Certification Practice Statement for the T-Systems Trust Center Public Key Infrastructure of the T-TeleSec GlobalRoot Class 3

Certification Practice Statement, CPS

Version: 6.0

Last revision: 01.05.2017

Status: final

Publication details

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

File name	Document number	Document name
CPS_T-TeleSec_GlobalRoot_Class_3_V6.0_EN_freigegeben.docx	1.3.6.1.4.1.7879.13.24	Certification Practice Statement, CPS

Version	Last revised	Status
6.0	01.05.2017	final

Author	Contents reviewed by	Approved by
T-Systems International GmbH Telekom Security Trust Center Services	M. Burkard	M. Etrich

Contact	Phone	E-mail
Service desk	Phone: +49 1805 268 204	telesec_support@t-systems.com

Brief info
Certification Practice Statement for the T-Systems Trust Center Public Key Infrastructure of the T-TeleSec GlobalRoot Class 3

Change history

Version	Last revised	Edited by	Changes/comments
0.1	Feb. 8, 2007	L. Eickholt	Initial version – draft
0.3	Feb. 13, 2007	L. Eickholt	Content updates - Draft
0.7	Mar. 19, 2007	M. Ulm, M. Graf, W. Pietrus	Content updates – Draft, corrections
0.9	Mar. 30, 2007	L. Eickholt	Content updates
0.95	Jul. 4, 2007	M. Ulm, L. Eickholt	Content updates
1.0	Aug. 15, 2007	L. Eickholt	Content update
1.1	Sept. 14, 2007	L.Eickholt, M. Ulm	Section 3.1.3 updated, 3.2.4 Term “end subscriber” deleted, Section 4.12 expanded, 5.4.1 Term “end subscriber” deleted, 6.3.1 Term “end subscriber” deleted, Section 6.2 updated, Section 4.6 expanded, Section 4.3.2 updated, Section 4.9.3 updated, Section 5.8 updated, Section 8 revised completely, Section 9.5 expanded, Section 9.9 changed into Section 9.12, 9.12.1 and 9.12.2 added, Section 9.13 added, Section 9.14 updated
1.2	Aug. 31, 2010	L.Eickholt, S.Kölsch, H.Gügel	Section 1 updated, Section 1.2 updated, Section 1.3.1 updated, Section 1.3.2.1 added, Section 1.3.3.1 added, Section 1.4.1.2 updated, Section 1.4.2 added, Section 1.5.1 updated, Section 1.5.2 updated, Section 2.1 updated, Section 2.2 updated, Section 3.1.3 updated, Section 3.4 updated, Section 4.1.1 updated, Section 4.1.2.1 added, Section 4.2.1 updated, Section 4.9.1 updated and expanded, Section 4.9.8 updated, Section 4.9.9 and 4.9.10 expanded, Section 4.9.14 to 4.9.16 added, Section 4.10 updated, Section 6 updated, Section 6.1.3 updated, Section 6.1.7 updated, Section 6.2 updated, Section 6.3.2 updated, Section 7.1.1.1 updated, Section 7.2.1 expanded and updated, Section 8 expanded, Section 8.1 rounded off, Section 9.1 updated, Section (Financial responsibilities, former 9.2) removed, Section (Disclaimer, former 9.5) removed, Section (Liability limitations) updated, Section 9.10 updated, Glossary updated
1.3	Mar. 8, 2012	L. Eickholt, C. Dahlenkamp	Section 1.4.1.3 updated, Section 1.4.2 updated, Section 4.9.9 updated, Glossary updated
1.3.1	May 24, 2012	L. Eickholt, C. Dahlenkamp	Clarification: External Sub-CAs are not permitted Update Section 1.3.1,1.3.3,1.4.1.3 and 4.1.2.1 Section 1.3.2.1 and 1.3.3.1 deleted
1.4	Jul. 1, 2012	L. Eickholt, C. Dahlenkamp	Requirements from Version 1.0 of the CA/Browser Forum baseline requirements incorporated
2.0	Jun. 17, 2013	L. Eickholt, B. Nakonzer	Adjustments according to the annual document review
2.1	May 23, 2014	B. Nakonzer	Wild card certificates adopted
3.1	25-Mar-15	B. Nakonzer	Changes following review
4.1	15-Mar-16	B. Nakonzer	Revision 2016
5.1	Apr. 5, 2017	B. Nakonzer	Section 6.3.2, 7.1, 7.1.3, 8.4 updated
5.2	May 23,.2017	A.Roth	Formal control

6.0	May 24, 2017	A.Roth	approval

Table of contents

List of figures

List of tables

1 Introduction

The Trust Center is operated by the Group unit T-Systems International GmbH (hereinafter referred to as "T-Systems"). Hereinafter referred to as **"T-Systems Trust Center"**.
The T-Systems Trust Center operates a number of different certification authorities under different root certification authorities (Root CA). The certification authorities of the certificate services differ with regard to application contexts for certificates, specific designs of the technical interfaces, registration procedures, certificate profiles, processes for revocations/suspensions as well as for the publication of information.
Both the structural and the organizational infrastructure meet the strict requirements of the German Digital Signature Act. Since starting operation, the T-Systems Trust Center has issued more than 4.6 million certificates. The services offered by the Trust Center also include the TeleSec Public Key Service (PKS) which covers the process of issuing signature certificates in accordance with eIDAS.

1.1 Overview

This document is the Certification Practice Statement (CPS) for the PKI of the "T-TeleSec GlobalRoot Class 3" root certification authority (Root CA) that is operated at the T-Systems Trust Center.
This CPS describes the security level required for operating the PKI, see Section 3.2 and includes security instructions as well as explanations of technical, organizational and legal aspects. This CPS can further supplement, specify and fine-tune the rules of the CP but not contradict these rules or reduce their quality or effectiveness.
This document is based on the international standard for certification policies RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework) of the Internet Society.

The CPS covers the following aspects in detail:

- Publications and directory service
- Identification and authentication of PKI subscribers
- Issue of certificates
- Renewal of certificates (re-certification)
- Revocation and suspension of certificates
- Structural and organizational security measures
- Technical security measures
- Certificate profiles
- Auditing
- Various general conditions.

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

The T-Systems Trust Center ensures that the root certification authority (Root CA) "T-TeleSec GlobalRoot Class 3" and all subordinate sub-CAs comply with and fulfill the requirements and regulations of the published [CAB-BR] as amended (http://www.cabforum.org/documents.html). In the event that this document and the [CAB-BR] contradict one another, the regulations from the [CAB-BR] have priority.

Subordinated sub-CAs must document a content-equivalent assurance in their respective CP or CPS as long as they issue TLS/SSL certificates.

1.2 Document identification

Name:	Zertifizierungserklärung für die T-Systems Trust Center Public Key Infrastruktur der Root-CA "T-TeleSec GlobalRoot Class 3"
Version:	6.0
Date	01.05.2017
Object identifier	1.3.6.1.4.1.7879.13.24

1.3 Parties involved in PKIs

1.3.1 Certification authorities

The T-Systems Trust Center operates the “T-TeleSec GlobalRoot Class 3” root CA for certification services. T-Systems issues solely certificates for subordinate certification authorities (Sub-CA). Issuing certificates for external, subordinate certification authorities (Sub-CA) is not permitted under this root certification authority (Root CA).
The certificate of the root certification authority (Root CA) is a self-signed certificate and is published by T-Systems. The publication makes it possible to check the validity of all certificates issued in this hierarchy. The root certification authorities (Root CA) only certifies certificates from direct subordinate certification authorities. The structure is schematically represented in the diagram below:

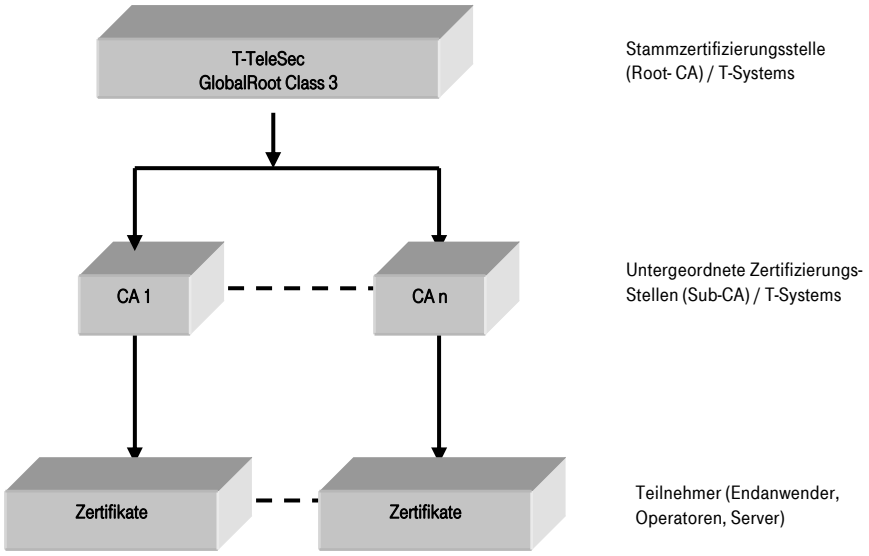

Figure 1: Certification authorities under the "T-TeleSec GlobalRoot Class 3" root CA.

Each subordinate certification authority (Sub-CA) has one or more CAs and service certificates issued by the relevant root certification authority (Root CA) that are re-issued at regular intervals.
All certification authorities shown above are operated by T-Systems and governed by the "T-TeleSec-GlobalRoot-CP".

1.3.2 Registration authorities

The "T-TeleSec GlobalRoot Class 3" certification authority operates only one central registration authority.

1.3.3 Certificate holder

Depending on the certification authority, certificates may be issued to natural or legal persons.
The certificate holder

- requests the certificate (represented by a natural person in the case of legal persons),
- is authenticated by the registration authority and identified by the certificate, and
- owns the private key that belongs to the public key in the certificate.

1.3.4 Certificate users

Certificate users are all natural or legal persons or organizational units that use certificates of certificate holders in the context of applications.

1.3.5 Other subscribers

Subscribers who have not entered into an obligation vis-à-vis T-TeleSec GlobalRoot Class 3 are not looked at in the policy.

1.4 Certificate usage

1.4.1 Permitted usage of certificates

1.4.1.1 Use for natural persons

Certificates are used for authentication purposes, digital signature as well as encryption as part of various applications depending on the assignment of the attributes on key usage and the CPS definitions of the relevant certification authority. Some examples include:

- Authentication as part of communication protocols (e.g., SSL, IPSec, S/MIME, XML SIG, SOAP),
- Authentication as part of processes (Windows logon),
- Encryption as part of communication protocols (e.g., SSL, IPSec, S/MIME, XML ENC, SOAP),
- Hard disk encryption.

Security level	Use		
	Signature	Encryption	Client authentication
High	✓	✓	✓

Table :1 Use for natural persons

The security level is described in Section 3.2.

1.4.1.2 Use for organizations

The legal existence of an organization must be ensured and the organization's features to be included in the certificate must also be checked (such as: domain name).
Table 2 illustrates the most common uses for organizational certificates, but it is also possible to implement other options.

Security level	Use			
	Code/content Signing	SSL (extended validation) secure SSL/TLS Internet sessions	Client authentication	Signature and encryption
High	✓	✓	✓	✓

Table 2: Use for organizations

The security level is described in Section 3.2.

1.4.1.3 Certificates in case of CA concatenation

T-Systems does not issue any sub-CA certificates that allow their use in a MitM scenario (also known as "transparent traffic management") for domains or IP addresses, which the subscriber does not legally own or control.

1.4.2 Prohibited usage of certificates

Certificates are not intended, designed or permitted for use or forwarding
for

- Management and control facilities in dangerous environments
- Environments in which fail-safe operation is required (e.g., operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems or weapon control systems) and where failure could lead to damage (e.g., personal injury, death, medium and serious environmental damage, other disasters)

It is also not permitted to use an sub-CA certificate that has been issued for a MitM scenario as described in Section 1.4.1.3.

1.5 Policy administration

1.5.1 Responsibility for the policy

This document (CP/CPS) is published by T-Systems International GmbH, ICTO-SDM CSS & Special Services– PSS-Security Solutions- Trust Center Services.

1.5.2 Contactdetails

Address:
T-Systems International GmbH
Telekom Security
Trust Center Services
Untere Industriestraße 20
57250 Netphen
Germany

Tel: +49 (0) 1805 268 204 (landlines: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute)
E-mail: telesec_support@t-systems.com
Fax: +49 (0) 2151 36607972
WWW: http://www.telesec.de

1.5.3 Policy maintenance

This CPS remains valid unless it is revoked by the responsible authority (see Section 1.5.1). It is updated where required and will then be assigned a new ascending version number.

1.5.4 Approval procedure of this document (CP/CPS)

The publisher named in Section 1.5.1 is responsible for this document (CP/CPS). The approval is given by the Change Advisory Board.

The CP/CPS to hand is subject to an annual review independently of additional changes. The department named in Section 1.5.3 is responsible for carrying out or coordinating the review.
The annual review must be noted in the change history of the CP/CPS. This shall also apply even if no changes are made to contents.

1.6 Definitions and Abbreviations

See Section 10 (glossary).

2 Publication and responsibilities for the directory service

2.1 Directory service

The T-Systems Trust Center provides the PKI certificate users on the Internet with a publicly and internationally available ARL (24/7).

LDAP:
ldap://pki.telesec.de/CN=T-TeleSec%20GlobalRoot%20Class%203,OU=T-Systems%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?AuthorityRevocationList

WWW/HTTP:
http://pki.telesec.de/rl/GlobalRoot_Class_3.crl

2.2 Publication of certificate information

The T-Systems Trust Center provides the certificate users of the PKI with the following information:

- the root CA certificate and its fingerprint (MD5 and SHA1),
- documentation on the change of a root CA or a CA certificate,
- information on a compromise or suspected compromise or revocation of a root CA or a CA certificate
- CPS in the released status.

The Internet pages can be found at http://www.telesec.de/pki/index.html.

2.3 Publication frequency

Revocation information for root CA and CA certificates is updated without delay in the event of a revocation (CRL, Repository for OCSP requests). The CPS and any additional information is provided on the Internet pages.

2.4 Access to the information services

Read access to the information listed in Section 2.1 and 2.2 is not subject to access control for certificate holders and certificate users of a certification authority.
Write access to all information listed in Section 2.1 and 2.2 is only used by authorized employees or systems.

3 Identification and authentication

3.1 Naming conventions

A Distinguished Name (DN) is a unique, global name for directory objects according to the X.500 standard. Distinguished Names allow people and systems to be clearly distinguished worldwide. The DN ensures that a digital certificate is never issued with the same name for different people.

3.1.1 Name format

The naming conventions for the “SubjectDistinguishedName” (Subject DN) and “IssuerDistinguishedName” (Issuer DN) must be defined in accordance with the X.501 standard. The requirements for using name attributes in the Subject DN and Subject Alternative Name depend on the individual application context of a certification authority. For example, the e-mail address of the certificate holder must be recorded for certificates that are used for secure e-mail communication. As a rule, the Subject DN should contain the “Common Name” (CN) attribute. The Issuer DN must contain the “Common Name” (CN) attribute. Certificates with wild card FQDN are permitted. That does not apply to certificates with the EV feature (Extended Validation Certificate). Confusing or ambiguous information is not permitted.
The conventions for the elements of the Subject DN should be described in the CP/CPS of the downstream services.

3.1.2 Meaningful names

The name in the "SubjectDistinguishedName" and in the "SubjectAlternativeName" must always clearly identify the certificate holder. Abbreviations of, for example, the name entered in the commercial register are permitted due to the limit on the number of characters. The abbreviation used must not be misleading.

3.1.3 Pseudonymity/anonymity

If certificates are created with pseudonyms, the certification authority must record the real identity of the certificate holder in its documentation.
It is also possible to issue an anonymous certificate if explicitly requested by the applicant. In this case, the applicant may select a pseudonym that will be included in the certificate, whereby pseudonyms are marked with the suffix “:PN”. If the same pseudonym exists more than once, it will be rendered 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 which suggest authorizations that the certificate owner does not have).

The certification authority transmits the identity of a signature key owner, encryption key owner and authentication key owner with pseudonym to the responsible areas if this is required 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.

3.1.4 Rules on the interpretation of different name formats

Assignment for the name fields must comply with the X.501 standard.

3.1.5 Uniqueness of names

The names of root CA and CA certificates that are issued by the T-Systems Trust Center must be unique.

3.1.6 Recognition, authentication and role of brand names

It is the responsibility of the certificate holder that the choice of name does not infringe upon any trademarks, trademark rights, etc. The certification authority is not obligated to check such rights.
Only the certificate holder himself is responsible for these checks. If a certification authority is notified of a violation of such rights, the certificate will be revoked.

3.2 Identity checks for new orders with high security level

The requested security level must be ensured at every point of the trust chain. A requested security level may become stronger in the trust hierarchy, but must not become weaker at any level.

3.2.1 Methods for checking the owner of the private key

In the event of a new order, the certificate holder must prove to the certification authority in a suitable manner that he owns the private key that is mapped to the public key to be certified. Proof of ownership is provided by the PKCS#10 method. This requirement does not apply where the key is generated at the certification authority.

3.2.2 Authentication of an organization

The basic requirement for commissioning a certification authority is the conclusion of a contract. This contractual relationship is generated by T-Systems sales units with legal help.
The following validation procedures apply in relation to the authentication of organizations:

- Ascertaining that the organization exists
- Verifying the company name and the business address

To carry out the validation process, the CA or the RA use the organization documents issued by a public body or authority.
The authentication of organizations is subject to requirements that correspond to the security level.

3.2.3 Authentication of a natural person

The authentication of natural persons is subject to the following requirements:
High security level
The following validation procedures must be carried out to identify a natural person who requests services with a high security level:

- Ascertaining that the natural person exists based on identification features that can be verified.

- Personal appointment at a CA or RA with an officially issued passport document with photo.

In order to verify such identification features, the CA or RA can access an identity verification service recognized by T-Systems or an identity verification database of a third party. or the organization documents issued by a public body or authority.

3.2.4 Unverified subscriber information

All information to be included in a certificate must be verified.

3.2.5 Authorization check

The authorization of a natural person as being entitled to act on behalf of an organization or a natural person is ensured by the conclusion of the contract and the prior mapping of responsibilities linked to this process.
It must be checked whether the customer has the right to use the domain or IP address. Checks will not be made on CAA entries in the DNS.

3.2.6 Criteria for interoperability

If a sub-CA uses a policy OID that represents fulfillment of and compliance with the [CAB-BR] in a certificate that it has issued, the corresponding CP or CPS of the sub-CA must contain an explicit assurance that all certificates issued by the sub-CA that contain this policy OID correspond to and comply with the specifications issued by the [CAB-BR].

3.3 Identity check and authentication in the event of re-certification

For re-certification, the identity check on new orders (see Section 3.2) must be carried out.

3.4 Identification and authentication for revocation orders

The T-Systems Trust Center offers a central revocation service so that the internal certificate can be revoked in the event of loss or suspicion of misuse. If revoked, the certificate is included in a revocation list. Persons and institutions authorized for revocations (see Section 4.9) may request a certificate to be revoked by e-mail or telephone.
A revocation is authenticated by entering the basic data (name, company, call-back number, e-mail address).
The revocation request is authorized by providing the revocation password.
The following input channels should be used for the revocation:
Telephone: +49 (0) 1805-268204 (landline 0.14 EUR/minute, mobile networks max. 0.42 EUR/minute)
E-mail: telesec_support@t-systems.com

4 Operational requirements in the life cycle of certificates

4.1 Placement of a certificate order

4.1.1 Who can order a certificate?

The certificate holder or a person authorized within the meaning of Sections 3.2.2 and 3.2.3 can order certificates.

4.1.2 Ordering procedure and obligations

A certificate for certification authorities can only be generated once the process of registration with the Order Management for TeleSec products has been successfully completed and documented.
Telephone Order Management: +49 271 708-1500
Fax: +49 1805 3344900091
PC-Fax.: +49 521 98840091
E-mail: telesec-auftrag@t-systems.com
The registration process includes at least the following steps:
the concluded contract is available,

- submission of the certificate order using the mechanisms prescribed by the certification authority (e.g. signed online order in the PKCS#10 format),
- possibly presentation of additional authorization and identification documents in accordance with the security level for organizations or natural persons,
- evidence of ownership of the private key in accordance with Section 3.2.1,
- full review of the order data by the registration authority, and
- archiving of the order data.

4.1.2.1 Registration process in case of CA concatenation

In order to become a sub-CA of the “T-TeleSec GlobalRoot Class 3”, a root certificate for CA concatenation must be applied for (only available to internal services - see 1.3.1 Certification authorities).
The registration process comprises at least the steps described in Section 4.1.2. The requirements specified in [TSYSROOTSIGN] must be met in addition.

4.2 Processing the certificate order

4.2.1 Performing identification and authentication

The responsible registration authority carries out the identification and authentication in accordance with the provisions of this CPS.

4.2.2 Approval or rejection of certification requests

A certificate order is accepted and forwarded for processing only if the review was successful. This is the case if all necessary customer data has been successfully identified and authenticated. (see Section 3.2)
If the order is rejected, the certificate holder is notified in a suitable manner, specifying the reasons.

4.2.3 Processing period for certificate requests

Processing of the certificate order starts within a suitable period following receipt of the order. There are no provisions for the processing time of an order if no processing time has been specified in an individual agreement.

4.3 Issue of certificates

4.3.1 Measures of the CA during the issuance of certificates

The certification authority normally receives orders that have been checked by the responsible registration authority. Communication with the registration authority takes place by personal handover or by signed and encrypted e-mail communication.
The certification authority checks the order regarding the technical formats and character sets permitted. Following this, the certificate is created. There must be clear mapping between the certificate holder and the key pair in cases where the certificate holder generates the key as well as in cases where keys are generated by the certification authority.

4.3.2 Notification of the certificate holder about the issuance of certificates

The certificate holder is notified in a suitable manner once the certificate has been issued. There are different options for delivery of the certificate:

- the certificate that has been issued is sent to the certificate holder by e-mail, or
- the certificate that has been issued is sent to the certificate holder by data media (CD) via recorded mail.
- the certificate that has been issued is handed over to the certificate holder in person.

4.4 Certificate acceptance

4.4.1 Acceptance by the certificate holder

The certificate holder must submit to the certification authority an acceptance confirmation (Akzeptanzbestätigung CA Zertifikat.rtf [CA certificate acceptance confirmation]) within 7 days.

4.4.2 Publication of the certificate by the CA

The publication of certificates in public directories is not envisaged. The regulations in Section 2.1apply.

4.4.3 Notification of other authorities about certificate issuance by the CA

The notification of other authorities is not envisaged.

4.5 Use of key pair and certificate

4.5.1 Use of the private key and the certificate by the certificate holder

Certificates issued as part of this CPS are issued for certification authorities only. The certificate holder guarantees that the security requirements are complied with.

4.5.2 Use of public keys and certificates by relying parties

Everyone who uses a certificate that was issued in the context of this CPS should

- 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 for authorized and legal purposes only in accordance with the relevant CPS.

4.6 Renewal of certificates (re-certification)

Sub-CA certificates:
It is not planned to renew CA certificates.

EE certificates:
Re-certification involves issuing a new certificate for the certificate holder while retaining the old key pair, if the information contained in the certificate has not changed. A prerequisite for this is that the unique mapping of the certificate holder and the key is retained, the key is not compromised and the cryptographic procedures (e.g. key length) are still sufficient for the period of validity of the new certificate. Re-key of EE certificates is possible, see Section 4.7.

4.6.1 Conditions for re-certification

It is not planned to renew CA certificates.

4.6.2 Who may request re-certification?

Re-certification may be ordered by the certificate holder only.

4.6.3 Expiry of the re-certification

The regulations in Section 3.3apply.

4.6.4 Notification of the certificate holder

The regulations in Section 4.3.1 apply.

4.6.5 Acceptance of re-certification

The regulations in Section 4.4.1 apply.

4.6.6 Publication of a re-certification by the CA

The regulations in Section 4.4.2 apply.

4.6.7 Notification of other authorities regarding a re-certification

The regulations in Section 4.4.3 apply.

4.7 Re-key of certificates

A new key pair is used in the case of a re-key. In all other respects, the statements made in Section 4.6apply analogously.
Detailed information must be described in the CP/CPS of the downstream services.

4.8 Amendment of certificate data

If information in the existing certificate changes, the certificate must be requested again. Detailed information must be described in the CP/CPS of the downstream services.

4.9 Certificate revocation and suspension

4.9.1 Reasons for revocation

The following reasons require the revocation of the certificate by the certificate holder:

- The private key has been compromised, lost, stolen, or disclosed or there is strong suspicion that this has happened.
- The details in the certificate (except for unverified end-entity information) are no longer up-to-date, are invalid, or incorrect.
- The certified key (public key) or the cryptographic algorithms used with it no longer meet current requirements.
- A case of misuse by the persons authorized to use the key has occurred or is suspected to have occurred.
- Legal requirements or court judgments.
- The certificate is no longer required or the certificate holder expressly requests the revocation of the certificate.
- In case of CA concatenation: the rules laid down in a contract and described in [TSYSROOTSIGN] are not adhered to.

The T-Systems Trust Center revokes certificates, if the following reasons apply:

- It becomes known that the private key has been lost (e.g., loss or theft).
- The private key has been or is suspected to have been compromised.
- There is a considerable payment default beyond the payment periods agreed in the contract.
- The details in the certificate (except for non-verified information) are no longer correct.
- There is a case of misuse or the suspicion of misuse of the certificate by the certificate holder or other persons authorized to use the key.
- The certificate is used or handled in conflict with the GT&C (General Terms and Conditions) or the certificate policy or certification practice statement (CP/CPS).

- The certified key or the algorithms used with it no longer meet current requirements.
- It comes to light that an essential requirement for issuing the certificate has neither been fulfilled nor had its fulfillment waived.
- The certification authority ceases operations.
- Legal requirements or court judgments.
- The certificate holder is no longer authorized to use the certificate.

4.9.2 Who can request that a certificate be revoked?

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

- Authorized persons representing legal persons.
- Registration staff from the T-Systems Trust Center.

The regulations in Section 3.4 apply in particular.

4.9.3 Revocation procedure

Persons and institutions authorized for revocation may request a certificate to be revoked by e-mail or telephone. The revocation is authorized in a suitable way.
If the conditions for the revocation are met, the revocation is carried out and the revoked certificate is included in the revocation information. The revocation information is provided in accordance with the standard (ARL). The person or institution authorized will be notified in a suitable manner that the revocation has been carried out.

4.9.4 Deadlines for a revocation order

The certificate holder must initiate the revocation without delay if the corresponding reasons apply.

4.9.5 Periods for processing of a revocation request by the CA

The revocation orders are accepted by the revocation service, see Section 3.4, and forwarded to the T-Systems Trust Center via a trouble ticket system. There the revocation is executed without delay following receipt of the details, and the revocation list is generated and published.

4.9.6 Checking methods for relying parties

Revocation information is provided in a standard form (ARL) in the DER format and can therefore be checked using applications that comply with the standard.

4.9.7 Frequency of the publication of revocation information

The revocation information is updated every six months in a standardized form (ARL) and provided. Any revocation of a certificate that is relevant for the list within these six months triggers a new ARL to be created at that time.

4.9.8 Maximum latency period of revocation lists

The revocation lists are made available in the Directory Service within an economically suitable period after they have been generated.

4.9.9 Online availability of revocation/status information

Revocation information will be provided online for the certificate users, see Section 2.1, based on a procedure that complies with the standard. All CA certificates revoked by this certification authority are included. Online information on the certificate status is available via OCSP at http://ocsp.telesec.de/ocspr.

T-Systems operates an OCSP responder signed by the Root CA to validate the validity of sub-CA certificates issued. The OCSP responses are valid for a maximum of five (5) days. The OCSP database is updated within one day if a certificate is revoked.

Provisions for sub-CAs:
Subordinate sub-CAs must operate their own OCSP responder for EE certificates they have issued. The OCSP responses can be valid for a maximum of ten (10) days (nextUpdate field). Sub-CAs must update their OCSP data source (repository) at least every four (4) days.

4.9.10 Requirements for an online checking process

Relying third parties must check the status of a certificate to find out whether a certificate that they wish to rely on is trustworthy. The OCSP service (OCSP Responder) is available for requesting up-to-date status information (see Section 4.9.9).

4.9.11 Other available forms of communicating revocation information

No other forms of communication are used at present.

4.9.12 Special requirements for compromised private keys

If a private key is compromised, the relevant certificate must be revoked as promptly as possible.

4.9.13 Suspension of certificates

Suspension (“on hold” revocation reason) is not permitted for a certification authority.

4.9.14 Who can request a certificate to be suspended?

Not defined.

4.9.15 Procedure for a suspension

Not defined.

4.9.16 Limitation of the suspension period

Not defined.

4.10 Status information services for certificates

An online status information service is available (see Section 4.9.9).

4.11 Ending the use of a certificate

If a contractual relationship is terminated by the certificate holder, the certificate is revoked.

4.12 Key storage and restoration

For certification authorities operated at the T-Systems Trust Center, the key pairs are stored on a security-checked hardware security module (HSM) in encrypted format and filed in a secure environment. Key storage at third parties is not implemented.

5 Building, administration and operation checks

The T-Systems Trust Center is housed in a specially protected building and operated by expert 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 following statements apply to the certification authorities operated by the T-Systems Trust Center. Certification authorities which are in the hierarchy of the "T-TeleSec GlobalRoot Class 3" of the T-Systems Trust Center, but which are operated externally, must implement regulations like the ones described below in an adequate manner and describe them in their CPS. If required, the security-relevant documents of the external certification authorities must also be submitted to T-Systems in order to be checked for compliance with this CPS.

5.1 Physical checks

5.1.1 Location and structural measures

T-Systems operates a Trust Center, which has two fully redundant parts, two separate energy wings (electrical, air conditioning, water) with property management system and emergency power supplies as well as an administration wing. Depending on customer requirements, it is possible to implement a graded anti-failure plan with defined security levels in the Trust Center.

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 Association of Indemnity Insurers (Verband der Schadenversicherer e.V., VDS)/new: German Insurance Association (Gesamtverband der Deutschen Versicherungswirtschaft, GDV), the pertinent DIN standards on fire protection, smoke protection and blocking of attacks. The Trust Center is accepted by VdS/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 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 between the security areas is only possible via turnstiles. Controlled access to the various security areas is also protected by means of a computer-controlled access control system. Guests are only received in exceptional cases and subject to prior notification. Specific security rules apply here.

5.1.3 Power supply and air conditioning

The suction openings 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 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 safety

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 sections are secured by fire-resistant components. Passages through fire protection walls are equipped with self-closing fire doors.

In areas with double floors as well as suspended ceilings the fire protection 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 and logical access controls which offer protection against accident damage (e.g., water, fire and electromagnetic damage).

5.1.7 Disposal

Confidential documents and materials are physically destroyed before being disposed of. Prior to their disposal, data media containing confidential information must be treated in such a way that this data cannot be extracted or restored. Prior to their disposal, cryptographic devices are physically destroyed according to the manufacturer's guidelines. Other waste is disposed of in accordance with T-Systems' regular disposal guidelines.

5.1.8 External backup

T-Systems 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

5.2.1 Trustworthy roles

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

Trustworthy persons are in particular:

- Trust Center staff (e.g., system administration)
- staff of cryptographic departments
- Security personnel
- Responsible technical personnel and
- Managerial staff responsible for managing the trustworthy infrastructure.

The above-named trustworthy persons must fulfill the requirements set out in this CP/CPS (see Section 5.3.1). The Change Advisory Board of the T-Systems Trust Center is responsible for initiating, performing, and controlling the methods, processes, and procedures that are illustrated in the security plans, in the CP/CPS of the certification authorities operated by the T-Systems Trust Center.

5.2.2 Number of persons required for a task

The operational maintenance of the certification authority and the directory service (administration, backup, restoration) is carried out by knowledgeable and trustworthy staff.
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 members of staff.

5.2.3 Identification and authentication for every role

T-Systems employees who are classed as trustworthy and who carry out trustworthy activities, are subject to a T-Systems internal security check (see Section 5.3.2).
T-Systems ensures that employees have achieved a trustworthy status and the department has given its approval before these employees:

- receive access devices and can access the necessary facilities
- receive electronic authorization to access the SBCA and other IT systems
- are permitted to carry out certain tasks in connection with these systems.

5.2.4 Roles that require a separation of functions

The following roles require a separation of functions and are therefore carried out by different employees:

- backing up and restoring databases and HSMs
- key lifecycle management of CA and root CA certificates.

5.3 Staff measures

5.3.1 Required qualifications, experience and security checks

Employees who wish to work as trustworthy persons 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.
T-Systems must be provided with a certificate of good conduct at regular intervals, but no later than after three years.

5.3.2 Security check

Before starting work in a trustworthy role, T-Systems runs a security check which includes the following:

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

If the requirements set out in this section cannot be fulfilled, T-Systems will use another legally permitted method of ascertaining essentially the same information.

Results of a security check which could lead to a candidate for a trustworthy person being rejected can include

- False statements by the candidate or the trustworthy person
- Particularly negative or unreliable employment references, and
- Certain previous convictions.

Reports containing such information are evaluated by employees of the HR department and security personnel, who determine the appropriate course of action. The measures involved in the course of action can even lead to candidates for trustworthy positions having their employment offer withdrawn or to trustworthy 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 T-Systems undergo the training measures required to fulfill their work obligations in a competent and satisfactory manner. T-Systems keeps records of these training measures.
The training programs at T-Systems are tailored towards the individual work areas and include, for example:

- Advanced PKI knowledge
- Procedures according to ITIL
- Data protection
- Security and operational guidelines and procedures of T-Systems
- 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.

5.3.4 Follow-up training intervals and requirements

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

5.3.5 Frequency and sequence of workplace rotation

Not applicable.

5.3.6 Sanctions in the event of unauthorized activities

T-Systems reserves the right to punish unauthorized activities or other violations of this CP/CPS and the procedures described therein, and to initiate corresponding 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

T-Systems reserves the right to use independent contractors or consultants to fill trustworthy positions. These persons are subject to the same functional and security criteria as employees of T-Systems in comparable positions.
The above persons, who have not yet concluded or successfully completed the security check described in Section 5.3.2, are given access to the secure facilities at T-Systems only under the condition that they are accompanied and directly supervised by trustworthy persons.

5.3.8 Documentation for the staff

To enable employees to properly fulfill their work obligations, T-Systems provides its employees with all the aids and documents they need for this (training documents, procedural instructions).

5.4 Log events

5.4.1 Type 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 lifecycle management of CA key pairs or CA systems, the T-Systems Trust Center logs at least the following events:
a) Generation, destruction, saving, back-up and restoration as well as archiving of the key pair or parts of the key pair
b) Events in the lifecycle management of cryptographic devices (e.g. HSM) as well as the CA software in use

5.4.1.2 5.4.1.2 EE and CA certificates

For the lifecycle management of both EE and CA certificates, the T-Systems Trust Center logs at least the following events:

- Initial request and revocation of certificates

- Request for renewal with and without a change of key (renewal and re-key)
- All activities relating to the verification of information
- The event, as well as the date/time and phone number of phone calls relating to the verification and the name of the contact person
- Acceptance or rejection of certificate orders
- Issuing of a certificate
- Generation of revocation lists and OCSP entries

5.4.1.3 Other security-related events

In addition, the T-Systems Trust Center logs all security-related events for the operation of the infrastructure. This includes at least the following events:

- Successful and unsuccessful attempts to access the PKI systems
- Actions performed on and by the PKI and other systems that are relevant for security
- Changes to the security profile
- System crashes, hardware failures and other anomalies
- Firewall and router activities
- When people access and leave Trust Center facilities

5.4.2 Processing interval of the logs

The audit logs/logging files are continuously examined for important events relevant to security and operations. Furthermore, T-Systems 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 Storage period for audit logs

Audit logs/logging files are archived after processing according to Section 5.5.2.

5.4.4 Protection of audit logs

Audit logs/logging files are protected against unauthorized access.

5.4.5 Backup procedures for audit logs

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

5.4.6 Audit recording system (internal vs. external)

Audit data/logging files at an application, network and operating system level are automatically generated and recorded. Manually generated audit data is recorded by T-Systems 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 Assessment of vulnerabilities

The Trust Center administrators are regularly informed about weaknesses found in software products. After analyzing the information, the vulnerability is assessed and counter-measures are determined which are then immediately implemented.

5.5 Data archiving

5.5.1 Type of archived datasets

T-Systems archives the following data:

- hard copy of request documents
- all audit/event logging files recorded pursuant to Section 5.4

5.5.2 Storage period for archived data

The following records and storage periods are stipulated:

- Order documents, in particular information regarding certificate requests, their validation and the certificates resulting from this and revocations executed are retained for at least ten (10) years after the certificate validity expires.
- Audit and event logging data are to be archived in accordance with the current legal provisions.

5.5.3 Protection of archives

T-Systems ensures that only authorized and trustworthy persons are given access to archives. Archive data is protected against unauthorized read access, changes, 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.

5.5.5 Requirements for timestamps of datasets

Datasets such as certificates, certificate revocation lists, OSCP responses and logging files are given information on the date and time. The time source is the receive signal of the DCF 77, from which the UTC is derived.

5.5.6 Archive recording system (internal or external)

T-Systems only uses internal archiving systems.

5.5.7 Procedures for obtaining and checking archive information

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

5.6 Key change

Within the period of validity, a key change or certificate change may be required if

- If the key material is compromised
- If the cryptographic algorithm needs to be changed
- If the key length needs to be changed
- If the certificate content is changed

The generation of new keys and certificates is documented and monitored in accordance with the rules of the key generation ceremony. New certificates and their fingerprints are published (see Section 2.3).
Certificates can only be renewed within the period of validity of the root certification authority (root CA) higher up in the hierarchy. Expired or revoked certificates remain available for validation on a website.

5.7 Compromising private keys of root CA and subordinate certification authority (sub-CA)

5.7.1 Handling of incidents and compromised situations

Incidents are submitted via the contacts defined in Section 1.5.2 and processed in the context of service management.

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 T-Systems security department. The event entails a corresponding escalation, incident investigation, incident response and finally incident resolution. Disaster recovery is carried out depending on the incident classification.

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

If it becomes known that the private key of a CA is compromised, the incident is immediately investigated, assessed and the necessary steps taken.
End entities are informed that the relevant websites may be compromised (see Section 2.3). If necessary, the certificate(s) must be immediately revoked and the corresponding certification authority revocation list (ARL) generated and published.

5.7.4 Business continuity after an emergency

T-Systems 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 regularly checked, tested and updated accordingly at least once a year to enable a targeted and structured response in the event of a catastrophe.

The emergency plan contains at least the following information:

- The necessary criteria for activating the plan

- Possible emergency measures (depending on the situation)
- Fallback procedure
- Restart procedure
- Procedure for regular maintenance, updating, and further development
- Awareness creating 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 (MTD) 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 catastrophe (emergency operation) until secured normal operation in line with the requirements is restored

As part of a compliance audit (see Section 8), the auditor is authorized to view the details of the emergency plan.

5.8 Cessation of operations

Cessation of operations may only be invoked by the T-Systems Board of Management.
If a T-Systems RA/CA has to be shut down, a cessation plan will be developed. Economically suitable efforts (or efforts promised in the individual agreements) will be made to notify in advance any subordinate authorities affected by these terminations of operations.

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.

6 Technical security measures

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 in a security plan (not publicly available).
The following statements apply to the certification authorities operated by the T-Systems Trust Center. Certification authorities which are in the hierarchy of the "T-TeleSec GlobalRoot Class 3" of the T-Systems Trust Center, but which are operated externally, must implement regulations like the ones described below in an adequate manner and describe them in their CPS.

6.1 Generation and installation of key pairs

6.1.1 Generation of key pairs

All key pairs for root CA and CA certificates are generated in a protected room on a security-checked hardware component and stored on a hardware component.
In the case of root CA and CA certificates, the private keys are generated and stored on a hardware security module that has been security-checked (FIPS 140-2 evaluated).

6.1.2 Delivery of private keys to certificate holders

Delivery of the private key of a root certification authority (Root CA) or a subordinate certification authority (sub-CA) to the certificate holder is secured.

6.1.3 Delivery of public keys of the certification authority to certificate users

Public keys of a certification authority can be obtained from the relevant directory as well as from the websites of the certification authority (there you can also find the corresponding fingerprints) (see also Section 1.5.3).

6.1.4 Delivery of public keys to trusting third parties

The delivery of CA certificates is contractually agreed with the customer.

6.1.5 Key lengths

RSA keys must have a minimum length of 2048.

6.1.6 Definition of the parameters of the public keys and quality control

Not relevant.

6.1.7 Key usage

The key usages of the root CA and CA certificates are defined in the “key usage” attribute. For root CA and CA certificates, the “key usage” attribute is restricted to the “keyCertSign” and “cRLSign” parameters. For CA certificates, whose keys are also used to sign log messages, the “digitalSignature” parameter may also be set.

6.2 Protection of private keys and technical checks of cryptographic modules

T-Systems has implemented physical, organizational and procedural mechanisms to ensure the security of CA keys.
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 a security-checked hardware security module (FIPS 140-2/level 3 evaluated). The keys are backed up using high-quality multi-person backup techniques (see also Section 6.2.2)

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

T-Systems has implemented technical, organizational and procedural mechanisms that require the participation of several trustworthy and trained persons of the T-Systems Trust Center to be able to carry out confidential cryptographic CA operations. The usage of the private key is protected by a divided authentication process (trusted path authentication with key). Every person involved in the process has secrets that only enable certain activities in their entirety.

6.2.3 Storage of private keys

The storage of private keys with trustees outside T-Systems is not permitted.

6.2.4 Backup of private keys

T-Systems creates backup copies of the key material of the CA certificate for restoration and disaster recovery purposes. These keys are stored in encrypted form within cryptographic hardware modules (HSM) and associated key storage devices.

6.2.5 Archiving of private keys

CA, root CA and OCSP keys are destroyed when they reach the end of their validity periods. They are not archived.

6.2.6 Transfer of private keys in or by a cryptographic module

T-Systems generates CA keys on cryptographic hardware modules (HSM). Copies of these keys are made for restoration and disaster recovery purposes (see Section 6.2.4 and 6.2.5). In this case the transfer between both modules takes place in encrypted form.

6.2.7 Storage of private keys on cryptographic modules

T-Systems stores CA keys in secure form on cryptographic hardware modules (HSM).

6.2.8 Method for activating private keys

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

6.2.8.1 Keys of end entities

The end entity is entitled to take economically suitable measures to physically protect the hardware/software used, to prevent the space/components and the respective private key being used without the end entity's authorization.

6.2.8.2 Keys of administrators

The administrator or operator must comply with the following provisions to protect the private key:

- Setting of a password or a PIN (according to Section 6.4.1) or integration of an equivalent security measure in order to authenticate the administrator or operator prior to activation of the private key. This can, for example, also contain a password for operating the private key, a Windows login or screensaver password or a login password for the network.
- Taking appropriate measures to physically protect the administrator or operator workplace against unauthorized access.

6.2.9 Method for deactivating private keys

The deactivation of private keys belonging to administrators and operators is event-based and the responsibility of the Trust Center staff at T-Systems. The end entity is responsible for the deactivation of private end-entity keys.

6.2.10 Method for destroying private keys

The destruction of CA keys requires the participation of several trustworthy persons of 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.
End entities are responsible for destroying their own private keys.

6.3 Other aspects of managing key pairs

6.3.1 Archiving of public keys

Certificates are backed up and archived as part of the regular T-Systems backup measures. Other procedures are defined in the individual agreements.

6.3.2 Validity periods of certificates and key pairs

The “T-TeleSec GlobalRoot Class 3” certificate is valid for 25 years. CA certificates can be issued up to the maximum validity period of the root CA (see also Section 7.1).
TLS/SSL EE certificates have a maximum duration of 39 months. As of Mar. 1, 2018, the duration of these certificates will be limited to a maximum of 825 days and the documents for checking the certificate information are valid for 825 days.

6.4 Activation data

6.4.1 Generation and installation of activation data

In order to protect the private keys of the CA certificates stored on the HSM, activation data (secret shares) is generated according to the requirements described in Section 6.2.2 of this CPS and the “key ceremony” document. The generation and distribution of secret shares is logged.

6.4.2 Protection of activation data

The Trust Center administrators or persons authorized by T-Systems undertake to protect the secret shares for activating the private keys of CA and OCSP certificates.

6.4.3 Other aspects of activation data

6.4.3.1 Transfer of activation data

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

6.4.3.2 Destruction of activation data

After the private keys have been deleted (Section 6.2.10) the activation data is no longer worth protecting.

6.5 Computer security checks

T-Systems carries out all PKI functions with the help of trustworthy and appropriate systems.

6.5.1 Specific technical requirements for computer security

T-Systems ensures that the management of CA systems is protected against unauthorized third-party access. T-Systems uses protection mechanisms (e.g., firewalls, access protection, dual control principle), to protect the CA functions, directory services and OCSP responder against internal and external intruders. Direct access to CA databases that support the CA functions is restricted to appropriate, trained and trustworthy operating personnel.

6.5.2 Assessment of computer security

As part of the security concept, different threat analyses are carried out to test the effectiveness of all measures implemented.

6.6 Technical checks on the lifecycle

6.6.1 System development checks

No provisions.

6.6.2 Security management checks

T-Systems has implemented mechanisms and/or guidelines to be able to control and monitor the configuration of its CA systems. The integrity is manually verified prior to installation.

6.6.3 Security checks on the lifecycle

No provisions.

6.7 Network security checks

The following network security measures must be implemented:

- The networks of subordinate certification services must be separated from the Internet by current, state-of-the-art firewalls. Data traffic must be limited to the necessary extent for the functions.
- Security-critical components and systems that are accessible from the Internet (e.g. directory service, OCSP responder) are to be separated from the Internet and internal networks by firewalls. All other security-critical components and systems (e.g. CA, DB, Signer) must be operated on a separate network.

6.8 Time stamp

Date and time information in certificates, revocation lists, online status checks and other important information should be derived from a reliable time source (see Section 5.5.5).

7 Certificate list, revocation list and OCSP profiles

7.1 Certificate profile

The certificate profile of the "T-TeleSec GlobalRoot Class 3" root certificate is shown in the following table:

Certificate field	Content		Notes
Version	v3		
SerialNumber	01		Hexadecimal (decimal 1)
SignatureAlgorithmIdentifier	RSA, SHA-256		
Issuer			
Country Name	DE		
Organization Name	T-Systems Enterprise Services GmbH		
Organizational Unit Name 1	T-Systems Trust Center		
Common Name	T-TeleSec GlobalRoot Class 3		
Validity			
Not Before	Oct 1 10:29:56 2008		GMT
Not After	Oct 1 23:59:59 2033		GMT
Subject			
Country Name	DE		
Organization Name	T-Systems Enterprise Services GmbH		
Organizational Unit Name 1	T-Systems Trust Center		
Common Name	T-TeleSec GlobalRoot Class 3		
SubjectPublicKeyInfo			
Algorithm	<OID for RSA>		
Subject Public Key	<Key>		Key length: 2048 bit
Extensions			
Subject Key Identifier	Non-critical	B5:03:F7:76:3B:61:82:6A:12:AA:18:53:EB:03:21:94:BF:FE:CE:CA	
Basic Constraints	Critical	CA:TRUE	
Key Usage	Critical	Certificate Signing, CRL Signing, Off-line CRL Signing	

Table 3: Certificate profile

The serial number must be created with a cryptographically secure pseudo-random number generator (CSPRNG). It must be greater than zero, divisible by 8 and have at least 64 bit entropy.

Certificate profiles for CA and subscriber certificates are defined in the CPS of a certification authority.

7.1.1 Version number(s)

Refer to the descriptions in the CPS of the relevant certification authority.

7.1.2 Certificate extensions

In order to meet the X.509v3 standard, T-Systems supplements the certificate profile with corresponding extensions, depending on the requirements of the subordinate certification authorities (Sub-CAs). These should be described in the CP/CPS of the downstream services.

7.1.3 Object IDs of algorithms

The following signature algorithm are currently used in CA and EE certificates:
- SHA256 RSA (OID 1.2.840.113549.1.1.11)
- SHA256 ECDSA (OID 1.2.840.10045.4.3.2)

Sub-CA, EE and OCSP certificates may not be issued with the SHA-1 hash algorithm. SHA-2 EE certificates may not be issued from a SHA-1 sub-CA.
Root-CA and cross-CA certificates that were issued with a SHA-1 hash algorithm may continue to be used.

7.1.4 Name forms

The end entity certificates of the subordinate certification authorities (sub-CAs) must be given a distinguished issuer name (issuer DN) for this service and a distinguished subject name (subject DN) as described in Section 3.1.1.

7.1.5 Name constraints

Name constraints can result from the character set used and/or field lengths.

7.1.6 Object IDs for certification policies

7.1.6.1 End-entity certificates

Public device certificates that are issued by a sub-CA below a root-CA "T-TeleSec GlobalRoot Class 3", must be given a policy OID which represents a dedicated assurance that the public device certificate and its management meets the requirements of the [CAB-BR] throughout its life cycle. This policy OID must be defined and described in the CP and/or CPS of the relevant sub-CA.

The sub-CAs (affiliate) operated by T-Systems must use the policy OIDs 2.23.140.1.2.1 (DV) or 2.23.140.1.2.2 (OV) defined by the CA/browser forum. An additional OID can be used if specially requested by the customer.

In the case of external customers (non affiliate), it must be agreed with them which policy OID the external sub-CA uses for this purpose.

7.1.6.2 Sub-CA certificates

This section refers solely to sub-CA certificates which were issued after July 1, 2012 under the "T-TeleSec GlobalRoot Class 3" root-CA:

External sub-CA certificates contain a policy OID which represents a dedicated assurance that the sub-CA meets the requirements of the [CAB-BR] throughout its life cycle.

The anyPolicy-OID (2.5.29.32.0) is not permitted in external sub-CA certificates (non affiliate). This OID cannot be used for internal sub-CA certificates (affiliate).

In internal sub-CAs (affiliate), the OIDs 2.23.140.1.2.1 (DV) or 2.23.140.1.2.2 (OV) defined by the CA/browser forum are used to assure compliance with the [CAB-BR]. An additional OID can also be used if specially requested by the customer.

In all cases, it must be ensured that at least one of the policy OIDs used is available both in the corresponding public device certificates and in the corresponding sub-CA certificate/s.

The regulations contained in this Section apply to all hierarchy levels hierarchically below the "T-TeleSec GlobalRoot Class 3" root-CA, i.e. also for the concatenation of sub-CA certificates.

7.1.7 Object IDs for baseline requirements certificate policies

The following requirements, which all sub-CAs must hierarchically comply with below the “T-TeleSec GlobalRoot Class 3” root-CA, apply to the policy OIDs defined by the CA/browser forum in the [CAB-BR].

1. Policy-OID 2.23.140.1.2.1
   If the policy OID 2.23.140.1.2.1 (DV) is used in a certificate, the following Subject DN fields may not be completed:

2. Policy OID 2.23.140.1.2.2
   If the policy OID 2.23.140.1.2.2 (OV) is used in a certificate, it is mandatory to complete the following Subject DN fields:
   stateOrProvinceName (if a meaningful value exists, e.g. federal state in Germany)

7.2 Revocation list profiles

The revocation lists issued by T-Systems meet the following requirements:

-

Table 4: Revocation list profiles

7.2.1 Version number(s)

Refer to the descriptions in the CPS of the relevant certification authority.

7.2.2 Revocation list and revocation list entry extensions

Refer to the descriptions in the CPS of the relevant certification authority.

7.3 OCSP profile

7.3.1 Version number(s)

Refer to the descriptions in the CPS of the relevant certification authority.

7.3.2 OCSP extensions

T-Systems does not offer any OCSP extensions.

8 Compliance audits and other checks

An annual ETSI audit for certification authorities (e.g. ETSI TS 102 042 or an equivalent audit) is carried out for the relevant components covered by the scope of this document.
T-Systems reserves the right to carry out audits or investigations at operators of certification authorities. The frequency of these audits will be specified in individual agreements. Particularly security-critical events may require unplanned audits. For CA concatenation with CAs of external customers the rules of [TSYSROOTSIGN] apply.

8.1 Audit intervals

According to the requirements, an audit is performed at least once a year. Special events or additional requirements can make further audits necessary.

Regular self-audits are carried out for EV certificates at intervals of three months. A sample of at least 3% of all EV certificates is used to do this.

8.2 Identity/qualification of the auditor

A recognized, reputable audit company will be commissioned to establish compliance with ETSI.

8.3 Relationship of the auditor to the authority to be audited

A recognized, reputable and independent audit company will be commissioned to establish compliance with ETSI.

8.4 Audit areas covered

The scope of the audit is determined by the auditor himself. The aim of the audit is to implement this document. All processes associated with the lifecycle management of certificates are to be checked:

- identity checks on end entities
- certificate request procedures
- certificate ordering procedures
- processing of certificate requests
- certificate revocations
- access protection
- authorization and role concept
- anti-burglary measures
- staff

In each case, the audit is performed in line with the currently valid versions of the following audit criteria:

- Root-CAs and sub-CAs which issue server certificates must be checked according to the following criteria:
  or
- Root-CAs and sub-CAs which issue SMIME certificates must be checked according to the following criteria:
  or
- Baseline requirements

8.4.1 Risk assessment and security plan

The T-Systems Trust Center performs an annual risk assessment. The assessment covers at least the following items:

- Identification of foreseeable external and internal risks (i.e. in particular the underlying vulnerabilities) that may 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.
- Assessment of the likelihood of occurrence and the resulting potential damage (i.e., extent of damage) due to exploitation of a vulnerability. Here, the particular need for protection 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., guidelines, procedures, security systems used, technologies, insurance policies) to remove the danger or minimize the risk.

Based on the risk assessment, the T-Systems Trust Center has developed a security plan that is regularly checked and, if necessary, modified. The security plan is made up of processes, measures, and products to support assessment and management during the risk assessment of identified risks. The security plan contains administrative, organizational, technical, and physical security measures according to the sensitivity of the data and the certificate management process.

8.5 Measures for rectifying any defects or deficits

If an auditor finds major deficits or errors during a compliance audit at the certification authority's operator, the appropriate corrective measures will be decided on. The director 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 the results

The results of the audit will be documented in a report prepared by the auditor and passed on to T-Systems. T-Systems reserves the right to publish results or partial results if misuse occurred or the image of T-Systems was harmed.

The relevant audit reports are published on the homepage of the T-Systems Trust Center at https://www.telesec.de/de/trust-center.

9 Other business and legal affairs

9.1 Charges

9.1.1 Charges for issuing or renewing certificates

T-Systems is entitled to charge for issuing, renewing, and managing certificates. Prices are governed by the certification authority's General Terms and Conditions (GT&C) applicable to the relevant service or by individual agreement.

9.1.2 Charges for access to certificates

T-Systems does not charge for access to certificates in the directory service.

9.1.3 Charges for access to revocation or status information

T-Systems 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

T-Systems does not charge for access to this document and the associated simple viewing.
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, 9.5) that owns the copyright.
The use of this document is also free of charge if it serves as a further applicable contractual document for the contractual relationship between the customer and T-Systems.

9.1.5 Reimbursement of charges

T-Systems reimburses charges in accordance with the legal regulations under German law. Detailed provisions can be found in the General Terms and Conditions (GT&C).

9.2 Financial responsibilities

Financial responsibilities are determined in the General Terms and Conditions (GT&C) or in an individual agreement.

9.2.1 Insurance coverage

The insurance coverage is described in the General Terms and Conditions (GT&C).

9.2.2 Other financial means

Not applicable.

9.2.3 Insurance cover or guarantees 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 1.3) which is not covered by Section 9.3.2.

9.3.2 Scope of non-confidential information

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

9.3.3 Responsibility regarding the protection of confidential information

T-Systems, as PKI service provider, is responsible for the protection of confidential information and compliance with data protection provisions. The registration authority of third parties must abide by the applicable statutory provisions and other regulations concerning data protection.

9.4 Protection of personal data (data protection)

9.4.1 Data protection concept

Personal data of certificate holders is recorded and verified to an extent as is required for issuing the subscriber certificates and to guarantee that these certificates can be trusted.
T-Systems shall ensure the technical and organizational security and other measures in accordance with § 9 BDSG [Federal Data Protection Act] and the annex to § 9 BDSG.

9.4.2 Data to be treated as confidential

The same regulations as in Section 9.3.1 apply for personal data.

9.4.3 Data to be treated as non-confidential

The same regulations as in Section 9.3.2 apply for personal data.

9.4.4 Responsibility for the protection of confidential data

The same regulations as in Section 9.3.3 apply for personal data.

9.4.5 Notification and consent for the use of confidential data

The certificate customer consents to the use of personal data by a CA or RA insofar as it is necessary for service provision purposes.
Furthermore, all information may be published that is not treated as confidential according to Section 9.4.3.

9.4.6 Disclosure according to legal or administrative processes

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 shall inform the other contracting party about this, taking into account the legal provisions.

9.4.7 Other circumstances for disclosure of data

No provisions.

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 T-Systems. Intellectual property rights to the certificates and the ARL remain with T-Systems. The rights of use to the certificates will be specified in individual agreements.

9.6 Assurances and guarantees

T-Systems commits to the following:

- That certificates do not include any statements that are known to or originate from the registration authorities that approve the certificate request or issue the certificate.
- That the certificates do not contain any errors made by the staff of the registration authorities that approve the certificate request or issue the certificate and which can be attributed to improper or careless certificate issuance and management.
- That all certificates comply with the essential requirements of this document.
- That the revocation functions and the use of the CA database (directory service, OCSP responder) fulfill all the essential requirements of the applicable CP/CPS.

9.6.1 Assurances and guarantees of the certification authority (CA)

Additional agreements must be described in the CP/CPS of the downstream services.

9.6.2 Assurances and guarantees of the registration authority (RA)

Additional agreements must be described in the CP/CPS of the downstream services.

9.6.3 Assurances and guarantees of the end entity

Additional agreements must be described in the CP/CPS of the downstream services.

9.6.4 Assurances and guarantees of relying parties

Relying parties must have sufficient information and knowledge to be able to evaluate the handling of certificates and their validation. The relying third party is responsible for its own decisions regarding whether the information provided is reliable and trustworthy.

9.6.5 Assurances and guarantees of other entities

No provisions.

9.7 Disclaimer

The exclusion of liability is described in the applicable General Terms and Conditions (GT&C).

9.8 Limitations of liability

A certification authority will have unlimited liability for damage arising from injury to life, limb, or health, and damage resulting from willful breaches of obligations. Apart from that, liability for damage resulting from a breach of obligations due to negligence will be governed by the General Terms and Conditions (GT&C) or by individual agreement.

9.9 Compensation for damages

Compensation is regulated in the applicable General Terms and Conditions (GT&C).

9.10 Term and termination

9.10.1 Contract duration

The CP/CPS comes into effect when it is published on the T-Systems websites.

Changes likewise come into effect when they are published on the public websites (see Section 2.3).

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 a service ends, all users remain bound by the regulations contained in the CP/CPS until the last certificate issued expires or is revoked.

9.11 Individual messages and communication with subscribers

Unless otherwise contractually agreed, the up-to-date contact details (address, e-mail, etc.) for individual messages will be given to the certification authority.

9.12 Changes to the CP/CPS

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

9.12.1 Amendment procedures

Amendments to the CP/CPS can only be made by the T-Systems 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 (see also Section 2.3).

Updated versions result in the previous document versions becoming invalid. In the event of contradictory provisions, the T-Systems Change Advisory Board will decide on how to proceed.

9.12.2 Notification procedures and periods

If the T-Systems Change Advisory Board believes that significant (e.g., security-relevant) amendments are required immediately, the new CP/CPS will enter into force immediately upon its release (see Section 9.12.1).

9.13 Provisions on dispute resolution

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

9.14 Applicable law

The law of the Federal Republic of Germany shall apply.

9.15 Compliance with the applicable law

The present document is subject to the applicable German laws, regulations, guidelines, 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, guidelines, ordinances, acts and orders result in the corresponding provisions of the present document becoming invalid.

9.16 Various provisions

9.16.1 Complete contract

Not applicable.

9.16.2 Assignment of claims

Not applicable.

9.16.3 Severability clause

If a provision of this CP/CPS is or becomes ineffective or cannot be implemented, the validity of this statement is not otherwise affected as a result. In place of the ineffective and unimplementable provision, such a provision is considered agreed as comes closest to the economic purpose of this document in a legally binding way. The same applies for additions made in order to close contractual lacunas.

9.16.4 Execution (attorney's fees and waiver of rights)

Not applicable.

9.16.5 Force majeure

This regulation is intended to ensure that the contractual partner agrees with his end entities that he does not fall into arrears if the service is delayed or becomes impossible due to a force majeure.

9.17 Other provisions

Not applicable.

10 Glossary

ARL	See Authority Revocation List.
Authority Revocation List	List showing digital certificates that have been revoked by certification authorities. Before a digital certificate of a certification authority is used, the ARL should be used to check whether the certificate may still be used.
CA	Certification Authority. See Certification Authority.
Certificate Policy	Defines the guidelines for generating and managing certificates of a certain type.
Certificate Revocation List	See Revocation list.
Certification Authority	See Certification Authority.
Certification Practice Statement	Explanations for operating a certification authority. In particular, the CPS implements the provisions and policies of the CP of a certification authority.
Chip card	Plastic card with an integrated computer chip. Telephone cards are an example of these. If the computer chip is able to perform calculations, it is also called a smartcard. Smartcards can also be used for cryptographic applications.
CP	See Certificate Policy.
CPS	See Certification Practice Statement.
CRL	Certificate Revocation List. See Revocation list.
CV certificate	card verifiable certificate: certificate in a day/value format (not an X.509 format)
Digital signature	A checksum created with a special mathematical procedure. Guarantees the authenticity of the signatory and the integrity of the data.
Digital certificate	Data record that contains the name of a person or a system, its public key and, if necessary, a few other details and a signature of a certification authority.
Distinguished Name	Format with which unique names can be specified according to the X.500 standard. A digital certificate must contain a DN.
DN	See Distinguished Name.
DMZ	Demilitarized zone: this is a protected computer network that is located between two networks. The computer network is protected against the network behind it by means of a packet filter.
Dual key	Option in which separate key pairs are used for encryption and signature purposes, i.e., a user has two corresponding certificates.
Electronic signature	See digital signature.
End-entity certificate	A certificate that does not use the “certification authority” basic constraint and therefore cannot sign certificates itself.
Device certificate	X.509 V3 certificate that contains either a host name or an IP address in the commonName field (CN) of the certificate holder’s distinguishedName (subject) field and/or in at least one subjectAltName extension.
Hardware security module	Hardware box to generate and store private keys securely.
Hash value	In this context, a fixed length cryptographic checksum (the correct name is cryptographic hash value). It should be as unlikely as possible to calculate the entry from the hash value or to find several possible inputs for the same hash value (hash value is used as a synonym for fingerprint). In most cases a hash value is signed instead of a complete digital document.
HSM	See hardware security module.

ISIS-MTT	Joint specification by TeleTrust and T7 Group for electronic signatures, encryption and public key infrastructures
Key Recovery	Mechanism for recovering keys. This can be necessary if users lose their key (such as through a damaged file).
Compromise	A secret key is compromised if it is made known to unauthorized persons or can be used by them. A compromise could occur through a criminal attack for example.
Cryptography	Science dealing with the encryption of data and related issues (such as digital signatures).
Latency period	Time period between generation and publication, for example of a revocation list
LDAP server	Server that saves the information that can be called up via LDAP.
Lightweight Directory Access Protocol	Protocol for querying directories. This has displaced the significantly more complicated Directory Access Protocol (DAP) in many areas. LDAP provides more options than HTTP and FTP (such as setting up a context that can be maintained using several queries). LDAP is used in particular to query digital certificates and revocation lists within public key infrastructures.
Mail request	Variant of a certificate order where the data is transmitted to the certification authority by e-mail.
Public device certificate	A device certificate that a sub-CA issues in the CA hierarchy below a root certificate.
OCSP	The Online Certificate Status Protocol makes it possible to query the validity of certificates online.
PIN	Personal Identification Number. Secret code used at cash machines, for example.
PKI	See Public Key Infrastructure.
PKIX	Public Key Infrastructure X.509. IETF standard that standardizes all relevant parts of a PKI.
PKS	Public Key Service. Service of the T-Systems Trust Center for issuing and administrating certificates that comply with the German Digital Signature Act.
Policy	Guidelines that determine the security level for creating and using certificates. A distinction is made between Certificate Policy (CP) and Certification Practice Statement (CPS).
PSE	Personal Security Environment. Security-relevant information such as the private key is saved in the personal security environment. The PSE can be available as an encrypted file or on a smartcard and is protected by a password or a PIN.
public key infrastructure	Total sum of the components, processes, and concepts that are involved in using public key processes. Typically, a public key infrastructure consists of central components such as a certification authority and a directory service and different client components.
RA	Registration Authority. Component with which a person or a system must communicate to obtain a digital certificate.
Registration Authority	Component with which a person or a system must communicate to obtain a digital certificate.
Registration authority	Component with which a person or a system must communicate to obtain a digital certificate.
Root CA	See root certification authority.
RSA	Procedure for encryption, for digital signature, and for the secure transmission of keys that is named after the three cryptographers Rivest, Shamir, and Adleman.
SAS 70	Statement of Auditing Standards (SAS) No.70 titled “Service Organizations” – this is an internationally recognized standard that was created by AICPA.
SCEP	Simple Certificate Enrollment Protocol. Protocol for ordering and loading certificates in IPSec devices.
S/MIME	Secure Multipurpose Internet Mail Extension. Extension of the MIME e-mail format, which describes additions for cryptographic services that guarantee the authenticity, integrity, and confidentiality of messages.

Key	In cryptography, a key refers to secret information (secret key) or an official counterpart to it (public key). There are procedures where data is encrypted and decrypted using the same secret key and where a public key is used for encryption and a secret one is used for decryption.
Secure Socket Layer	Crypto protocol for ensuring end-to-end connections on the Internet. Can be used instead of the more complex IPSec in many cases.
SigG	German Digital Signature Act (Signaturgesetz)
SigV	German Digital Signature Regulation (Signaturverordnung)
Signature	See digital signature.
Single key	Option in which the same key pair is used for encryption and signature purposes, i.e., a user has one certificate.
Smart card	Chip card with computing function that can be used for cryptographic purposes.
SOAP	Simple Object Access Protocol: SOAP provides a simple mechanism for exchanging structured information between users in a decentralized, distributed environment.
Software PSE	The file that is protected by encryption for saving a user's private key.
Revocation authority	Component that revokes the certificates.
Revocation list	List of digital certificates that have been revoked. Before a digital certificate is used, a revocation list should be used to check whether it may still be used. It is also referred to as a certificate revocation list (CRL).
SSL	See Secure Socket Layer.
Directory service	Database that enables certificates and information about certificates (especially revocation lists) to be called up.
Web request	Variant of a certificate order where the data is transmitted to the certification authority via a web form.
Wildcard certificate	A certificate that has an asterisk (*) in the left-most position of a fully qualified domain name of the subject contained in the certificate.
Root certification authority	Top-level certification authority in a CA hierarchy whose certificate was thus not issued by another certification authority but signed by the root CA itself.
X.509	Standard whose most important element is a format for digital certificates. Version X.509v3 certificates are supported in all common public key infrastructures.
Certificate	See digital certificate.
Certification authority	Component that issues digital certificates by digitally signing a data record consisting of a public key, name, and various other data. The certification authority also issues revocation information.
Certificate holder	Person or object using a certificate and the corresponding private key.
Area of responsibility	Sub-area in the CA administration hierarchy that is administrated by an RA operator.

11 References

BDSG]	Federal Data Protection Act, Federal Law Gazette (Bundesgesetzblatt) I 2003 p.66.
[CAB-BR]	Version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" document published by CA/Browser Forum at http://www.cabforum.org/documents.html valid at the time.
[EU-RL]	Directive of the European Parliament and of the Council on a Community framework for electronic signatures, 1999/93/EC, EU, 1999
[PKCS]	RSA Security Inc., RSA Laboratories "Public Key Cryptography Standards", http://www.rsasecurity.com/rsalabs
[PKIX]	RFCs and specifications by the Public Key Infrastructure (X.509) IETF working group
	[SigG] Law on general conditions for digital signatures and for the amendment of additional provisions (Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung von weiteren Vorschriften), Federal Law Gazette (Bundesgesetzblatt) I 2001, p. 876
[SigV]	Digital signature regulation (Verordnung zur elektronischen Signatur), BGB1 (German Civil Code). I p. 3074, Nov. 21, 2001
[TSYSROOTSIGN]	T-Systems Root Signing Service Specification