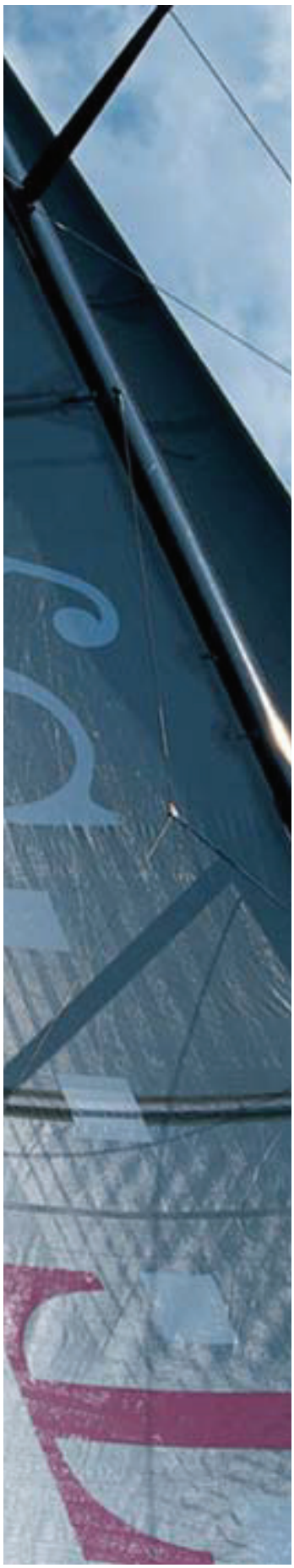
Public Key Service

Certificate Practice Statement



Version:	3.4
Last revised:	August 23.08.2017
Status:	final

T · · Systems ·

T · · Systems ·

Publication details

Published by

T-Systems International GmbH
Trust Center
Untere Industriestraße 20
57250 Netphen

Contact	Phone/fax	E-mail
TeleSec Support Line	Tel.: +49 1805 268204	TeleSec_Support@t-systems.com

Brief summary

Certificate Practice Statement for the TeleSec Public Key Service

Change history

Version	Last revised	Edited by	Changes/comments
1.0	Jan. 14, 2005	Jog	Original version in English
1.1	Jan. 21, 2005	Jog	Editorial changes
1.2	Jun. 17, 2005	Jog	Revision
1.3	Aug. 10, 2005	SB	Translation into German
1.33	Sep. 7, 2005	Jog, SB	Revision
2.0	Sep. 20, 2007	PS	QA checked and updated Certificates for Netkey3.0 (RSA2048)
2.1	Sep. 21, 2007	PS	Comments and notes by DD, TH and JK regarding Quality Assurance added
3.0	Apr. 19, 2013	TH	Adapted in line with updated ETSI TS 102 042 requirements
3.1	May 19, 2014	JS	Adapted, on-line revocation and amendments in accordance with ETSI audit
3.2	Apr. 21, 2015	TH	2015 review
3.3	Apr. 8, 2016	TH, LK, JS	2016 review
3.3	Apr. 8, 2016	DD	Release
3.4	May 2, 2017	LK, TH JS	Review, revision for eIDAS

Table of contents

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 and advanced certificates in the context of the PKS.

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 Telekom Group unit T-Systems International GmbH. The Telekom Trust Center has been certified in accordance with ISO 9002 and ISO 9001:2000 since 1996 and January 2001, respectively.

Deutsche Telekom AG has been operating a Trust Center since 1994; in 1998 it 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*). This approval saw the start of the Public Key Service (PKS) in early 1999, the Trust Center was continually expanded and, since Jul. 1, 2016, has been compliant with the European Regulation on electronic identification and trust services (eIDAS).
Both its structural and organizational infrastructure meet the strict requirements of the German Digital Signature Act. Since starting operation, the Telekom Trust Center has issued more than 200 million certificates. The services offered by the Telekom Trust Center also include the T-TeleSec Public Key Service (PKS) which covers the process of issuing qualified certificates in accordance with EU Regulation No. 910/2014 (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 T-Systems International GmbH's PKS. This 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 PKS CPS covers the following aspects in detail:

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

A PKS Public Key certificate enables a subscriber to prove that they have electronically signed an electronic document with their (private) signature key which is stored on a secure signature creation unit (chip card). 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 use PKS attribute within certificates to restrict the use of the corresponding signature key or disclose additional information (e.g., power of representation).

1.2 Document name and identification

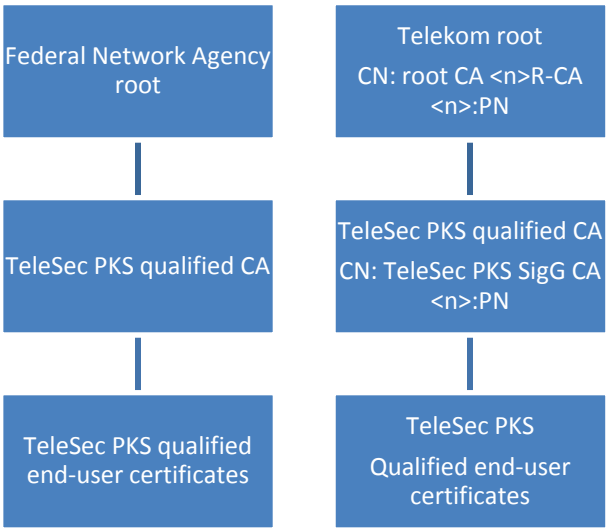
Name:	Certification Practice Statement for the TeleSec Public Key Service ® (PKS CPS)
Version:	3.4
Date	23.08.2017
Object identifier	1.3.6.1.4.1.7879.13.27

1.3 PKI participants

1.3.1 Certification authorities

1.3.1.1 Qualified certificates

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



The root certificates and the CA and service[1] certificates of PKS are created by the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway (hereinafter referred to as "BNetzA") as the responsible supervisory authority or by T-Systems International GmbH in accordance with the requirements of the eIDAS

[1] Certificates for signing Online Certificate Status Protocols (OCSPs), revocation lists, and qualified time stamps

Regulation. In order to acquire the status of a qualified trust service, certificates are included and published in the European Union's[2] Trust List after confirmation of eIDAS conformity. The above graphic illustrates the certification hierarchy, taking examples of selected certificates.

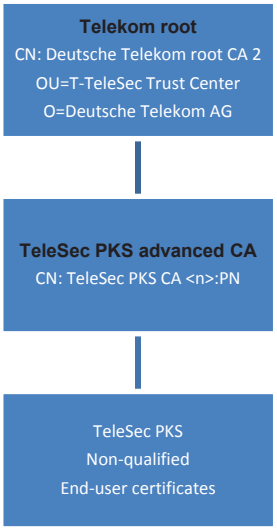
In accordance with the eIDAS Regulation, the PKS CA only issues qualified certificates. The certification path of PKS certificates can be audited right through to a root certificate. The PKS CA is operated in the high-security area of the Telekom Trust Center.

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

1.3.1.2 Non-qualified certificates

The issue 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 special closed user groups may possibly not receive non-qualified certificates. This depends on the agreements reached with the manager 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:



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+.

[2] Provisions regarding the Trust List can be viewed in the eIDAS Regulation.

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 who 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.

T-Systems' registration authorities have the following tasks in particular:

- Accepting orders and checking identification documents
- Checking that documents are genuine and complete
- Verifying identities

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

1.3.3 Subscribers

Subscribers 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 participants

1.3.5.1 Identity verifier

Identity verifiers 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.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

In the event of loss or misuse of a chip card/certificate, the subscriber 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.

1.4.2 Prohibited certificate uses

TeleSec PKS Public Key Service qualified certificates are used for qualified signatures in the meaning of the eIDAS Regulation.
Qualified user certificates match the policy QCP-n-qcsd.
In the event of loss or misuse of a chip card/certificate, the subscriber must arrange revocation immediately. This also applies if misuse is suspected or it is suspected that the key material used has been compromised.

1.4.3 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 (cf. Section1.3.1, Certification authorities). In addition, no OCSP service is offered for advanced certificates (cf. Section 2.1).

1.4.4 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 before the first of August 2017.
The chain model states that every certificate must have been valid at the point in time when it was used. This means 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 diagram below illustrates this.

The shell model has applied to end-user certificates since the eIDAS-compliant certification hierarchy was first put into service at the first of August 2017.

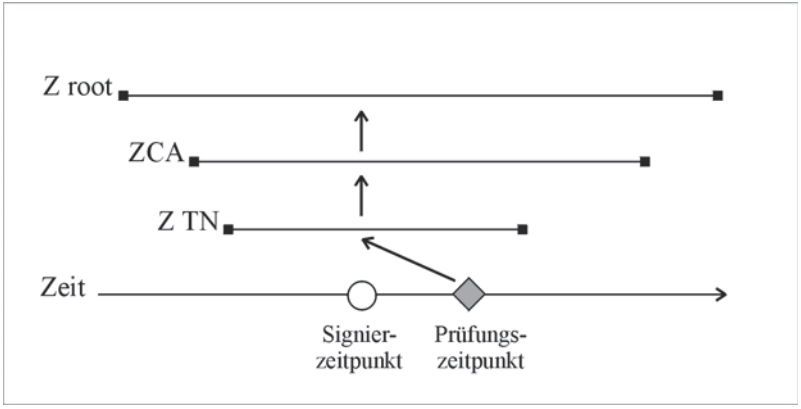


Fig. 1: Shell model

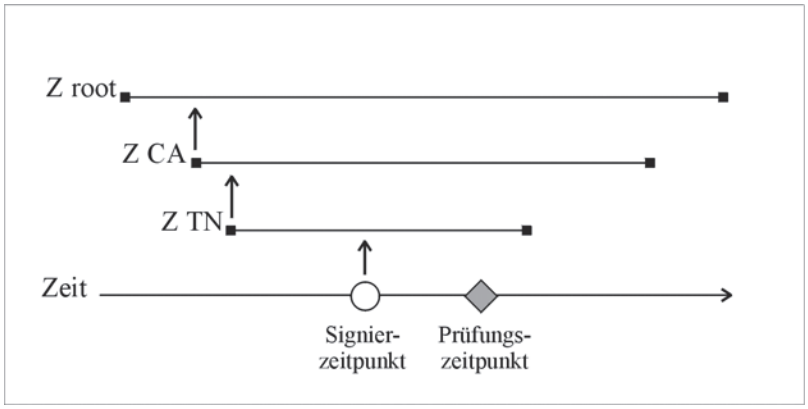


Fig. 2: Chain model

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 Organization administering the document

This CPS was published and will be maintained by T-Systems International GmbH.

1.5.2 Contact information

Address:
T-Systems International GmbH

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

Tel: +49 1805 268 204 [3]

Revocation hotline:

From Germany	116 116
From abroad	+49 30 4050 4050

E-mail: telesec_support@t-systems.com

[3] 14 cents/minute from the German fixed network, max. 42 cents per minute from mobile networks

WWW: http://www.telesec.de

1.5.3 Authority determining CPS suitability for the policy

Section 1.5.1 names the organization that is responsible for ensuring that this CP/CPS or 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 dealt with in accordance with the quality assurance and release process defined in the Trust Center's Operation Guide. This Guide makes provision for quality assurance and subsequent release by the Trust Center Manager in the event of revisions.

This CPS undergoes annual review, regardless of any other amendments. The annual review must be noted in the change history of the CPS. This applies even if no substantive amendments were made.

BNetzA	Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway
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 Institute
FIPS	Federal Information Processing Standards is the name for publicly announced USA standards
LDAP	Lightweight Directory Access Protocol
LRA	Local RA
OCSP	Online Certificate Status Protocol
PKD	Public Key Directory
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.
RA	Registration authority
SigG	German Digital Signature Act (*Signaturgesetz*)
SigV	German Digital Signature Regulation (*Signaturverordnung*)
Subscriber	Certificate recipient
Certificate recipient	Denotes a person who is the subject matter of a certificate and to whom a certificate has been issued.

2 Publication and repository responsibilities

2.1 Repositories

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

- http://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 on-line from the Public Key Directory (PKD). 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.

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 profile
- Information about the revocation service

The subscriber 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 certification service provider's website. In addition, in the event of security-critical incidents, the subscriber is notified directly in writing or by e-mail.

2.3 Time or frequency of publication

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 a year after their validity expires.
- Revocation lists are updated at least once every six hours.
- Policies are updated as required.

2.4 Access controls on repositories

Certificates and revocation lists are retrieved using LDAPv3 and OCSP responders are accessed by http. All access is not subject to any kind of access restrictions. There are no restrictions on read access to this information.

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

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 RS/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 RS/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

Issued Public Key certificates contain the name of the subscriber. The name of the subscriber 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.

E-mail addresses may only be included in a certificate if the subscriber has confirmed that they have access to the specified e-mail mailbox.

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 e-mail address, or other data of the principal (e.g., organization affiliation etc.) is entered in the certificate in addition to a name or a pseudonym.

3.2 Need for names to be meaningful

A name must uniquely identify the subscriber 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 match 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 for an entry in the certificate is too long the Trust Center will truncate it.

3.3 Anonymity or pseudonymity of subscribers

It is also 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 (for example, names such as "Telekom CA," political slogans, and names that suggest authorizations that the subscriber does not have are excluded).

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 Federal Armed Forces Counter-Intelligence Office, or the financial authorities or where courts have requested this in the context of pending proceedings in accordance with the relevant applicable provisions.

3.4 Recognition, authentication, and role of trademarks

Not applicable because certificates are only issued to natural persons and contain the name of the person in the subject DN.

3.5 Initial identity validation

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

The nature of the identity document, the ID number and validity dates of the ID are stated on the application form and stored in a database. A copy of the identity document must be enclosed with the application and is stored in the Trust Center's archives.

The subscriber'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.

3.6 Identification and authentication for re-key requests

The subscriber is notified in good time before the validity of their certificates expire. New certificates are issued to the subscriber if they apply for certificates before the validity of their existing certificates expire. Follow-up orders can be placed by providing a qualified signature using the certificate that is still valid.

3.7 Identification and authentication for revocation request

Persons and institutions who are authorized for revocations (see Section 4.9) may request the revocation of certificates in writing or by sending an informal letter.

A written revocation is authorized by comparing the signature on the letter with the signature on the original order form.

A certificate can be revoked immediately by calling the revocation hotline which operates 24/7. The "Tele PIN" of the certificate is needed in order to effect revocation by phone. The Tele PIN is defined by the ordering system and notified to the principal during the process of placing an order. The Tele PIN is used to authenticate the subscriber.

4 Certificate life-cycle operational requirements

4.1 Certificate Application

In the context of the TeleSec Public Key Service, orders must be in written form. The order must include the principal's handwritten signature. The necessary forms can be found on the TeleSec Public Key Service's 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 Who can submit a certificate application

Besides a completely and legibly filled-in order form a copy of the identification document (e.g., ID card) is required in order 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 Placement of an order for non-qualified certificates

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

4.2 Certificate application processing

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.

Key	Used until/since
RSA 1024 bit	31-Dec-07
RSA 2048 bit	31-Dec-14
Elliptic curves	Used since Jan. 15, 2013

In the case of all certificates, their validity cannot exceed the validity of the algorithm catalog published by the Federal Network Agency and the Federal Office for Information Security (BSI) which classifies used algorithms as suitable for qualified signatures. The details in the algorithm catalog supplement details given here regarding the maximum validity period and take precedence over details stated here.

Non-qualified end-user certificates have the same validity period as a qualified certificate on the same chip card.

An order for a qualified certificate is placed as follows:

- Fill in the requisite forms using the on-line 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 are duly signed.
- Personal identification of the principal in a Deutsche Telekom AG RS/LRA, using the PostIdent procedure, the BehördenIdent procedure or 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 subscriber. 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 related to orders before the 31. of July 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.

All order documents related to orders past the first of August 2017are archived in the Trust Center, in accordance with the requirements of the eIDAS, for 10 years after the last certificate that was issued on the basis of an order expires.

In case of subsequent orders the archiving period was determined by the longer period.

Purely digital transmission of a new order in order to create qualified certificates is not offered.

4.3 Certificate issuance

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 orders on hand and persons in the Trust Center's customer database.

4.3.1 CA actions during certificate issuance

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 issued certificate is either stored immediately on the subscriber's chip card or stored in the Trust Center's customer database so that it can be e-mailed to the subscriber later.

4.3.2 Issue of non-qualified certificates

Non-qualified certificates are created in parallel to qualified certificates. The checking, generation, and delivery procedures are identical.

4.4 Certificate acceptance

Certificates are delivered by sending the subscriber's personal chip card in a sealed envelope to the delivery address specified by the owner in the order.

The principal's confirmation of receipt is also part of the delivery process. See the next Section.

4.5 Confirmation of receipt of certificates

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

The chip card has a built-in protection mechanism. This procedure, patented as the NullPIN method, 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.

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 when they are issued. If a subscriber returns their confirmation of receipt and requests revocation in it, certificates are revoked.

The principal can transfer the confirmation of receipt on-line (by using a web form) or by mail. 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 mail.

4.6 Key pair and certificate usage

4.6.1 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 placed on 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 signature card, 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 protection requirements.
If the subscriber becomes aware that their private key has been compromised or if they suspect that their private key has been compromised, the subscriber is obliged to arrange revocation of their certificate immediately.

4.6.2 Relying party public key and certificate usage

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.

4.7 Certificate renewal

Automated certificate renewal is not offered. Principals who submit a follow-up order as described in Section 3.6 receive new key material. There is no provision in the current process for re-certifying existing key material.

4.8 Certificate modification

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 e-mail address of the subscriber 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 subscriber or other persons authorized to use a key have misused the key or are suspected of having misused it.
6. Legal provisions

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

- The subscriber.
- Third parties authorized to revoke certificates, these are:
    - Representatives of the subscriber.
    - Persons for whom the subscriber has a power of representation and this fact has been entered in the qualified certificate (see Section1.1.1).
    - The department that is responsible for work-related or other details if work-related or other details have been included in a qualified certificate (see Section1.1.1).
    - Bill recipient (*German: Rechnungsempfänger*)
- 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 on-line revocation form (website) or by a telephone call. An informal letter will only be accepted if it bears the handwritten signature of the 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 stationery.

In order to enable revocation, the Trust Center operates an on-line 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 on-line 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 on-line revocation form are published on the following website:
http://www.telesec.de/signaturkarte/ → Revocation service.

Even in the event of system defects, service work and/or other factors that are beyond T-Systems' control, T-Systems 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 subscriber receives an e-mail notifying them that their certificate has been revoked. This e-mail also informs them of the precise revocation time.

Certificates are managed in the revocation list for at least a 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.

4.10 Certificate status services

4.10.1 Operational characteristics

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 without its owner's explicit permission and cannot be downloaded from the LDAP server.

The interface specification for the LDAP server is available on TeleSec's PKS web pages.

4.10.2 Service availability

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 shown below http://pks.telesec.de/ocspr.

The interface specification for this service is available on TeleSec's PKS web pages.

No OCSP information is provided for non-qualified certificates.

4.10.3 Optional features

Revoked, non-qualified certificates are included in the revocation list (CRL) which is updated regularly at least once every 6 hours.
The inclusion of a certificate in the revocation list is regarded as confirmation that revocation completed successfully. The revocation list for advanced certificates can be retrieved at any time from the LDAP server at ldap://pks-ldap.telesec.de/o=T-Systems International GmbH,c=de

The technical specification for the revocation list is available on TeleSec's PKS web pages.

4.11 End of subscription

The storage and restoration of keys was not offered.

5 Facility, management, and operational controls

The T-Systems Trust Center is housed in a specially protected building and operated by knowledgeable staff. All processes for requesting and generating certificates of the certification authorities operated there are defined in detail. All technical security measures are documented.
The facility, management, and operational controls applied are defined in a security concept based on IT baseline protection (in German "IT-Grundschutz"), with their effectiveness being demonstrated 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, i.e., there are stipulations regarding

- Risk assessment in the framework of ISMS
- Information security guidelines
- Asset management

.

5.1 Physical controls

Signature cards are produced in T-Systems' Trust Center. The Trust Center is authorized as a certification authority and has been eIDAS-compliant since July 1, 2016 and thus fulfills very strict requirements concerning physical security. 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 Site location and construction

T-Systems operates a Trust Center, which has two fully redundant parts, two separate energy wings (electrical, air conditioning, water) with a property management system and emergency power supplies.
The Trust Center is set up and operated in observance of the relevant guidelines 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 protection, smoke protection and blocking of attacks. The Trust Center is accepted by 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 access regulations that regulate 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 protected by a computer-controlled access control system. Guests are only received in exceptional cases and subject to prior notification. Particular security requirements apply here.

5.1.3 Power and air conditioning

The suction intakes for outside air are arranged 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 fresh air openings are access-protected. Filters are fitted to ensure protection against air contamination due to airborne particles. The fresh air intake is continuously checked for aggressive gases. In the event of an emergency (e.g., fire in the environment), the fresh air intake is automatically closed by means of air flaps.
An independent AC power supply in accordance with VDE regulations is installed to protect the power supply against power outages. It offers protection against voltage fluctuations, uninterruptible short-term bridging and long-term bridging using two separate stationary emergency generators having an output equal to the data centers full load.

5.1.4 Water exposures

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 and protection

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 closing devices. By agreement with the fire department, water is only used for firefighting purposes in extreme emergency situations.
Fire compartments are made secure by fire-resistant components. Openings through fire protection walls are fitted with fire doors that close automatically
In areas with double floors as well as suspended ceilings the fire protection walls extend right through to the ceilings/floors of the storey.
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 fitted in the other rooms.

5.1.6 Media storage

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).

5.1.7 Waste 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. Cryptographic equipment is physically destroyed in accordance with the manufacturer's guidelines before being disposed of. Other waste is disposed of in accordance with T-Systems' regular disposal guidelines.

5.1.8 Off-site backup

T-Systems takes routine backups of critical system data, audit log data, and other confidential information. Backup copies are stored physically separately from original data.

5.2 Procedural controls

These organizational measures are set out in the Public Key Service's security concept which is not publicly available. The security concept and the measures described therein 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 safeguard security:

- Measured to determine, assess, and regularly review residual risks are included in the Public Key Service's security concept.
- The provisions for integrating external service providers originate from specifications in the actual laws and was implemented in contracts so that the implementation of 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 protection and security policies of the Deutsche Telekom AG Group.
- 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 service.
- All security-relevant processes are documented and tested in the security concept.

5.2.1 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, a project is examined in terms of the security aspects that it must meet.
Importance is attached to trustworthy manufacturers when choosing external software. Open source components are used in departments where this is possible. In the case of software that has to be specially developed for the Trust Center, the manufacturer must store the source code in the Trust Center after project completion.

5.3 Procedural controls

The organizational measures are set out in the security concept and are implemented on the basis of the Trust Center's operations plan. The relevant requirements under ETSI EN 319 401 Section 7.4 b, c, d and e are implemented.

5.3.1 Trusted roles

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

- The validation of information in certificate orders
- The acceptance, rejection, or other processing of certificate requests, revocation requests or renewal requests
- The granting or withdrawal of certificates, including personnel who have data access and physical access to database systems
- The way informational orders are dealt with by end subscribers

Trusted persons are in particular:

- Trust Center staff (e.g., system administration)
- Employees of cryptography departments
- Security personnel
- Responsible technical staff and
- managerial staff responsible for managing the trusted infrastructure.

The above-mentioned trustworthy persons must meet the requirements set out in this CPS (see Section 5.4.1).

The Change Advisory Board of the T-Systems Trust Center is responsible for initiating, performing and controlling the methods, processes and procedures that are described in the security concepts in the CP/CPS of the certification authorities operated by the T-Systems Trust Center.

5.3.2 Number of persons required per task

The operational maintenance of the certification authority and the directory service (administration, backup, restoration) is carried out by knowledgeable and trusted staff.
Working on highly sensitive components (e.g., key creation system, HSM) is regulated by special in-house control procedures and is carried out by at least two employees.

5.3.3 Identification and authentication for each role

T-Systems employees who are classed as especially trusted and who carry out especially trusted activities are subject to a T-Systems internal security check (see Section 5.4.2).
T-Systems ensures that employees have achieved a trusted status and the department has given its approval before these employees:

- Are given access devices and access to the required facilities,
- Are given authorization to access systems of the certification authority and other IT systems,
- Are allowed to perform certain tasks in connection with the systems.

After positive vetting, Trust Center employees are formally appointed by the Trust Center Manager.

5.3.4 Roles requiring separation of duties

The following roles require a separation of duties and are therefore supported by different employees:

- Order entry and certificate of approval
- Backing up and restoring of databases and HSMs,
- Generation of qualified certificates,
- Key life-cycle management of CA and root CA certificates.

5.4 Personnel controls

T-Systems implements a comprehensive range of personnel-related security measures that ensure a high level of protection for their facilities and certification services. The use of qualified trained personnel 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.

5.4.1 Qualifications, experience, and clearance requirements

Employees who are to assume a trusted role are required by T-Systems to prove that they have the qualifications and experience necessary to fulfill their prospective work obligations in a competent and satisfactory manner.
A new certificate of good conduct must be submitted to T-Systems at regular intervals.

5.4.2 Background check procedures

Before employment is taken up in a trustworthy role, T-Systems carries out security checks that involve the following:

- Reviewing and confirming the recruit's previous employment relationship,
- Examining their employment references,
- Confirming their highest or most relevant school-leaving/professional qualification,
- Police certificate of good conduct.

If the requirements stipulated in this section cannot be met, T-Systems instead makes use of a legally permitted investigation method that essentially produces the same information.
Examples of results of security checks that can result in a candidate being rejected as a trusted person include

- The candidate or trusted person providing false details,
- Particularly negative or unreliable professional references, and
- certain previous convictions.

Reports that contain such information are assessed by HR Department employees and security personnel who decide the appropriate subsequent course of action. The subsequent course of action can result in measures such as withdrawing offers of employment made to candidates applying for trustworthy positions and include the dismissal of trustworthy persons.
The use of information obtained during the course of security checks in order to take such measures is subject to applicable law.

5.4.3 Training requirements

T-Systems Trust Center personnel participate in advanced training measures that are required in order for them to fulfill their professional duties competently and satisfactorily. T-Systems documents these training measures. Training programs are aligned with individual activity areas and include, among other aspects:

- Advanced PKI knowledge,
- Procedures in accordance with ITIL,
- Data protection,
- Data secrecy and telecommunications secrecy,
- Information protection,
- Access protection,
- Anti-corruption,
- T-Systems security and operating policies and procedures,
- Use and operation of hardware and software used,
- Reporting and dealing with incidents and compromised security and
- Procedures for repairing damage in emergencies (Disaster Recovery) and Business Continuity.

Employees who deal with the validation of certificate orders receive additional training on the following topics:

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

5.4.4 Retraining frequency and requirements

T-Systems staff attend refresher courses and further training courses to the necessary extent and at the required intervals.

5.4.5 Job rotation frequency and sequence

Not applicable.

5.4.6 Sanctions for unauthorized actions

T-Systems reserves the right to punish unauthorized activities or other violations of this CPS and the procedures resulting therefrom and to take appropriate disciplinary measures. Such disciplinary action may involve measures up to and including dismissal and depend on the frequency and seriousness of said unauthorized activities.

5.4.7 Independent contractor requirements

T-Systems reserves the right to appoint independent contractors or consultants to trusted positions. These individuals are subject to the same functional and security criteria as T-Systems employees working in a comparable job.
The above group of people who have not yet concluded or successfully completed the security screening described in Section 5.4.2 will only be granted access to T-Systems' secure facilities provided they are always accompanied by trustworthy persons and are closely supervised.

5.4.8 Documentation supplied to personnel

T-Systems provides its employees with all the requisite documents (training documents, procedural instructions) that they need in order to be able to fulfill their professional duties appropriately.

5.5 Records archival

Changes in the life cycle of certificate (CA and end user) are logged. In detail, this relates to the following events:

- Generation
- Backup
- Save
- Restoration
- Destruction
- Modifications to hardware and software
- Logs of events in the life cycle of CA certificates:
- Certificate order (successful/failed processing and enclosed documents)
- Certificate renewal
- Certificate revocation
- Generation of certificates
- Revocation lists
- Logging of internal and external audits.

5.6 Backup of records

All records in the T-Systems Trust Center according to certificates under German Digital Signature Act are kept for 30 years in accordance with the requirements of the German Digital Signature Act. Other records are kept for ten (10) years.

5.7 Key changeover

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.

5.8 CA or RA termination

The affected CA certificates are immediately revoked when such keys are compromised. User certificates issued by these certificates are also revoked. The affected subscribers are informed of revocation.

5.9 Cessation of operations

5.9.1 Certification service provider in accordance with eIDAS

If the certification service ceases operations, the certification authority proceeds in accordance with the requirements in ETSI EN 319 401 Section 7.12 and has to draw up a termination plan for this.

All possible measures will be taken prior to cessation of the service in order to minimize the potential damage for all concerned and to ensure that all those involved 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.

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

5.9.2 Non-qualified certificates

Termination of operations may only be invoked by the T-Systems Board of Management.
A termination plan may include the following regulations:

- Continuation of the revocation service
- Revocation of issued CA certificates
- Any transition 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.

6 Technical security controls

6.1 Key pair generation and installation

All key pairs for end-user certificates are generated in a closed-off protected space that has no connection to any external network, on a security-tested hardware component or on the actual subscriber's signature card which is certified for qualified signature creation units in accordance with eIDAS (QSCD). After they are generated, keys are securely stored on the chip card. A private key can no longer be read out once it has been stored. Key generation (preproduction) and the generation and storage of an end-user's certificate take place in separate production steps.

The requirements in the algorithm catalog which is updated annually by the Federal Network Agency and Federal Office for Information Security (BSI) apply to key generation and the use of keys.

6.1.1 Private key protection and cryptographic module engineering controls

Security-tested hardware is used as a key carrier for CA certificates. This hardware is, for instance, certified in accordance with eIDAS QSCD or FIPS-140-2 or similarly certified.

6.2 Key pair generation

CA certificates are generated on an off-line system that has no network connections, adopting the dual-control principle.
Key backups are, providing the hardware used on the CA key supports this, only taken using the dual-control principle. 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.
Anyone interested can register to receive the newsletter by sending an e-mail to PKS-Support@t-systems.com.
Shortly before a CA or service certificate expires, it is replaced by a newly generated certificate. CA or server certificates that are no longer needed (as in the case of non-qualified CA certificates and any existing backups of private keys) are made unusable by destroying the chip card on which they are stored.

6.3 Other aspects of key pair management

Only systems that are designed for use in data centers are used in the T-Systems 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 regularly checked 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 respond 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 protected in a manner that makes it possible to detect retrospective changes.

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

6.3.1 Data backup

All important certification service data is backed up regularly. The usability of data backups is tested 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.

6.3.2 Certificate operational periods and key pair usage periods

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 access restrictions of the system usage is supported by a strict password policy.

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

6.3.3 Use of security-tested components

The German Digital Signature Act and the eIDAS Regulation require 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 chip cards used to generate and store private keys are evaluated in accordance with Common Criteria EAL4+ and are approved as a qualified signature creation unit in accordance with the eIDAS Regulation.

6.4 Network security measures

All the network 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.

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

Communication between the Trust Center's various sites takes place using encrypted VPN connections. Session keys, which are regularly changed, are used for VPN connections. Encryption equipment only accepts connections from other encryption equipment that is included in its own White List.

Network components' settings are regularly audited by a conformity assessment body in accordance with eIDAS.

7 Certificate, CRL, and OCSP profiles

7.1 Certificate profile

The specification for the certificate profile for qualified signatures and attribute certificates 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 CRL profile

The specification for the revocation list (CRL) is available on the TeleSec PKS website
https://www.telesec.de/signaturkarte/→ Support → Download area → Technical documentation

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 audit and other assessments

The certification service is compliant with the ETSI standards listed in Section **Fehler! Verweisquelle konnte nicht gefunden werden.** . In order to check this 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 documentation (security concept, operating concept and other internal documents), the implementation of processes and compliance with relevant provisions are inspected.

8.1 Frequency or circumstances of assessment

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

8.2 Identity/qualifications of the assessor

Trust Center-specific compliance audits are performed by qualified employees of T-Systems or a third party (e.g., qualified companies such as TÜV IT) that can demonstrate the necessary experience in the areas of Public Key Infrastructure technology, security auditing and information security procedures and tools.

8.3 Assessor's relationship to assessed entity

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

Self-assessments (quality assessments) are carried out by suitably qualified T-Systems staff.

8.4 Topics covered by assessment

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

- Identity verification of end subscribers
- Procedure for placing certificate orders
- Processing of certificate orders
- Certificate renewal
- Certificate revocations
- Access protection
- Authorization and role concept

- Anti-intruder measures
- Staff

In any event, auditing is carried out in accordance with the applicable versions of the audit criteria of the ETSI standards listed in Section **Fehler! Verweisquelle konnte nicht gefunden werden.**.

The T-Systems Trust Center carries out an annual risk assessment.

This review covers at least the following aspects:

- Identifying foreseeable potential external and external risks (i.e., especially their underlying vulnerabilities) which might lead to
    - Unauthorized access to relevant data or systems,
    - Disclosure or misuse of relevant data,
    - Changes to or destruction of relevant data,
    - Impairment, disruption, or failure of all or part of the certificate administration process

    .
- Assessing the likelihood of occurrence and the resulting potential damage (i.e., level of damage) caused by someone exploiting a vulnerability. In doing so, the special protection requirements of certificate data and the certificate management process must be taken into account.
- Assessing the effectiveness and adequacy of the countermeasures taken (e.g., policies, procedures, security systems used, technologies, insurance) to eliminate the potential threat or mitigate risk.

Based on this risk assessment, the T-Systems Trust Center has developed a security plan that is regularly reviewed and adapted as needed. This security plan consists of procedures, measures and products used to aid the evaluation and management of risks that are identified during the risk assessment. The security plan contains administrative, organizational, technical, and physical security measures commensurate with the sensitivity of the data and certificate management process in question.

8.5 Actions taken as a result of deficiency

If defects or mistakes are detected in the case of an operator of a certification authority during a compliance audit or by an auditor, a decision is made regarding the particular corrective measures that must be taken. The Trust Center Manager decides, together with the auditor, on suitable measures and their implementation within an economically reasonable period. In the event of serious security-critical defects, a correction plan must be developed within 10 days and the deviation must be rectified. In the event of less serious deficits, the Trust Center Manager will decide on the rectification time frame.

8.6 Communication of results

The results of audits are documented in a report that is drawn up by the auditor and handed over to T-Systems.

T-Systems reserves the right to publish results or partial results if there has been any misuse or if T-Systems has suffered reputational damage.

9 Other business and legal matters

9.1 Fees

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

9.2 Financial responsibility

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

9.2.1 Insurance coverage

T-Systems has public liability insurance and directors' and officers' liability insurance cover. Steps are taken to ensure that the insurance cover requirements are met.

9.2.2 Other assets

Not applicable.

9.2.3 Insurance or warranty coverage for end-entities

Not applicable.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Confidential information is any information from parties involved in PKIs (see Section **Fehler! Verweisquelle konnte nicht gefunden werden.**) that has not been published or has not been explicitly approved for publication and which is not covered by Section 9.3.2 .

9.3.2 Information not within the scope of confidential information

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

9.3.3 Responsibility to protect confidential information

T-Systems, as a certification authority, is responsible for the protection of confidential information and compliance with data protection provisions.
Furthermore, in taking on tasks within the framework of approval and attribute confirmation, chamber employees are also obliged to handle confidential information accordingly, see Section **Fehler! Verweisquelle konnte nicht gefunden werden.**.

9.4 Privacy of personal information

9.4.1 Privacy plan

T-Systems has to electronically store and process personal data in order to provide this service. T-Systems ensures the technical and organizational security precautions and measures in accordance with § 9 German Federal Data Protection Act (BDSG) and the appendix to § 9 BDSG.
A data protection concept has been drawn up in accordance with Group regulations. This data protection concept summarizes the data protection-relevant aspects of the PKI service.
Excerpts of the data protection concept can be supplied upon request.

9.4.2 Information treated as private

For personal data, the provisions analogous to Section 9.3.1apply.

9.4.3 Information not deemed to private

For personal data, the provisions analogous to Section 9.3.2apply.

9.4.4 Responsibility to protect private information

For personal data, the provisions analogous to Section 9.3.3apply.

9.4.5 Notice and consent to use private information

The applicant consents to the use of personal data by the certification authority or the responsible practice, 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 9.4.3 may be published.

9.4.6 Disclosure pursuant to judicial or administrative process

The obligation to maintain secrecy in respect of confidential information or personal data does not apply where disclosure is ordered by law or by a court decision or by an administrative authority or is used to implement legal judgments. As soon as there are pointers to the introduction of court or official proceedings that could lead to disclosure of confidential or private information, the party involved in the proceedings shall notify the other party in compliance with the legal provisions.

9.4.7 Other information disclosure circumstances

No provisions.

9.5 Intellectual property rights

9.6 Representations and warranties

Despite the utmost care taken while creating this documentation, Deutsche Telekom AG or T-Systems International GmbH are unable to exclude that possibility that the policies described herein may contain any errors. Deutsche Telekom AG as well as T-Systems International GmbH exclude any liability in this case.

There is no statutory right to have the TeleSec Public Key Service issue a certificate.

9.7 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 web page at any time
https://www.telesec.de/signaturkarte/→ Support → Download area → General Terms and Conditions and prices

9.8 Indemnities

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 web page at any time
https://www.telesec.de/signaturkarte/→ Support → Download area → General Terms and Conditions and prices

9.9 Term and termination

Deadlines, dates and notices of termination are regulated in the General Terms and Conditions (GT&C) for the TeleSec Public Key Service, these are available from the following web page at any time
https://www.telesec.de/signaturkarte/ → Support → Download area → General Terms and Conditions and prices

9.10 CPS amendments

In order to respond to changing market requirements, security requirements and legislation etc., T-Systems International GmbH reserves the right to amend or adapt this CPS. Amendments to the CPS are announced on the web page (https://www.telesec.de/pks) and apply from the moment the CPS enters into force. The CPS enters into force two weeks after publication of the amendments, unless publication makes provision for a different period.
Any claims beyond this for individual end users to be notified are explicitly excluded.

T-Systems reviews the current CPS at least once a year. Certificate recipients, relying parties or other persons or organizations involved in the PKS can submit their comments regarding the content of the CPS to T-Systems. T-Systems retains the authority to make decisions regarding amendments to the CPS.

Amendments to this CPS are made by Trust Center employees. After amendments have been made, the document is submitted to the Trust Center's Change Advisory Board which includes, among other members, the Trust Center Manager. The Change Advisory Board examines the amendment and releases the CPS for publication.

Amendments to the CPS that only rectify spelling mistakes or are of an editorial nature come into force without any prior announcement.

A new version number and date is created for every amendment to the CPS.

9.11 Governing law

Generally speaking, the German Digital Signature Act and the eIDAS Regulation regulate the issue of qualified certificates. The law of the Federal Republic of Germany shall apply. The place of performance and the exclusive place of jurisdiction is Frankfurt/Main, Germany.

9.12 Other regulations

9.12.1 CPS

All certificates, in the context of the PKS, are issued in accordance with the latest applicable version of the CPS at the time of issue. The current version of this CPS can be downloaded at any time from the URL http://pks.telesec.de/cps/cps.pdf.

9.12.2 Up-to-dateness of certificate data

The data needed for the service is verified at the time of registration. No assurance can be given regarding the subsequent up-to-dateness of this data. Data is, nevertheless, verified again at the time of re-certification.

9.12.3 Complaints and escalation

9.12.3.1 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 the other affected party in order to attempt to resolve the dispute amicably.

9.12.3.2 Escalation

If the dispute cannot be resolved within ten (10) days after preliminary notification in accordance with CPS § 9.12.3.1, a party to the dispute may refer the matter, in writing or electronically, to T-Systems and request auditing.

T-Systems then convenes a body comprised of PKI experts in order to gather the relevant facts with a view to resolving 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 e-mail, teleconferences, couriers and mail during the course of its work. The body's recommendations are not binding on the parties. This procedure does not exclude legal recourse.