of the private key and the certificate by the certificate user (subscriber)

TeleSec PKS qualified certificates may only be used to generate digital signatures (in the sense of non-repudiation) of data or documents in compliance with the security requirements for the components that are used (environment, software, card reader, etc.).

Non-qualified certificates are issued for authentication and encryption purposes and in order to create advanced signatures.

The end user must abide by the prerequisites for using the certificate, for instance handling their PIN; these are described in the information about the Public Key Service. This document can be downloaded from the Trust Center's website at https://www.telesec.de/signaturkarte/ ▯ Support ▯ Download area ▯ Notes.

In addition, unpublished certificates are subject to data privacy requirements.

If the certificate end user becomes aware that their private key has been compromised or if they suspect that their private key has been compromised, the certificate end user is obliged to arrange revocation of their certificate immediately.

4.5.2 Use of public keys and certificates by relying parties

Everyone who uses a certificate that was issued under the terms of this CPS, for checking a signature, or for authentication or encryption purposes, must

- check the validity of the certificate before using it by validating the entire certificate chain up to the root certificate, amongst other things, and
- use the certificate only for authorized and legal purposes in accordance with this CPS.

4.6 Renewal of certificates (re-certification)

Automated renewal of a certificate is not offered. Customers who place follow-up orders receive new key material. There is no provision in the current process for re-certifying existing key material.

4.7 Re-key of certificates

No stipulation.

4.8 Modification of certificate data

If the identification data of the certificate changes (e.g., in the event of name changes as a result of marriage), re-identification is required.

If the address or email address of the certificate owner changes, re-identification is not required.

4.9 Certificate revocation and suspension

The following reasons cause a certificate to be revoked:

1. Loss of the private key (e.g., loss or theft of a key carrier).
2. A private key is compromised or it is suspected that a private key has been compromised.
3. The details in the certificates are no longer correct.
4. The certified key or the algorithms used with it no longer meet current requirements.
5. The certificate owner or other persons authorized to use a key have misused the key or are suspected of having misused it.
6. Legal requirements
7. The certificate is no longer compatible with the valid version of the CP.

The following persons and institutions are authorized to initiate the revocation of a qualified certificate:

- The certificate owner.
- Third parties authorized to revoke certificates, these are:
- Representatives of the certificate owner.
    - Persons for whom the certificate owner has a power of representation and for whom this fact has been entered in the qualified certificate.
    - Authorities responsible for professional or other information, if professional or other information is included in the qualified certificate.
    - Bill recipient
- The Telekom Trust Center can arrange the revocation of a certificate in accordance with the General Terms and Conditions for the TeleSec Public Key Service or for legal reasons.
- The Federal Network Agency can order the revocation of a certificate pursuant to legal regulations.

Revocation of certificates can be initiated by an informal letter, the online revocation form (website), or by a telephone call. An informal letter will only be accepted if it bears the handwritten signature of an authorized person who wants to revoke the certificate. If a certificate is revoked by a third party authorized to revoke a certificate, it is necessary to use the third party's business letterhead.

In order to enable revocation, the Trust Center operates an online revocation form and a revocation phone hotline that can be contacted 24 hours a day, 7 days a week. The Tele PIN is needed in order to execute revocation.

Telephone and online revocation are performed immediately as soon as a request is received. Written revocations are executed no later than by the next working day after they are received.

The contact details for the revocation hotline and the online revocation form are published on the following website:

https://www.telesec.de/signaturkarte/ → Revocation service.

Even in the event of system defects, service work and/or other factors that are beyond Telekom Security' control, Telekom Security will do its best to ensure that revocation orders are actually executed within the above-mentioned times. An emergency scenario plan has been developed for such situations and regular practice drills are held.

After revocation has been performed, the certificate owner receives an email notifying them that their certificate has been revoked. This email also informs them of the precise revocation time.

Certificates are managed in the revocation list for at least one year after their validity expires.

Comment: The revocation of a certificate is final and cannot be reversed. Certificate suspension is not permitted for qualified certificates and is therefore not possible.

4.9.1 Circumstances for suspension

The suspension (temporary revocation) of certificates is not supported.

4.9.2 Who can request the suspension of a certificate?

No stipulation.

4.9.3 Procedure for suspension

No stipulation.

4.9.4 Limitation of the suspension period

No stipulation.

4.10 Status information services for certificates

4.10.1 Operating characteristics

Every CA eligible to issue certificates issues certificates for the OCSP responder so that the OCSP service can be performed. This certificate type is available exclusively to the PKI operator Telekom Security/Deutsche Telekom AG. OCSP certificates are changed regularly, without notification.
No revocation lists are offered for qualified certificates.

4.10.2 Availability of the service

Both the OCSP services and the CRL/ARL on the LDAP directory service are available around the clock. Under normal operating conditions, the response time of the OCSP responder and the LDAP directory service is less than ten seconds.

4.10.3 Download of certificates

The Telekom Trust Center operates a publicly accessible LDAP server. This server makes certificates available for download if their owners have explicitly consented to publication. An issued certificate is not published and cannot be downloaded from the LDAP server without its owner's explicit consent.

The interface specification for the LDAP server is available on the TeleSec PKS websites.

4.10.4 Status information service

The Telekom Trust Center operates a publicly accessible OCSP responder, which can be used at any time (24/7) to check the status of qualified certificates. The address of the OCSP responder is as follows http://pks.telesec.de/ocspr.
The interface specification for this service is available on the TeleSec PKS websites: https://www.telesec.de/de/signaturkarte/support/downloadbereich/category/12-technische-dokumentation?download=15:pks-ocsp-responder
The OCSP response is not dependent on the life cycle of the CA, as the TSP provides authorized OCSP information even after expiry of the issuing CA.

An ARL is available to check the CA certificates. This is renewed when necessary (creation or revocation of a CA) or at the latest after 6 months.

4.10.5 Revocation list

No stipulation.

4.10.6 Optional functions

No stipulation.

4.11Termination of the contractual relationship

4.12Key storage and restoration

Storage and restoration of keys on the signature card is not offered for security reasons. This also applies to individual remote electronic signature keys if, for example, the end user has forgotten their access data.
In the event of a malfunction in one of the HSMs used for the remote electronic signature service, all required data can be found on the backup system. After replacement of the defective HSM, the keys are synchronized via a protected mechanism.

4.12.1 Guidelines for key storage and restoration

No stipulation.

4.12.2 Session key encapsulation and guidelines for restoration

No stipulation.

5 BUILDING, ADMINISTRATION, AND OPERATION CHECKS

The Telekom Security Trust Center is located in a specially protected building and operated by expert staff. All processes for requesting and generating certificates by the certification authorities operated there are defined in detail. All technical security measures are documented.
The physical, organizational, and personnel-related security measures applied are defined in a security concept based on IT baseline protection ("IT-Grundschutz"), with their effectiveness being proved on the basis of a threat analysis.
The security measures required for operational purposes are described in the Service and Organization manual as well as the Operating Guidelines for the Trust Center.
The requirements of ETSI EN 319 401 Sections 5, 6.3, and 7.3 are implemented, they include stipulations regarding

- risk assessment in the framework of ISMS,
- information security guidelines,
- asset management.

Management approves the risk assessment and accepts the identified residual risk.

5.1 Physical checks

Signature cards are produced in the Telekom Security Trust Center. The Trust Center is eIDAS-compliant as a certification authority and thus meets very high physical security standards. The measures are described in detail in the security concept. The requirements under ETSI EN 319 401 Section 7.6 are implemented.

5.1.1 Location and structural measures

Telekom Security operates a Trust Center that consists of two fully redundant locations. Both locations have independent energy tracts (electricity, air conditioning, water) with their own facility management system and emergency generators.
The Trust Center is set up and operated in observance of the relevant policies of the Federal Office for Information Security (BSI) and the German Insurance Association (Gesamtverband der Deutschen Versicherungswirtschaft – GDV) and the pertinent DIN standards on fire prevention, smoke protection, and blocking of attacks. The Trust Center is accepted by the GDV in terms of security technology.
The technical measures are supplemented by organizational elements that include the handling of security-relevant techniques and regulations regarding access to security zones for employees and third parties (visitors, external staff and cleaning staff), delivery of materials (hardware, accessories, resources), and tidiness at the work station as well as in computer rooms.

5.1.2 Physical access

The Trust Center is subject to an access regulation that regulates access rights for employees, employees of third party companies, and guests in the individual security zones. Access to the security areas is only possible via turnstiles. Controlled access to the various security zones is further secured by a computer-controlled access control system. Guests are only received in exceptional cases and following prior notification. Specific security rules apply here.

5.1.3 Power supply and air conditioning

The intake openings for outside air are installed in such a manner that pollutants such as dust or dirt as well as corrosive, poisonous, or highly flammable gases cannot enter. The systems are operated using a very low proportion of outside air. The required fresh air openings are access-protected. Filters are installed to protect against air pollution resulting from floating particles. The fresh air intake is continuously checked for aggressive gases. In the event of an emergency (e.g., fire in the surrounding area), the fresh air intake is automatically closed by means of air flaps.
To protect against power supply failure, an independent alternating current supply is installed in accordance with VDE regulations. It provides protection against variations in voltage, short-term bridging that is free of interruptions as well as long-term bridging with two separate stationary emergency generators with a performance corresponding to the full load of the data center.

5.1.4 Water risk

The Trust Center is situated in a protected area, i.e., it is not situated close to any body of water or in low-lying areas (danger of flooding). Any fire is extinguished using inert gas.

5.1.5 Fire prevention

The applicable fire regulations (e.g., DIN 4102, requirements of the local fire department, regulations regarding fire resistance, VDE-compliant electrical installation) are complied with. All fire doors have automatic locking mechanisms. As agreed with the fire department, water will only be used to put out fires in extreme emergencies. Fire compartments are secured by fire-resistant components. Passages through fire walls are equipped with self-closing fire doors.
In areas with double floors as well as suspended ceilings the fire walls go right through to the ceilings/floors of the story.
Early fire detection systems (suction systems) are installed in all system rooms, system operator rooms, archive rooms, UPS rooms as well as in other selected rooms. The supply air and exhaust air of the air-conditioning devices in the individual rooms are monitored. Fire alarms are installed in the other rooms.

5.1.6 Storage of data media

Data media containing production software and data, audit, archive, or backup information, are stored in rooms with appropriate physical access controls, which offer protection against accident damage (e.g., water, fire, and electromagnetic damage).

Order documentation, in particular information on certification applications and revocations that have been implemented, is stored until expiry of the statutory retention period.

Audit and event logging data is archived in accordance with the current legal provisions.

5.1.7 Disposal

Confidential documents and materials are physically destroyed before being disposed of. Before being disposed of, data media that contain confidential information are treated in a manner that makes such data impossible to read or restore. Prior to their disposal, cryptographic devices are physically destroyed according to the manufacturer's guidelines. Other waste is disposed of in accordance with Telekom Security' regular disposal guidelines.

5.1.8 External backup

Telekom Security carries out routine backups of critical system data, audit log data, and other confidential information. The backup copies are kept in a different room from the original data.

5.2 Organizational measures

The organizational measures are set out in the security concept and are implemented on the basis of the Trust Center's operating concept. The relevant requirements of ETSI EN 319 401 Section 7.4 b, c, d, e are implemented and are regularly reviewed by a conformity assessment body in accordance with eIDAS.

The list below states some of the organizational measures, from various sources, that have been taken to ensure security:

- Measured to determine, assess, and regularly review residual risks are included in the Public Key Service security concept.
- The provisions for integrating external service providers are implemented in contracts in accordance with the applicable laws and regulations so that compliance with security measures can be checked at any time by the Trust Center or by external auditors.
- All Trust Center employees are obliged to observe the strict internal data privacy and security policies of Deutsche Telekom AG.
- The Trust Center's systems are regularly examined for any modifications that are relevant to security. All security-relevant modifications must be approved by the Trust Center's Change Advisory Board before they are put into operation.

All security-relevant processes are documented and tested in the security concept.

5.2.1 Trusted roles

Trusted persons are all persons (Telekom Security employees, contractors, and consultants) with access to or control over authentication or cryptographic processes which can have a significant impact on the following:

- The validation of information in certificate requests
- The acceptance, rejection, or other processing of certificate requests, revocation requests, or renewal requests
- The issuance or withdrawal of certificates, including staff who have access to the database systems
- The handling of information or requests from end entities.

Trusted persons are in particular:

- Trust Center employees (e.g., system administration)
- Employees of cryptographic departments
- Registration employees
- Security Officers
- System auditors
- Security personnel
- Responsible technical personnel and
- Executives responsible for managing the trusted infrastructure.

The following tasks are currently wholly or partially provided by contractors or independent third parties:

- Operation of the data center (max. up to operating system level of the IT systems)
- Registration of end customers
- Archiving of documents in corresponding high-security archives

The above-mentioned trusted persons must meet the requirements set out in this CPS (see Section 5.3.1).
These trusted persons must also be freed of conflicts of interest to ensure that the roles they hold can be exercised impartially and without prejudice. The employees undertake to acknowledge and adhere to the Group's Code of Conduct.The Change Advisory Board of the Telekom Security Trust Center is responsible for initiating, performing, and monitoring the methods, processes, and procedures that are described in the security concepts and in the CP/CPS of the certification authorities operated by the Telekom Security Trust Center.

5.2.2 Number of involved persons per task

The operational maintenance of the certification authority and the directory service (administration, backup, restoration) is carried out by qualified and trusted employees.
Work on highly sensitive components (e.g., key generation system, HSM) is governed by special internal control procedures and carried out by at least two employees.

5.2.3 Identification and authentication for every role

Telekom Security employees who are classed as especially trusted and who carry out especially trusted activities are subject to a Telekom Security internal security check.
Telekom Security ensures that employees have achieved a trusted status and the unit has given its approval before these employees:

- receive access devices and can access the necessary facilities,
- are given authorization to access systems of the certification authority and other IT systems,
- are permitted to carry out certain tasks in connection with these systems.

The Trust Center employees are formally appointed by the head of the Trust Center following a positive check.

5.2.4 Roles that require a separation of functions

The following roles require a separation of duties and are therefore supported by different employees:
Order entry and certificate approval
Backing up and restoring databases and HSMs
Generation of qualified certificates,
Key life-cycle management of CA and root CA certificates.

Exclusions for the various roles are implemented via both parts (remote electronic signature and card-based signature) of the TSP. If there are further role conflicts from the activity in both parts of the TSP, the corresponding employee will only be deployed in one of the two parts.

5.2.5 Vulnerability assessments

Following every significant change in the system or network or as requested by the CA/Browser forum, an automatic vulnerability scan is performed within a week, though at least once per calendar quarter. Potential vulnerabilities are analyzed, assessed, and registered. Based on the assessment, measures are determined and implemented in a defined plan. The vulnerability scans, their results and actions (resolutions, replacement) are documented.

5.2.6 Security measures in software development

Software development by Trust Center employees takes place in the Trust Center's protected environment. A version control system is used. Before development starts, the project is examined in terms of the security aspects that it must meet.
Importance is attached to trusted manufacturers when selecting external software. Open source components are used in areas where this is possible. In the case of software that has to be developed specifically for the Trust Center, the manufacturer must store the source code in the Trust Center after project completion.

5.2.7 Standards and controls for cryptographic modules

The private keys of the CAs are stored on an FIPS 140-2/level 3-evaluated hardware security module (HSM) or QSCD-evaluated devices. When HSMs are used, the keys are backed up using high-quality multi-person backup techniques.
To protect cryptographic devices during operation, transport, and storage, the manufacturer-specific mechanisms examined during FIPS and CC certifications are used. The devices are stored separately from the token required for operation and use so that the compromise of a single location is not sufficient to misuse the devices.

5.3 Staff measures

Telekom Security implements a comprehensive range of personnel-related security measures that ensure a high level of security for their facilities and certification services. The use of qualified and trained staff is mandatory in the Trust Center, HR measures are laid down in the security concept.
The requirements under ETSI EN 319 401 Section 7.2 are implemented and inspected during the course of both internal and external audits.
The trusted persons must fulfill the requirements set out in this CP/CPS.
These trusted persons must also be freed of conflicts of interest to ensure that the roles they hold can be exercised impartially and without prejudice. The employees undertake to acknowledge and adhere to the Group's Code of Conduct.
The Telekom Security Advisory Board is responsible for initiating, performing, and monitoring the methods, processes, and procedures that are illustrated in the security concepts and CP/CPS of the certification authorities operated by the Telekom Security Trust Center.

5.3.1 Required qualifications, experience, and security checks

Employees who are to assume a trusted role are required by Telekom Security to prove that they have the qualifications and experience necessary to fulfill their prospective work obligations in a competent and satisfactory manner.
A police clearance certificate must be submitted to Telekom Security at regular intervals.

5.3.2 Security check

Prior to employment in a trusted role, Telekom Security carries out security checks that involve the following:

- Checking and confirming the previous work relationships
- Checking employment references
- Confirming the highest or most relevant educational/vocational qualification
- Police clearance certificate.

If the requirements set out in this section cannot be fulfilled, Telekom Security will use another legally permitted method of ascertaining essentially the same information.
Results of a security check that could lead to a candidate for a trusted person being rejected can include

- False statements by the candidate or the trusted person

- Particularly negative or unreliable employment references, and
- Certain previous convictions.

Reports containing such information are evaluated by HR and security employees, who determine the appropriate course of action. The measures involved in the course of action can even lead to candidates for trusted positions having their employment offer withdrawn or to trusted persons being dismissed.
The use of information obtained in a security check in order to take such measures is governed by the applicable law.

5.3.3 Education and training requirements

The staff at Telekom SecurityTrust Center undergo the training measures required to fulfill their work obligations in a competent and satisfactory manner. Telekom Security keeps records of these training measures.
The training programs at Telekom Security are tailored toward the individual task areas and include, for example:

- Advanced PKI knowledge
- Procedures in accordance with ITIL
- Data privacy
- Data and telecommunications secrecy,
- Information protection
- Access control
- Anti-corruption
- Security and operational policies and procedures of Telekom Security
- Use and operation of the hardware and software in use
- Reporting and handling of faults and compromises, as well as
- Procedures for disaster recovery and business continuity

Employees who are involved with validating certificate requests receive additional training in the following areas:

- Guidelines, procedures, and current developments regarding validation methods
- Contents and particularly relevant amendments to this CPS
- Relevant requirements and specifications from the certification standards
- General threat and attack scenarios regarding the validation methods (e.g., social engineering)

5.3.4 Follow-up training intervals and requirements

The staff at Telekom Security receive refresher training and further training courses to the extent required and at the intervals required.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions in the event of unauthorized activities

Telekom Security reserves the right to punish unauthorized activities or other violations of this CPS and the procedures resulting therefrom and to take appropriate disciplinary measures. These disciplinary measures can extend to dismissal of the employee and are based on the frequency and severity of the unauthorized activities.

5.3.7 Requirements for independent contractors

Telekom Security reserves the right to use independent contractors or consultants to fill trusted positions. These persons are subject to the same functional and security criteria as employees of Telekom Security in comparable positions.
The above-mentioned group of persons who have not yet completed or have failed the described security check are not granted access to the secure facilities at Telekom Security.
All utilized independent contractors shall will be incorporated through corresponding contracts before starting their work. The TSP ensures that the service provided by the contractor is defined in such a way that the TSP, for its part, can meet all of its requirements. This applies in particular to the protection of personal data and other legal obligations.
Violations against the regulations can be sanctioned differently depending on the cause and severity of the violation. These sanctions range from follow-up training of the personnel, to the exclusion of certain employees of the service provider from work for the TSP and on to complete termination of the collaboration with this service provider.

5.3.8 Documentation for the staff

To enable employees to properly fulfill their work obligations, Telekom Security provides its employees with all the aids and documents they need for this (training documents, process instructions).

5.4 Log events

What data and events are recorded by whom and at what intervals is defined in the logging concept as well as the installation manual. In addition, rules are laid down that govern how long the log data is stored and how it is protected against loss and unauthorized access. Here the requirements under [ETSI EN TSP] Section 7.10 are implemented.

5.4.1 Types of events recorded

Generally, all log entries contain at least the date and time of the entry, a reference to the person or system that generated the entry, and a description of the event.

5.4.1.1 CA key pairs and CA systems

For the life cycle management of CA key pairs or CA systems, the Telekom Security Trust Center logs at least the following events for Fehler! Unbekannter Name für Dokument-Eigenschaft.:

a) Generation, destruction, storing, backup, and restoration as well as archiving of the key pair or parts of the key pair
b) Events in the life cycle management of cryptographic devices (e.g., HSM) as well as the CA software in use

5.4.1.2 EE and CA certificates

For the life cycle management of EE and CA certificates and their validation, the Telekom Security Trust Center logs at least the following events for Fehler! Unbekannter Name für Dokument-Eigenschaft.:

a) Ordering and revocation of certificates
b) All activities relating to the verification of information
c) Acceptance or rejection of certificate orders
d) Issuance of a certificate
e) Generation of revocation lists (CRL) and OCSP entries

5.4.1.3 Other security-related events

In addition, the Telekom Security Trust Center logs all security-relevant events for operation of the infrastructure. This includes at least the following events:

a) Successful and unsuccessful attempts to access the PKI systems
b) Actions performed on and by the PKI and other security-relevant systems
c) Changes to the security profile
d) System crashes, hardware failures, and other anomalies
e) Firewall and router activities
f) Entering and exiting of Trust Center facilities
g) Results of network checks (vulnerability scans)
h) Start and termination of the logging process

5.4.2 Processing interval for logs

The created audit logs/history data/logging files are continuously examined for important events relevant to security and operations. Furthermore, Telekom Security checks its audit logs/logging files for suspicious and unusual activities resulting from irregularities and faults.

Measures taken in response to the analysis of audit logs/logging files are also logged.

5.4.3 Retention period for audit logs

After processing, audit logs/history data/logging files are archived in accordance with the legal requirements.

5.4.4 Protection of audit logs

Audit logs/history data/logging files are protected against unauthorized access by means of operating system mechanisms.

5.4.5 Backup procedures for audit logs

An incremental backup of audit logs/history data/logging files is carried out on a daily basis.

5.4.6 Audit recording system (internal vs. external)

Audit data/history data/logging files at an application, network and operating system level are automatically generated and recorded. Manually generated audit data is recorded by Telekom Security employees.

5.4.7 Notification of the subject that triggered the event

Events recorded by the audit monitoring system are assessed and passed on to the Trust Center staff responsible. High priority events are immediately passed on to the Trust Center staff, including outside of regular working hours.

5.4.8 Vulnerability assessments

Following every significant change in the system or network or as requested by the CA/Browser forum, an automatic vulnerability scan is performed within a week, though at least once per calendar quarter. Potential vulnerabilities are analyzed, assessed, and registered. Based on the assessment, measures are determined and implemented in a defined plan. The vulnerability scans, their results and actions (resolutions, replacement) are documented.

Critical vulnerabilities are handled via the ISMS process. Critical vulnerabilities reported to the TSP are evaluated by the ISMS team within 48 hours and a solution scenario is presented. In the event that immediate and complete elimination of the vulnerability is not possible, a treatment plan is set up with the aim of reducing the critical vulnerabilities.

5.5 Data archiving

5.5.1 Types of archived data records

Telekom Security archives the following data:

- Order documents on paper (e.g., quotations, orders)
- Information in certificate requests and regarding the certificate life cycle (e.g., revocation and renewal requests)
- All audit data/history data/logging files recorded pursuant to Section 5.4

5.5.2 Retention period for archived data

All records in the Telekom Security Trust Center are, if they relate to qualified certificates in the sense of the German Digital Signature Act, kept for 30 years. Other records are stored in accordance with the currently valid laws.
Audit, history, and event logging data is archived for up to forty-two (42) days.

5.5.3 Protection of archives

Telekom Security ensures that only authorized and trusted persons are given access to data media archives. Archive data is protected against unauthorized read access, amendments, deletions or other forms of manipulation.

5.5.4 Backup procedures for archives

An incremental backup of the electronic archives is carried out on a daily basis.

Telekom Security retains data media that contain archive data and applications that are required for processing the archive data in order to ensure that the archive data is retained for the archiving period specified in this CP/CPS.

5.5.5 Requirements for time-stamping of data records

Data records such as certificates, certificate revocation lists, OSCP responses and logging files shall contain information on the date and time. The time source is the received signal of the DCF 77, from which the UTC is derived.

5.5.6 Archive recording system (internal or external)

Telekom Security uses only internal archiving systems for electronic archiving. Paper documents are, if no further access is required in the normal workflow, kept by a certified external service provider in highly secure archives.

5.5.7 Procedures for obtaining and checking archive information

Only authorized and trusted personnel receive access to archives and archive data. When archive data is restored, its authenticity is verified.

5.6 Key change

For key changes involving CA certificates, the generation of new keys and certificates must be documented and monitored in accordance with the conditions of the relevant security concept.

Affected users shall be informed about this measure.

5.7 Compromised situations and disaster recovery

5.7.1 Handling of incidents and compromised situations

Telekom Security has established an IT service management in accordance with ITIL and ISMS processes that processes faults and security incidents in line with defined standard processes.

By stipulating all required contacts and appropriately established groups in the IT service management system as well as establishing an on-call suport service and the MoD (Manager on Duty), it is ensured that the handling of faults and security incidents begins promptly so that damage is minimized and can be eliminated quickly.

The end entity submits faults via the Service Desk contacts defined in the PKS Info and they are then processed as part of service management.

The Service Desk staff first evaluates the fault before it is entered into the Telekom Security fault resolution application, prioritized and forwarded to the functional unit(s) for fault resolution. All the information is saved in the IT application in a transparent and audit-proof manner so that the processing status of the fault can be traced at any time up until resolution.

The functional untit informs the Service Desk about the processing status in accordance with the fault class so that the Service Desk can provide the delegated third party with relevant information.

If required, affected customers are informed as quickly as possible and integrated in the process.

If an incident has a security-critical impact, the responsible supervisory authority will be informed within 24 hours using the procedure defined in the German Trust Services Act.

5.7.2 Damage to IT equipment, software, and/or data

If the IT components, software, and/or data are damaged, the incident is immediately investigated and reported to the Telekom Security security units. The event initiates a corresponding escalation, incident investigation, incident response, and finally incident resolution. Disaster recovery is carried out depending on the incident classification.

All hardware and software that is required for provision of the PKS is managed as an asset and application in Telekom Security' configuration management.

This application also forms the basis for problem management.

5.7.3 Procedure in the event of compromised private keys of certification authorities

If it becomes known that the private keys of a CA or root CA are compromised, the incident is immediately investigated, assessed, and the necessary steps are taken.

The relevant parties involved shall be informed of the possible compromise in writing. If necessary, the certificate(s) must be immediately revoked and the corresponding information forwarded to the supervisory authority. The generation of new keys and certificates must be documented in accordance with the work instructions and monitored in accordance with the conditions of the relevant security plan.

User certificates issued by these certificates are also revoked. The affected certificate owners are informed of the revocation. Information on the revocation status of end-user certificates as well as the end-user certificates that are based on compromised private keys may no longer be valid.

5.7.4 Business continuity after a disaster

Telekom Security has developed, implemented, and tested an emergency plan for data center operation in order to alleviate the effects of catastrophes of all kinds (natural catastrophes or catastrophes of human origin) and to restore the availability of critical business processes as quickly as possible. This also includes all Trust Center processes, components, systems, and services. This plan is reviewed at least once a year, tested and updated accordingly, so as to be able to respond in a targeted and structured manner in the case of a disaster. Regularly created backups are used in order to restore data after a disaster. These are checked for functionality on a regular basis.

The emergency plan contains at least the following information:

- The necessary criteria for activating the plan
- Possible emergency measures (depending on the situation)
- Fallback procedures
- Restart procedure
- Procedure for regular maintenance, updating, and further development
- Awareness-raising measures
- Training requirements for the affected personnel
- The responsibilities of the individuals (role description and assignment)
- Recovery time objective (RTO)
- Regular execution of the emergency plans for test purposes
- A procedure for maintenance or timely restoration of business activities following an interruption or failure of critical business processes
- An obligation to back up or keep critical cryptographic devices and information at a different location
- Specification of the maximum tolerable downtime (MTO) and corresponding restoration times
- Frequency at which backups are created of critical business information and the software used including its configuration
- Physical distance between the backup locations or facilities and the main office or the Trust Center data center
- Procedure for securing the business premises and facilities as well as possible following a disaster (emergency operation) until secured normal operation in line with the requirements is restored.

As part of a compliance audit, the auditor is authorized to view the details of the emergency plan.

Key material of the end entity which has been issued on smartcards is not covered under this emergency plan.

5.8 Cessation of a certification or registration authority's operations

5.8.1 Cessation of the certification authority

5.8.1.1 Certification service provider in accordance with eIDAS

If the certification service ceases operations, the certification authority proceeds in accordance with the requirements of ETSI EN 319 401 Section 7.12 and shall draw up a termination plan for this. This cessation plan applies to all qualified signature certificates (signature cards and remote electronic signature) of the TSP.

Among other things, the cessation plan covers the following:

- Notification of the end entity and relying parties of the planned cessation of the service. This information also includes a description of the future access to the archived data
- Continuation of revocation functions, including the regular generation of revocation lists, retrieval of certificate status information and service desk functions
- Revocation of issued CA certificates
- Any transitional regulations required for a successor CA
- Reimbursement of costs depending on the content of existing individual agreements
- Retention of the documentation and archives of the certification authority (CA)

All possible measures shall be taken prior to cessation of the service in order to minimize the potential damage for all parties involved and to ensure that all those concerned are informed as early as possible.

All rights are withdrawn from the employees of the certification authority and the registration authorities and the private keys of the CA are destroyed. All certificates that are still valid are revoked. The certificate owner's remote electronic signature key will be deleted at the time of cessation of operation.

All electronically recorded data is deleted with the exception of the certificates and revocation lists. The certificates, revocation lists, and paper documents are archived so that they can, if necessary, be accessed for evidential purposes in case of litigation.

Archiving will continue to be carried out in accordance with the requirements of this document and the valid laws.

5.8.1.2 Certification service providers for non-qualified certificates

Termination of operations may only be invoked by the Telekom Security Board of Management.

A cessation plan may include the following regulations:

- Continuation of the revocation service
- Revocation of issued CA certificates
- Any transitional regulations required for a successor CA
- Reimbursement of costs depending on the content of existing individual agreements
- Retention of the documentation and archives of the CA

If operations (the revocation service, in particular) are not taken over by another certification authority, all certificates issued will be revoked. Necessary precautionary measures are taken to ensure continued operation of the revocation service.

5.8.2 Cessation of the external registration authority

As all customers are managed centrally via the certification authority, and no documents remain with a registration authority, the cessation of a registration authority has no impact on operation and the customers.

6 TECHNICAL SECURITY CONTROLS

6.1 Generation and installation of key pairs

6.1.1 Generation of key pairs

6.1.1.1 Generation of end-user key pairs

Key pairs for end-user certificates are generated on the QSCD itself (certificate owner's chip card or HSM of the TSP) which possess certification for qualified signature creation units in accordance with eIDAS (QSCD). After they are generated, keys are securely stored on the respective QSCD. For remote electronic signature, the keys are stored on an HSM in the Telekom Security Trust Center. The private keys of the end users are subject to the same protection measures as the key materials of the TSP. With regards to the chip card, the private key is securely stored on the chip card. In both cases, the private key can no longer be read out after storage. Key generation (preproduction) and the generation and storage of an end-user certificate take place in separate production steps.

The requirements of the SOG-IS algorithm catalog apply to key generation and usage.

6.1.1.2 Generation and renewal of CA or root certificates

All key pairs are generated and stored by qualified and trusted experts (trusted roles) in a low-radiation room on a security-checked hardware security module (FIPS 140-2/level 3-evaluated) or on QSCD devices in what is known as the "key ceremony."

All activities during the key ceremony are logged and signed by all persons involved. These records are stored for auditing and tracking purposes for a period deemed suitable by Telekom Security.

In the course of a regular change of a CA certificate, Telekom Security guarantees a reasonable period for the transition between CA certificates. In particular, the validity check for the existing end-user certificates is taken into account.

The offline CA systems – consisting of a certification instance, cryptographic hardware module (HSM) (incl. backup token) and browser – are operated "offline," i.e., without a connection to any network structure. The systems of the offline CA are accommodated in a lockable computer rack and are sealed against opening and exchange. The integrity of the seal is checked and documented with each use of the offline CA.

Key backups are only carried out using the dual-control principle, providing the hardware used on the CA key supports this. These backups (including restoration) can only be accessed using the dual-control principle.

The algorithms for CA and root certificates are selected in cooperation with the Federal Network Agency and the conformity assessment body for eIDAS.

Any interested party can register as a recipient of the newsletter with PKS Support. Shortly before a CA certificate expires, it is replaced by a newly generated certificate. CA certificates (incl. backups of the private key) that are no longer required are rendered unusable.

The validity of certificates begins with generation of the certificate and ends when the validity period expires or through revocation. The validity period of key pairs is the same as the validity period for the corresponding certificate.

More details on this process can be found in the process documentation of the offline CA.

The CA keys are only used for signing of end-user certificates.

6.1.2 Assignment of private keys to end entities

Smartcards are sent to end entities by post.
No keys are delivered in the remote electronic signature variant.

6.1.3 Assignment of public keys to certification authorities

Certificates are issued exclusively by the TSP.

6.1.4 Assignment of public certification authority keys to relying parties

No stipulation.

6.1.5 Key lengths

The algorithms of the keys that are used and the signature algorithms are regularly adapted in line with technological progress. The following table shows an overview of when particular keys have been used.

Table 4 – Key algorithms used

Key	Used until/since
RSA 1024 bit	Dec. 31, 2007
RSA 2048 bit	Dec. 31, 2014
Elliptic curves	Used since Jan. 15, 2013
RSA 2048 bit	Used since March 1, 2020 for remote electronic signature certificates

All certificates may only be valid as long as the algorithm catalog published by the SOG-IS Crypto Working Group classifies algorithms used as secure. The details in the algorithm catalog supplement details given here regarding the maximum validity period and take precedence over details stated here.

6.1.6 Generating the parameters of public keys and quality control

No stipulation.

6.1.7 Key usage (according to the X.509v3 expansion "key usage")

The key usage is based on the rules of RFC5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” and is described therein.

6.2 Protection of private keys and technical controls of cryptographic modules

The Telekom Security Trust Center has implemented physical, organizational, and procedural mechanisms to ensure the security of CA and root CA keys. These mechanisms are also used for protection of end-user keys on the HSM to ensure that the key and the certificate are under the sole control of the legal user. The end user is responsible for protection of the private key on the chip card.

To prevent the risk of a key being compromised during the transfer between two HSMs, encryption mechanisms are applied. The valid key for the connection between two HSMs is stored on a carrier medium in a TSP safe. The safe is not located at the data center location. In addition to the key used, direct access to the HSM at the respective data center location is required. This ensures that there is no possibility of compromise in the transfer channel.

End entities are obliged to take all necessary precautions to prevent the loss, disclosure, or unauthorized use of private keys.

6.2.1 Standards and checks for cryptographic modules

The private keys of the CAs are stored on suitable QSCDs. Keys are backed up using high-quality multi-person backup techniques.

To protect cryptographic devices during operation, transport, and storage, the manufacturer-specific mechanisms are applied.

6.2.2 Multi-person controls (m out of n) for private keys

Telekom Security has implemented technical, organizational, and procedural mechanisms that require the involvement of several trusted and qualified persons of the Telekom Security Trust Center (trusted roles) to be able to carry out confidential cryptographic CA operations. The usage of private keys is protected by a divided authentication process (Trusted Path Authentication with Key) known only to the persons responsible for it. Every person involved in the process has access to pieces of confidential information. However, certain activities can only be carried out if the aforementioned information is known in its entirety.

6.2.3 Storage of private keys

No stipulation.

6.2.4 Backup of private keys

No stipulation.

6.2.5 Archiving of private keys

No stipulation.

6.2.6 Transfer of private keys in or from a cryptographic module

No stipulation.

6.2.7 Storage of private keys on cryptographic modules

The Telekom Security Trust Center saves CA keys in a secure manner on cryptographic hardware security modules (HSM) that are evaluated in accordance with FIPS 140-2/level 3.

Smartcards save externally generated or self-generated keys in a secure form.

6.2.8 Method for activating private keys

All end entities must protect the activation data (e.g., PIN) for their private key against loss, theft, change, disclosure, and unauthorized usage in accordance with the present CP/CPS.

The private key of a certificate from a sub-certification authority (Sub-CA) remains active until the validity period has been exceeded or there is a revocation reason that triggers revocation of the certificate.

6.2.9 Method for deactivating private keys

The deactivation of CA and root CA keys is event-based and the responsibility of the Trust Center staff at Telekom Security.

The deactivation of private keys (end entities, registrars) is the end user's responsibility.

6.2.10 Method for destroying private keys

The destruction of CA keys requires the participation of several trusted persons (trusted roles) from the Trust Center. After the key has been destroyed, it needs to be ensured that there are no residual fragments which could lead to the key being reconstructed.

Telekom Security uses an integrated deletion function of the HSM for secure destruction of keys.

End entities are responsible for destroying their own private keys.

6.2.11 Evaluation of cryptographic modules

See Section 6.2.1

6.3 Other aspects of managing key pairs

6.3.1 Archiving of public keys

The certificates (CA and root certificates) are backed up and archived during Telekom Security regular backup measures.

6.3.2 Validity periods of certificates and key pairs

The validity of certificates begins with generation of the certificate and ends when the validity period expires or through revocation. The validity period of key pairs is the same as the validity period for the corresponding certificate. However, the certificates can continue to be used for decryption and signature validation provided the corresponding key is available.

6.4 Activation data

6.4.1 Generation and installation of activation data

In order to protect the private keys of the CA and root CA certificates stored on the HSM, activation data (pieces of confidential information) is generated according to the requirements described in Section 6.2.2 of this CP/CPS and the "key ceremony" document. The generation and distribution of confidential information pieces are logged.

6.4.2 Activation data protection

The Trust Center administrators or persons authorized by Telekom Security undertake to protect the confidential information parts for activating the private keys of CA, root CA, and OCSP certificates.

6.4.3 Other aspects of activation data

If activation data for private keys is transferred, regardless of the transfer medium, the Trust Center administrators must protect the transfer applying methods for protecting against loss, theft, changes, unauthorized disclosure, or use of these private keys.

When using a combination of user name and password to log on to networks as activation data for an end entity, the passwords to be transmitted in a network also need to be protected against access by unauthorized third parties.

6.5 Computer security controls

Only systems that are designed for use in data centers are used in the Telekom Security Trust Center. Only software components that are needed for operational purposes are installed on these systems in addition to the operating system. All the Trust Center's core systems are redundant. Hardware is monitored for malfunctions and defects and is regularly replaced. Settings that are made are automatically checked ona regular basis in order to detect any changes. Functions of the services provided are tested at short intervals. Security-relevant modifications, malfunctions, or defects are immediately forwarded to the responsible persons as soon as they occur so that the responsible persons can react appropriately.

All systems are operated in controlled-access areas in order to exclude the possibility of physical modifications to systems or data media being manipulated.

All important actions on servers are centrally logged. After completion, the integrity of logs is secured in a manner that makes it possible to detect retrospective changes.

The created audit logs/history data/logging files are continuously examined for important events relevant to security and operations. Furthermore, Telekom Security checks its audit logs/logging files for suspicious and unusual activities resulting from irregularities and faults.

Audit, history, and event logging data is archived in accordance with the current legal provisions. The retention period for log data that is not directly associated with the certificate life cycle is 42 days. Measures taken in response to the analysis of audit logs/logging files are also logged.

Operating systems that support the implementation of security settings are used on the Trust Center's systems. None of the systems can be used without user registration.

The enforcement of access restrictions on the systems is supported by the implemented restrictive password policy.

Particularly security-critical applications (such as certificate generation) also require authentication of the user at the Trust Center.

All these measures are in agreement with the access concept created by the TSP.

Use of the application to issue certificates is secured by multi-factor authentication.

The TSP performs a penetration test (PEN test) on the TSP systems

- upon setup,
- extensive upgrades or changes to the infrastructure or applications that the TSP considers to be significant,
- but at least once per year.

The TSP provides evidence that each penetration test has been conducted by a person or organization that has the capabilities, tools, knowledge, ethics, and independence required to produce a reliable report.

The systems' settings are regularly audited by a conformity assessment body in accordance with eIDAS.

6.5.1 Specific technical requirements for computer security

6.5.1.1 Use of security-tested components

The eIDAS Regulation requires the use of security-tested media for storing certificates and key materials for various purposes. The following list shows some of the components that are used:

- The QSCDs used to generate and store private keys are approved as a qualified signature creation device in accordance with the eIDAS Regulation.

- The HSMs used for the certificate signature and OSCP have similar certifications.

6.5.1.2 Access control to the systems

Operating systems that support the implementation of security settings are used on the Trust Center's systems. None of the systems can be used without user registration. Security-critical settings (user accounts for instance) can only be modified using the dual-control principle. The enforcement of access restrictions on the systems is supported by the implemented restrictive password policy.

Particularly security-critical applications (such as certificate generation) also require authentication of the user at the Trust Center.

In particular, Telekom Security has implemented mechanisms to protect the revocation status service (CRL, ARL, OCSP) against unauthorized access attempts to prevent manipulation of revocation status information (add, delete, change).

6.5.1.3 Data backup

All relevant certification service data is backed up regularly. The usability of these data backups is checked by means of spot checks. Data backups are relocated at specific intervals in order to ensure continued operation in the event of a catastrophic event.

Telekom Security has implemented mechanisms to protect the central data storage (Repository) against unauthorized access attempts to prevent manipulation of revocation status information (add, delete, change).

6.5.2 Assessment of computer security

Following every significant change in the system or network, an automatic vulnerability scan is performed within a week, but at least once per calendar quarter. Potential vulnerabilities are analyzed, assessed, and registered. Based on the assessment, measures are determined and implemented in a defined plan. The vulnerability scans, their results and actions (resolutions, replacement) are documented.

Critical vulnerabilities are handled via the ISMS process. Critical vulnerabilities reported to the TSP are evaluated by the ISMS team within 48 hours and a solution scenario is presented. In the event that immediate and complete elimination of the vulnerability is not possible, a treatment plan is set up with the aim of reducing the critical vulnerabilities.

In addition, “penetration tests” are implemented once a year. In this case, corresponding measures are derived and implemented too, if necessary.

6.6 Technical controls on the life cycle

6.6.1 System development controls

Telekom Security has implemented mechanisms and controls to monitor and protect purchased, developed, or modified software for damaging elements or malicious code (e.g., Trojans, viruses). The integrity is manually verified prior to installation.

New software versions (planned updates) or fault resolutions (short-term bug fixes) are initially provided and tested on the manufacturer's/developer's development system.

After a check, the software is installed on the Telekom Security test system. The software is installed on the Telekom Security live system only following successful tests. All changes to the systems are documented in accordance with the requirements of the Telekom Security change and release process.

Telekom Security' established change and release management is applied.

6.6.2 Security management controls

Telekom Security has implemented mechanisms and/or policies to be able to control and monitor the configuration of its CA systems. The integrity is manually verified prior to installation.

The system accounts of the Trust Center administrators are checked after 90 calendar days at the latest. Accounts that are no longer needed are deactivated.

6.6.3 Security controls on the life cycle

Telekom Security has implemented mechanisms and controls to ensure that security patches are installed within a reasonable time after they are available. The integrity of the security patch is manually verified prior to installation.

A security patch is not installed if additional security gaps or instabilities arise that outweigh the advantages of using the security patch. The reason for not applying security patches is documented.

6.6.3.1 Capacity management

Telekom Security carries out all PKI functions with the help of reliable and appropriate systems. The functionality and capacity of the systems are continuously checked by monitoring systems so that resources can be extended promptly if necessary.

The monitoring data collected on the CPU, storage, and disk utilization (periodically every 5 minutes) is provided with warning and alarm thresholds. At the latest when the warning level occurs, the resource planning is reviewed and, if necessary, adapted by extensions (e.g., hardware retrofitting, relocation of services to other systems, or assignment of further resources to virtual machines).

6.7 Network security controls

All the network core components are redundant. Connections to the internet and other communication networks are redundant and provide the necessary bandwidth to meet operational needs. The network components are automatically and regularly monitored for malfunctions, defects, or manipulation. In addition, the network structure is subject to a review at regular intervals. Systems that are used to implement the security policy must not be used for any other functions.

The Trust Center's network is divided up into several zones that have different security requirements. Each zone can communicate with another zone only via a firewall. Only the minimum required rules for communication between the various zones are permitted in the firewalls. The IT systems are administrated via a separate network.

Communication between the Trust Center's various locations takes place via encrypted VPN connections. Session keys, which are regularly changed, are used for VPN connections. Encryption devices only accept connections from other encryption devices that are included in its own white list.

All authorized users must identify themselves to the systems using established mechanisms; accounts that are no longer required are deleted or deactivated.

The requirements under [ETSI EN 319 401] Section 7.8 are implemented.

6.8 Time stamp

Certificates, revocation lists, online status checks, and other important information comprise date and time information derived from a reliable time source. A cryptographic time stamp is not used.

7 CERTIFICATE, REVOCATION LIST, AND OCSP PROFILES

7.1 Certificate profile

The specification for the certificate profile for qualified signatures is available on the TeleSec PKS website
https://www.telesec.de/signaturkarte/ → Support → Download area → Technical documentation
The specification for the certificate profile for advanced certificates is available on the TeleSec PKS website
https://www.telesec.de/signaturkarte/ → Support → Download area → Technical documentation

7.2 Revocation list profile

No stipulation.

7.3 OCSP profile

The specification for the OCSP responder is available on the TeleSec PKS website
https://www.telesec.de/signaturkarte/ → Support → Download area → Technical documentation

8 COMPLIANCE AUDITS AND OTHER REVIEWS

In order to check compliance, the TSP is audited by both internal auditors as well as by a recognized conformity assessment body (in accordance with ETSI EN 319 403). Besides the documentation (security concept, operating concept, and other internal documents), the implementation of processes and compliance with provisions are reviewed in the course of the audits.

TeleSec Public Key Service (qualified area): The Telekom Security processes are subject to a regular annual audit (ETSI EN 319411-2, policy QCP-n-qcsd) by an independent third party. In addition, Telekom Security carries out internal audits at regular intervals.

TeleSec Public Key Service (non-qualified area): The Telekom Security processes are subject to a regular annual audit (ETSI EN 319411-2 policy NCP+) by an independent third party.

For TeleSec PKS, the required audits are stored in accordance with the ETSI EN 319 411-2 criteria (in combination with ETSI EN 319 401 and ETSI EN 319 411-1). The corresponding reports are published on the website https://www.telesec.de/en/.

8.1 Interval or reason for audits

Compliance audits generally take place annually or as required. In addition, the Trust Center conducts annual emergency exercise drills.

8.2 Identity/qualifications of the auditor

The Trust Center-specific compliance audits are carried out by qualified employees of Telekom Security or a third party (e.g., qualified company such as TÜV IT) with experience in the fields of public key infrastructure technology, security auditing, as well as procedures and aids for information security.

8.3 Relationship of the auditor to the authority to be audited

The auditor for the eIDAS certification is an independent, qualified auditor (e.g., external auditor, expert).

8.4 Topics covered by audit

The aim of the audit is to implement this document. All processes associated with the life-cycle management of certificates are to be reviewed:

- Identity verification of end entities
- Certificate request procedures
- Processing of certificate requests
- Certificate renewal
- Certificate revocations

- Access control
- Authorization and role concept
- Anti-break-in measures
- Human resources

In any event, auditing is carried out in accordance with the applicable versions of the audit criteria of the ETSI standards listed above.

8.5 Measures for resolving deficits

If defects or deficits are detected on the operator of a certification authority's side during a compliance audit or by an auditor, a decision is made regarding the specific corrective measures to be taken. The head of the Trust Center decides together with the auditor which suitable measures should be implemented in an economically suitable timeframe. In the event of serious security-critical deficits, a correction plan must be devised within 10 days and the deviation rectified. In the event of less serious deficits, the head of the Trust Center will decide on the rectification timeframe.

8.6 Communication of results

The results of the audit will be documented in a report prepared by the auditor and passed on to Telekom Security.

Telekom Security reserves the right to publish results or partial results if misuse occurred or the image of Telekom Security was harmed.

8.7 Internal audits

In addition, Telekom Security carries out internal audits at regular intervals. These internal audit measures (quality assessments) are carried out by suitably qualified Telekom Security employees.

The Telekom Security Trust Center also carries out an annual risk assessment.

The assessment covers at least the following items:

- Identifying foreseeable potential external and internal risks (i.e., especially their underlying vulnerabilities) which might lead to
  - Unauthorized access to relevant data or systems,
  - Handover or misuse of relevant data,
  - Modification or destruction of relevant data,
  - Impairment, interruption, or failure of parts of or the entire certificate management process,
  - An economic risk.
-
- Assessment of the probability of occurrence and the resulting potential damage (i.e., extent of damage) due to exploitation of a vulnerability. Here, the special security requirements of certificate data and the certificate management process must be taken into account.

- Assessment of the effectiveness and suitability of the countermeasures taken (e.g., policies, procedures, security systems used, technologies, insurance policies) in order to remove the danger or minimize the risk.

Based on the risk assessment, the Telekom Security Trust Center has developed a security plan that is regularly reviewed and, if necessary, modified. This security plan consists of procedures, measures, and products used to support the assessment and management of risks that are identified during the risk assessment. The security plan contains administrative, organizational, technical, and physical security measures according to the sensitivity of the data and the certificate management process.

9 OTHER BUSINESS AND LEGAL PROVISIONS

9.1 Charges

The current price list is available on the TeleSec PKS website

https://www.telesec.de/signaturkarte/ → Support → Download area → General Terms and Conditions and prices

9.1.1 Charges for the issuance or renewal of certificates

Telekom Security is entitled to charge for issuing end entity certificates. This applies in particular to the provision and handover of the PKS service.

9.1.2 Charges for certificate access

Telekom Security does not charge for access to certificates in the directory service of the Public Key Service.

9.1.3 Charges for access to revocation or status information

Telekom Security does not charge for access to revocation or status information for the relevant parts that fall under the scope of this document.

9.1.4 Charges for other services

Telekom Security does not charge for accessing and viewing this CP/CPS document. Any other usage, e.g., reproduction, amendment, or production of a derived document, is subject to the written consent of the authority (Section 1.5.1) that owns the copyright (Section **Fehler! Verweisquelle konnte nicht gefunden werden.**).
The use of this CP/CPS is also free of charge provided it is used as an applicable contract document for the contractual relationship between the respective partner and Telekom Security.

9.1.5 Compensation

Telekom Security reimburses charges in accordance with the legal regulations under German law.

9.2 Financial responsibilities

The financial responsibilities are described in the General Terms and Conditions (GT&C) for the TeleSec Public Key Service, which are available at any time at
https://www.telesec.de/signaturkarte/ → Support → Download area → General Terms and Conditions and prices

9.2.1 Insurance coverage

Telekom Security has business liability insurance and D&O liability insurance cover. It is guaranteed that the requirements arising from the insurance cover are fulfilled.

9.2.2 Other financial resources

No stipulation.

9.2.3 Insurance or warranty coverage for end entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Confidential information is any information from parties involved in PKI that has not been published or has not been explicitly approved for publication and that is not covered by Section **Fehler! Verweisquelle konnte nicht gefunden werden.**.

9.3.2 Scope of non-confidential information

Non-confidential information is any implicit and explicit information that is included in issued certificates, revocation lists, or status information, or can be derived from these.

9.3.3 Responsibility regarding the protection of confidential information

Telekom Security, as a certification authority, is responsible for the protection of confidential information and compliance with data privacy provisions.
Furthermore, in taking on tasks within the framework of approval and attribute confirmation, chamber employees are also obliged to handle confidential information accordingly.

9.4 Protection of personal data

9.4.1 Data privacy concept

Telekom Security has to electronically store and process personal data in order to provide this service. Telekom Security will ensure the technical and organizational security and other measures in accordance with § 9 BDSG [Federal Data Protection Act] and the annex to § 9 BDSG.
A data privacy concept has been set up in accordance with Group provisions. This data privacy concept summarizes the aspects of the PKI service that are relevant to data privacy.
Excerpts from the data privacy concept can be provided upon request.

9.4.2 Data to be treated as confidential

For personal data, the provisions analogous to Section **Fehler! Verweisquelle konnte nicht gefunden werden.** apply.

9.4.3 Data not to be treated as confidential

For personal data, the provisions analogous to Section **Fehler! Verweisquelle konnte nicht gefunden werden.** apply.

9.4.4 Responsibility for the protection of confidential data

For personal data, the provisions analogous to Section **Fehler! Verweisquelle konnte nicht gefunden werden.** apply.

9.4.5 Notification and consent for the use of confidential data

The applicant consents to the use of personal data by the certification authority or the responsible chamber, provided such use is required in order to render the service.

Furthermore, any information that does not have to be treated as confidential in accordance with Section **Fehler! Verweisquelle konnte nicht gefunden werden.** may be published.

9.4.6 Disclosure pursuant to legal or administrative process

The obligation not to disclose confidential information or personal data does not apply if disclosure of such information/data has been ordered by force of law or by a court ruling or an administrative authority, or serves to implement legal judgments. As soon as there is reason to institute legal or official proceedings, which could lead to confidential or private information being disclosed, the contracting party involved in the proceedings will inform the other contracting party about this, taking into account the legal provisions.

9.4.7 Other reasons to disclose data

No stipulation.

9.5 Intellectual property rights (Copyright)

This document is protected by copyright. It is not permitted to use the texts or diagrams or extracts thereof without the written consent of Telekom Security.

9.6 Assurances and guarantees

9.7 Exclusion of liability

Despite the utmost care taken while creating this documentation, Deutsche Telekom AG or Deutsche Telekom Security GmbH are unable to exclude the possibility that the policies described herein may contain any errors. Deutsche Telekom AG as well as Deutsche Telekom Security GmbH rejects any liability in this case.
There is no statutory right to have the TeleSec Public Key Service issue a certificate.

9.8 Limitations of liability

Liability issues are regulated in the General Terms and Conditions (GT&C) for the TeleSec Public Key Service, these are available from the following website at any time
https://www.telesec.de/signaturkarte/→ Support → Download area → General Terms and Conditions and prices

9.9 Claim for damages

Claims for damages are regulated in the General Terms and Conditions (GT&C) for the TeleSec Public Key Service, these are available from the following website at any time
https://www.telesec.de/signaturkarte/→ Support → Download area → General Terms and Conditions and prices

9.10 Term and termination

9.10.1 Term

The initial publication of this CP/CPS document as well as modifications to this document enter into force at the time of publication on public Telekom Security websites.

9.10.2 Termination

This CP/CPS remains in effect in the latest version until it is replaced by a new version.

9.10.3 Effect of termination and continuance

When the Public Key Service ends, all end-entity certificates remain bound by the regulations contained in the CP/CPS until the last certificate issued expires or is revoked.

9.11 Individual notices and communications with subscribers

Unless otherwise contractually agreed, the up-to-date contact details (address, email, etc.) for individual messages and communication with the TSP Deutsche Telekom AG will be given).

9.12 Changes

In order to respond to changing market requirements, security requirements and legislation, etc., Telekom Security reserves the right to amend or adjust this document.

9.12.1 Procedure for amendment

Amendments to this CP/CPS can only be made by the publisher's Change Advisory Board. With every official change, this document receives a new ascending version number and publication date.
Amendments enter into force immediately upon publication.

Updated versions of this document result in the previous document versions becoming invalid. In the event of contradictory provisions, the Telekom Security Advisory Board shall decide on how to proceed.

Within existing contracts, the delegated third party must be informed about amendments to this CP/CPS in writing at least six weeks before they come into force. In the event of amendments to the detriment of the delegated third party, they have the right to special termination at the time the amendments come into effect. If the delegated third party does not terminate the agreement in writing within six weeks after receipt of the change notification, the changes will become part of the agreement effective from the time they enter into force.

9.12.2 Notification procedures and periods

Tenants will be notified about amendments and are given the opportunity to object within six weeks. If no objections are made, the new document version enters into force as specified in Section 9.12.1. Any claims beyond this for individual end users to be notified are explicitly excluded.
If the Telekom Security Advisory Board believes that, for example, significant security-relevant amendments are required immediately, the new CP/CPS will enter into force immediately upon its release (see Section 9.12.1).

9.12.3 Reasons that lead to the object ID having to be changed

The Telekom Security Advisory Board decides whether the object ID of the CP/CPS needs to be changed. Otherwise, amendments do not lead to the object ID of the Certificate Policy having to be changed.

9.13Provisions for settling disputes

In the event of disputes, the parties shall come to an agreement taking into account any applicable laws, regulations, and agreements made.

9.14Applicable law

The eIDAS Regulation regulates the issuance of qualified certificates in general. The law of the Federal Republic of Germany shall apply. The place of performance and the exclusive place of jurisdiction is Frankfurt/Main, Germany.

9.15Compliance with applicable law

The present document is subject to the applicable German laws, regulations, policies, ordinances, acts, and orders, in particular the import and export provisions for security components described therein (software, hardware, or technical information). Applicable mandatory laws, regulations, policies, ordinances, acts and orders result in the corresponding provisions of this CP/CPS becoming invalid.

9.16Miscellaneous provisions

9.16.1 Complete contract

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability clause

If a provision of this CP/CPS is or becomes ineffective or cannot be implemented, the validity of the remainder of this CP/CPS is not otherwise affected as a result. Instead of the ineffective and unenforceable provision, a provision that comes closest to the economic purpose of this document in a legally binding manner is considered agreed. The same applies to additions made in order to close contractual lacunas.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force majeure

The regulations in the individual contract apply.

Within the legally permissible framework, contracts with partners, relying parties, or end entities must contain protection clauses regarding force majeure in order to protect Telekom Security.

This regulation is intended to ensure that Telekom Security agrees with its tenants, relying parties, or end entities that Telekom Security will not fall into arrears if the service is delayed or becomes impossible due to force majeure.

9.17 Other provisions

9.17.1 Other documents

Other documents, such as the GT&Cs and the PKS Info can be accessed via the following link:
https://www.telesec.de/en/signaturecard/support/download-area

9.17.2 Barrier-free accessibility

Access to the TC services is essentially browser-based. Operating systems offer a variety of different accessibility features to make it easier for disabled persons to access the web portals of the Trust Center Services. In particular, these compensate for visual and hearing impairments, physical disabilities, and sensory disorders (e.g., “Information on barrier-free accessibility for IT experts”).
In addition, analyses with the software development partners of the Trust Center are carried out to check whether there are further, meaningful, operating system-independent ways for barrier-free accessibility (e.g., via HTML5) in addition to these standard tools.
If the abovementioned measures are insufficient, Telekom Security also offers disabled persons free telephone support for assistance with the application for, acceptance, and revocation of certificates.

9.17.3 Complaints and escalation

9.17.3.1 Notification of the parties to a dispute

Before initiating proceedings to settle a dispute (including litigation or mediation) in connection with a dispute relating to an aspect of this CPS or an issued certificate, the persons who feel that their rights have been infringed shall notify the TeleSec Trust Center, the LRA/RS in question, or any other affected party in order to attempt to resolve the dispute amicably.

9.17.3.2 Escalation

If the dispute cannot be resolved within ten (10) days after preliminary notification in accordance with CPS § 9.17.3.1, a party to the dispute may refer the matter, in writing or electronically, to Telekom Security and request examination.

Telekom Security then convenes a body comprised of PKI experts in order to gather the relevant facts with a view to settling the dispute. The diligent party shall submit a copy of the matters of fact and law to all the other parties. A party who has not raised a matter can, within one (1) week after the date on which the dispute was referred to the body, communicate relevant information to the body. The body must give its recommendation and communicate it to the parties within three (3) weeks (unless the parties agree to extend this deadline by a specific time) after the date on which the matter was referred to the body. The body normally uses email, teleconferences, couriers, and letter mail during the course of its work. The body's recommendations are not binding on the parties. This procedure does not exclude legal recourse.