Certification Practice Statement for the T-Systems Trust Center Public Key Infrastructure of Root CA "Deutsche Telekom Root CA 2"

Certification Practice Statement, CPS

Version:	1.8
Last revised:	15.09.2012
Status:	Final

Business flexibility T · · Systems · · ·

Publishing Information

Published by

T-Systems International GmbH
Production, CSS Deutschland, PSS, Identity Management Solutions
Trust Center Services
Untere Industriestraße 20
57250 Netphen, Germany

File name	Document number	Document name
CPS_DT_CA_2_V1.8_EN _ final.docx	1.3.6.1.4.1.7879.13.21	Certification Practice Statement, CPS

Version	Last revised	Status
1.8	15.09.2012	Final

Author	Contents reviewed by	Approved by
T-Systems International GmbH Production, CSS, Global Customer Unit Midmarket Public & Healthcare Security PSS-Trust Center Services	L. Eickholt	A. Treßel

Contacts	Phone/fax	E-mail
Service Desk	Tel: +49 (0) 1805 268 204 (landlines: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute)	telesec_support@t-systems.com

Summary

Certification Practice Statement for the T-Systems Trust Center Public Key Infrastructure of Root CA Deutsche Telekom Root CA 2

Change history

Version	Last revised	Revised by	Changes/comments
0.1	August 8, 2006	L. Eickholt	Initial version - Draft
0.3	October 13, 2006	L. Eickholt	Content updates - Draft
0.9	November 10, 2006	L. Eickholt	Content updates - Draft
1.0	November 29, 2006	M. Graf, W. Pietrus	Corrections
1.1	May 4, 2007	M. Ulm, L. Eickholt	Corrections
1.2	August 15, 2007	M. Ulm, L. Eickholt	Corrections
1.3	September 13, 2007	L. Eickholt	Section 2.2 updated, Section 3.2.4 “End subscriber” deleted, Section 5.4.1 term “end subscriber” deleted, Section 6.3.1 term “end subscriber” deleted, Section 5.8 updated, Section 9.13 added, Section 9.14 updated, Section 9.9 CP changed to CPS, Section 6.2 updated, Section 4.6 expanded, Section 3.1.3 updated, Section 4.3.2 updated, Section 8 completely revised, Section 4.9.3 updated, Section 9.5 expanded, Section 9.9 changed into Section 9.12,Sections 9.12.1 and 9.12.2 added
1.5	April 17, 2009	L. Eickholt, S. Kölsch	Various amendments CA concatenation Section 1.1 amended, Section 1.3.1 updated, Section 1.3.2.1 added, Section 1.3.3.1 added, Section 1.3.5 updated, Section 1.4 expanded, Section 1.5.2 updated, Section 2.1 updated, Section 2.2 updated, Section 3.4 updated, Section 4.1.2.1 added, Section 4.9.1 expanded, Section 4.12 expanded, Section 5 expanded, Section 6 expanded, Section 8 expanded, Section 9.10 updated
1.6	February 28, 2012	L. Eickholt , C. Dahlenkamp	Section 1.4.1.2 updated, Section 1.4.2 updated
1.6.1	March 16th, 2012	L. Eickholt , C. Dahlenkamp	Section 4.9.9 expanded
1.7	July 01,2012	L. Eickholt , C. Dahlenkamp	Incorporating the requirements of the CA / Browser Forum's Baseline Requirements version 1.0
1.8	September 15, 2012	L. Eickholt, C. Dahlenkamp	Updating various telephone numbers and email addresses: Publishing Information, Section 1.5.2, Section 3.4, Section 4.1.2, Section 9.10 Section 1 updated, Section 1.3.1 updated, Section 1.3.1.1 deleted, Section 1.4.1.1 updated, Section 5.3 updated, Section 6.1.1 updated, Section 6.1.5 updated, Section 6.1.7 updated, Section 6.2 updated, Section 8.1 updated, figure 1 updated

Table of Contents

List of figures

1 Introduction

Deutsche Telekom AG' s Trust Center is operated by the Group unit T-Systems International GmbH, Production, Computing Services & Solutions (CSS), Trust Center Applications (**"T-Systems Trust Center")**.

The T-Systems Trust Center operates a number of different certification authorities under different root CAs. 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. Among others the services offered by the Trust Center also include the TeleSec Public Key Service (PKS) which covers the process of issuing qualified certificates in accordance with the German Digital Signature Act (Signaturgesetz, SigG).

1.1 Overview

This document is the **Certification Practice Statement (CPS)** for the PKI of the "Deutsche Telekom Root CA 2" root CA that is operated at the T-Systems Trust Center.

This CPS describes the security level required for operating the PKI 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, in particular the handling of third party concatenated CAs (sub-CAs).
- Issue of certificates
- Renewal of certificates
- Revocation and suspension of certificates
- Structural and organizational security measures
- Technical security measures
- Profiles
- Auditing

- Various general conditions.

1.1.1 Adherence to the CA/Browser Forums Baseline Requirements

T-System's Trust Center warrants that the Root CA „Deutsche Telekom Root CA 2" and all sub CA issued beneath conforms at all times to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ([CAB-BR]) published at http://www.cabforum.org/documents.html. In the event of any inconsistency between this document and the [CAB-BR], the [CAB-BR] take precedence over this document.

Sub CAs at any hierarchy level chaining to the Root CA „Deutsche Telekom Root CA 2" shall publicly give effect to the [CAB-BR] by representing an equivalent statement like to one above in its CP or CPS.

1.2 Document name and identification

Name:	Certification Practice Statement for the T-Systems Trust Center Public Key Infrastructures
Version:	1.8
Date	15.09.2012
Object identifier	1.3.6.1.4.1.7879.13.21

1.3 PKI participants

1.3.1 Certification authorities

In addition to operating certification authorities for internal products and services, the T-Systems Trust Center issues CA certificates for other operators of certification authorities. The structure of the certification authorities is explained below.

The T-Systems Trust Center operates the "Deutsche Telekom Root CA 2" root CA. The root CA certificate 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 these hierarchies. The root CA only certifies certificates from direct subordinate certification authorities.

The structure is schematically represented in the diagram below:

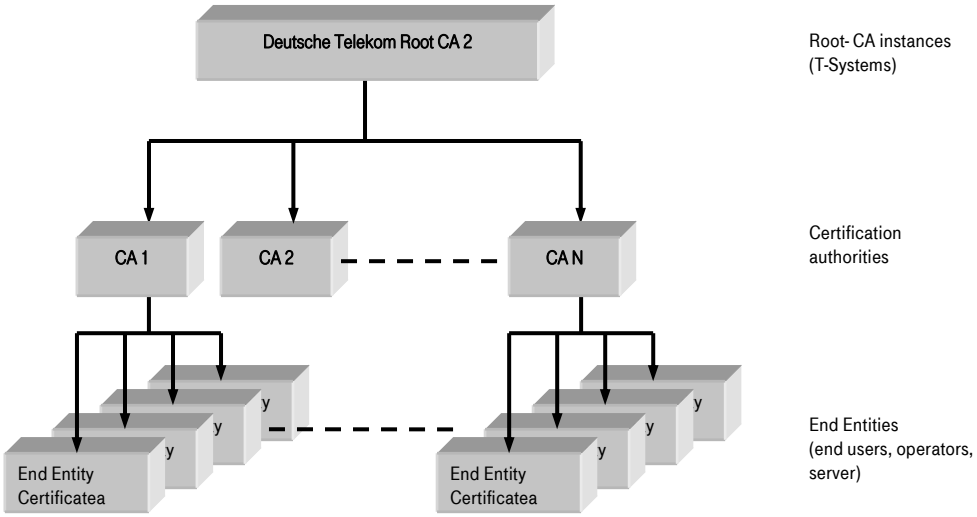

Figure 1: Certification authorities under the "Deutsche Telekom Root CA 2" instance.

Each certification authority has one or more CA and service certificates issued by the relevant higher-level root CA that are re-issued at regular intervals.

The certification authorities shown above and operated by T-Systems or other operators are governed by the T-Systems CP.

1.3.2 Registration authorities

The "Deutsche Telekom Root CA 2" certification authority operates only one central registration authority.

1.3.2.1 Registration authorities in case of CA concatenation

If a CA of an external customer is concatenated as a sub-CA with the "Deutsche Telekom Root CA 2", registration is carried out directly by employees of the T-Systems Trust Center. The provisions of the "T-Systems Root Signing" [TSYSROOTSIGN] Service Specification apply as the contractual and registration basis. The registration will be in accordance with the rules laid down in individual agreements.

1.3.3 Subscribers

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.

1.3.3.1 Subscribers in case of CA concatenation

Subscribers who operate their own CA and want to concatenate this with the "Deutsche Telekom Root CA 2" must meet special requirements. The requirements for being included in the hierarchy as a sub-CA under the "Deutsche Telekom Root CA 2" are described in detail in the "T-Systems Root Signing" [TSYSROOTSIGN] Service Specification.

1.3.4 Relying parties

Relying parties are all natural or legal persons or organizational units that use certificates of subscribers in the context of applications.

1.3.5 Other participants

Subscribers who have not entered into an obligation vis-à-vis Deutsche Telekom Root CA 2 are not considered in the policy.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

1.4.1.1 End entity certificates

Certificates are used for authentication purposes, the digital signature and 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

- advanced signatures in the meaning of the German Digital Signature Act,
- authentication as part of communication protocols (e.g., SSL, IPSec, S/MIME, XML SIG, SOAP),
- authentication as part of processes,
- encryption as part of communication protocols (e.g., SSL, IPSec, S/MIME, XML ENC, SOAP),
- hard disk encryption.

1.4.1.2 Certificates in case of CA concatenation

The root certificates signed in the context of the "T-Systems Root Signing" [TSYSROOTSIGN] service may only be used for issuing digital certificates which on the one hand meet the requirements of this and all other applicable documents and on the other hand comply with the contractually defined reference areas.

T-Systems International will not issue a Sub-CA certificate that can be used for MITM or "traffic management" of domain names or IPs that the subscriber does not legitimately own or control.

1.4.2 Prohibited certificate usage

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

- management and control facilities in dangerous environments,
- environments where 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 not permitted to use a Sub-CA certificate for any kind of MitM scenario as stated in section 1.4.1.2.

1.5 Policy administration

1.5.1 Organization administering the document

This CPS is issued by T-Systems International GmbH, ITO - AL Region – PSS - Security Solutions - Trust Center Services.

1.5.2 Contact

Address:

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

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

1.5.3 Maintenance of the statement

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 Responsibility for recognizing a CPS

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.

1.6 Definitions and abbreviations

See Section 10 (glossary).

2 Publication and repository responsibilities

2.1 Repositories

The T-Systems Trust Center provides the relying parties of the PKI with a public ARL that can be reached 24/7 internationally in the form of an LDAP directory under:

ldap://pki.telesec.de/CN=Deutsche%20Telekom%20Root%20CA%202,OU=T-TeleSec%20Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?AuthorityRevocationList

and on the Internet under

http://pki.telesec.de/rl/DT_ROOT_CA_2.crl

2.2 Publication of certification information

The T-Systems Trust Center provides the relying parties of the PKI with the following information:

- the root CA certificate and its fingerprint (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, and
- CPS in the Released status,
- Specification of Services & requirements profile “T-Systems Root Signing" for the issuing of root certificates (CA concatenation),

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

2.3 Update of the information / publication frequency

Revocation information for root CA and CA certificates is updated without delay in the event of a revocation. 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 Sections 2.1 and 2.2 is not subject to access control for subscribers and relying parties of a certification authority.

Write access to all information listed in Sections 2.1 and 2.2 is only granted to authorized employees or systems.

3 Identification and authentication

3.1 Naming conventions

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 subscriber must be included 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.

3.1.2 Meaningful names

The name must clearly identify the subscriber.

3.1.3 Pseudonymity / anonymity

If certificates are created with pseudonyms, the certification authority must record the real identity of the subscriber 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 service provider transmits the identity of a signature key owner, encryption key owner and authentication key owner with pseudonyms 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 offices 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

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 subscriber's responsibility that his choice of name does not violate any trademark and trademark rights etc. The certification authority is not obligated to check such rights.

Only the subscriber 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 Initial identity validation

3.2.1 Methods for checking the owner of the private key

In the event of a new request, the subscriber 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 external customer

The basic requirement for a new request is an existing contractual relationship. This contractual relationship is generated by T-Systems sales units with help from the legal departments. This ensures sufficient authentication of the external customer.

3.2.3 Authentication of an internal customer

The certification authority checks at least the request data feeding into the certificate in a suitable and conscientious manner.

3.2.4 Unverified information

Unverified information is information that is included in the certificate without being checked and includes:

- Organizational unit (OU)
- other information that is identified as unverified in the certificate.

3.2.5 Authorization to sign

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.

3.2.6 Criteria for Interoperation

Each sub CA shall represent in its CP/CPS that all certificates issued by this sub CA containing a policy identifier indicating compliance with the [CAB-BR] are issued and managed in accordance with the [CAB-BR].

3.3 Identification and authentication for re-key requests

For re-key requests the identity check for initial requests (see Section 3.2) must be carried out.

3.4 Identification and authentication for revocation requests

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 must be used for the revocation:
Telephone: +49 (0) 1805 268 204 (landlines: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute)
E-mail: telesec_support@t-systems.com

4 Operational requirements in the life cycle of certificates

4.1 Placement of a certificate request

4.1.1 Who can request a certificate

The subscriber or a person authorized in the meaning of Sections 3.2.2 and 3.2.5 can request certificates.

4.1.2 Registration process

A certificate for certification authorities can only be generated once the registration process has been successfully completed and documented by Order Management.
Fax: +49 (0) 391 580 108 755
E-mail: trustcenter.notary@t-systems.com

The registration process includes at least the following steps:

- the concluded contract is available,
- submission of the certificate request using the mechanisms prescribed by the certification authority (e.g., signed online request in the PKCS#10 format),
- possibly submission of additional documents for authorization and identification
- evidence of ownership of the private key in accordance with Section 3.2.1,
- full review of the request data by the registration authority, and
- archiving of the request data.

4.1.2.1 Registration process in case of CA concatenation

In order to become a sub-CA of the “Deutsche Telekom Root CA 2”, a root certificate for CA concatenation must be applied for.

The registration process comprises at least the steps described in 4.1.2. The requirements specified in [TSYSROOTSIGN] must be met in addition.

4.2 Processing the certificate application

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 Acceptance or rejection of certificate applications

A certificate application 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 request is rejected, the subscriber is notified in a suitable manner, specifying the reasons.

4.2.3 Processing time

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

4.3 Issue of certificates

4.3.1 Other checks by the certification authority

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

4.3.2 Notification of the subscriber

The subscriber is notified in a suitable manner once the certificate has been issued. Depending on the certification authorities the certificate can be delivered in various ways:

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

4.4 Certificate acceptance

4.4.1 Acceptance by the subscriber

The certificate received is accepted by returning the acceptance confirmation to the certification authority within 14 days following receipt of the certificate, in accordance with the services agreed in the contract.

4.4.2 Publication of the certificate

The regulations in Section 2.1 apply.

4.4.3 Notification of other authorities

Other authorities are not notified.

4.5 Use of key pair and certificate

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

Certificates issued as part of this CPS are issued for certification authorities only. The subscriber 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

Renewal involves issuing a new certificate for the subscriber 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 subscriber 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. It is not planned to renew CA certificates.

4.6.1 Conditions for renewal

Renewal is only permitted before the existing certificate has expired.

4.6.2 Who may request a renewal

Renewal may be requested by the subscriber only.

4.6.3 Expiry of the renewal

The regulations in Section 3.3 apply.

4.6.4 Notification of the subscriber

The regulations in Section 4.3.2 apply.

4.6.5 Acceptance of a renewal

The regulations in Section 4.4.1 apply.

4.6.6 Publication of renewal

The regulations in Section 4.4.2 apply.

4.6.7 Notification of other authorities regarding a renewal

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 4.6 apply analogously.

4.8 Amendment of certificate data

If contents of attributes to the certificate change, re-identification as for initial requests is required.

4.9 Certificate revocation and suspension

4.9.1 Reasons for revocation

The following reasons of the subscriber cause a certificate to be revoked:

- Loss of the private key (e.g., loss or theft).
- There is a case or suspected case of compromise of the private key.
- The details in the certificate are no longer correct.
- Use and handling of the certificate that violates contractual regulations or the CP/CPS of the subscriber or certificate issuer.

- The certified key or the algorithms used with it no longer meet current requirements.
- Misuse or the suspicion of misuse by the subscriber or other persons authorized to use the key.
- The subscriber no longer requires a certificate and therefore terminates the contract.
- Legal provisions
- In case of CA concatenation: the rules laid down in a contract and described in [TSYSROOTSIGN] are not adhered to.

The following reasons of the T-Systems Trust Center cause a certificate to be revoked:

- Loss of the private key (e.g theft).
- There is a case or suspected case of compromise of the private key.
- Considerable payment default beyond the payment periods agreed in the contract.
- There is a case of misuse or the suspicion of misuse by the subscriber or other persons authorized to use the key.
- The certified key or the algorithms used with it no longer meet current requirements.

4.9.2 Who can request a certificate to be revoked?

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

- the subscriber,
- the T-Systems Trust Center.

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 a format that complies 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 request

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

4.9.5 Deadlines for the certification authority

The revocation requests 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 Methods for checking revocation information

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 and provided every six months in a standardized form (ARL). 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 latency period for revocation lists is a minimum of 12 hours.

4.9.9 Availability of online revocation information

Revocation information will be provided online for the relying parties (see Section 2.1) based on a procedure that complies with the standard. All certificates revoked by this certification authority are included.

T-Systems maintenance a OCSP responder signed by the Root-CA to validate issued Sub-CA certificates. OCSP responses are valid for three (3) days. The OCSP repository is updated within 24 hours in cases a certificate is revoked.

Sub-CA Requirements:

Sub-CAs must maintain an OCSP responder to validate issued certificates. OCSP responses must have a maximum expiration time of ten (10) days. The OCSP repository must be updated at least every four (4) days.

4.9.10 Requirements for an online checking process

Not defined.

4.9.11 Other available forms of communicating revocation information

No other forms of communication are used at present.

4.9.12 Compromising 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 is able to arrange a suspension

Not defined.

4.9.15 Suspension process

Not defined.

4.9.16 Restriction of the suspension period

Not defined.

4.10 Status information services for certificates

A status information service is not available.

4.11 Termination by the subscriber

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

4.12 Key storage and recovery

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 pairs for externally operated certification authorities (external sub-CAs in the event of CA concatenation) must be handled according to the rules in [TSYSROOTSIGN].

5 Structural and organizational controls

The T-Systems Trust Center is housed in a specially protected building and operated by knowledgeable staff. All processes for requesting and generating certificates of the certification authorities operated there are defined in detail and, in the case of qualified certificates, have been checked by an independent authority. All structural and organizational 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 root CAs 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 plan of the external certification authorities must also be submitted to T-Systems in order to be checked for compliance with this policy. The minimum requirements for externally operated CAs are described in [TSYSROOTSIGN] and must be implemented by the external customer before the sub-CA goes into operation.

5.1 Trust Center security measures

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: the German Insurance Association (Gesamtverband der Deutschen Versicherungswirtschaft, GDV), the applicable 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 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 intakes for outside air are arranged in such a manner that pollutants such as dust or dirt as well as corrosive, poisonous or highly flammable gases cannot enter. The systems are operated using a very low proportion of outside air. The 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 damage

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 protection

The applicable fire regulations (e.g., DIN 4102, requirements of the local fire department, regulations regarding fire resistance, VDE-compliant electrical installation) are complied with. All fire doors have automatic locking mechanisms. As agreed with the fire department, water will only be used in extreme emergencies for putting out fire.

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

In areas with double floors as well as suspended ceilings the fire protection walls go right through to the ceilings/floors of the storey.

Early fire detection systems (suction systems) are installed in all system rooms, system operator rooms, archive rooms, UPS rooms and in other selected rooms. The supply air and exhaust air of the air conditioning devices in the individual rooms is monitored. Fire alarms are installed in the other rooms.

5.2 Organizational measures

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 (not publicly available) and in the CPS documents of the certification authorities operated by the T-Systems Trust Center.

5.3 Personnel controls

The reliability of the personnel working at the T-Systems Trust Center is checked by an independent organization. The staff attends training courses at regular intervals.

A division of roles for critical processes is defined in the relevant security plan (not publicly available). Organizations acting as a registration authority for the T-Systems Trust Center have concluded contractual agreements that ensure the reliability and expert knowledge of their staff as well as compliance with specific tasks that are assigned.

5.4 Log events

5.4.1 Recorded events

Changes in the life cycle of the CA key are logged. In detail, this relates to the following events:

- Generation
- Backup
- Storage
- Recovery
- Archiving
- Destruction
- Amendments to hardware and software
- Logs of events in the life cycle of CA certificates:
- Certificate request (successful / failed processing and enclosed documents)
- Renewal
- Key renewal
- Certificate revocation
- Generation of certificates
- Revocation lists
- Logging of internal and external audits.

5.5 Backup of records

All records in the T-Systems Trust Center are retained for a period of ten (10) years following the end of the service.

5.6 Key changeover for root CA and CA

For key changes involving a root CA or CA the generation of new keys and certificates must be documented and monitored in accordance with the conditions of the relevant security plan. New certificates and their fingerprints must be published (see Section 2.2).

5.7 Compromising private keys of root CA and CA

If private keys of a root CA or CA are compromised, this must be communicated without delay (see Section 2.2). CA certificates must then be revoked without delay and the corresponding ARL must be published immediately. The generation of new keys and certificates must be documented and monitored in accordance with the conditions of the relevant security plan. New certificates and their fingerprints must be published (see Section 2.2).

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 cessations of operations.

A cessation plan may include the following regulations:

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

If operations (the revocation service, in particular) are not taken over by another certification authority, all certificates issued will be revoked.

6 Technical security controls

The T-Systems Trust Center is housed in a specially protected building and operated by knowledgeable staff. All processes for requesting and generating certificates of the certification authorities operated there are defined in detail. All technical security measures are documented 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 "Deutsche Telekom Root CA 2" 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 plan of the external certification authorities must also be submitted to T-Systems in order to be checked for compliance with this CPS. The minimum requirements for externally operated CAs are described in [TSYSROOTSIGN] and must be implemented by the external customer before the sub-CA goes into operation.

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 140-1/ Lev2-evaluated).

6.1.2 Delivery of public keys to certificate issuers

Public keys are delivered to the certificate issuer securely in the form of signed PKCS#10 requests.

6.1.3 CA public key delivery to relying parties

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 2).

6.1.4 Delivery of public keys to third parties

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

6.1.5 Key lengths

The key length for newly issued CA certificates must be at least 2048 bits. Key lengths for the T-Systems root CA and CA certificates are 2048 bits. They are based on the latest technological developments.

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

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 can also be set.

6.2 Backing up private keys

In the case of root CA and CA certificates, the private keys are stored on a hardware security module that has been security-checked (FIPS 140 – 2 evaluated). Keys are backed up using high-quality multi-person backup techniques. The use of the private key is protected by a PIN which is known only to persons responsible for this. The security plan regulates the details.

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 "Deutsche Telekom Root CA2" certificate is valid for 20 years. CA certificates can be issued up to the maximum validity period of the root CA (see also Section 7.1.1).

7 Profiles for certificates and revocation lists

7.1 Certificate profile

7.1.1 Certificate profile of the root certificate

7.1.1.1 "Deutsche Telekom Root CA 2" certificate profile

Certificate field	Content		Comments
Version	v3		
SerialNumber	26		Hexadecimal (decimal 38)
SignatureAlgorithmIdentifier	RSA, SHA-1		
Issuer			
Country Name	DE		
Organization Name	Deutsche Telekom AG		
Organizational Unit Name 1	T-TeleSec Trust Center		
Common Name	Deutsche Telekom Root CA 2		
Validity			
Not Before	9.7.1999 12:11		GMT
Not After	9.7.2019 23:59		GMT; validity 20 years
Subject			
Country Name	DE		
Organization Name	Deutsche Telekom AG		
Organizational Unit Name 1	T-TeleSec Trust Center		
Common Name	Deutsche Telekom Root CA 2		
SubjectPublicKeyInfo			
Algorithm	<OID for RSA>		
Subject Public Key	<Key>		Key length: 2048 bit
Extensions			
Subject Key Identifier	non critical	31 c3 79 1b ba f5 53 d7 17 e0 89 7a 2d 17 6c 0a b3 2b 9d 33	
Basic Constraints	non critical	CA=1	
		PathLenConstraint=5	
Key Usage	critical	keyCertSign, cRLSign	

7.1.2 Certificate profiles of the certification authorities

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

7.1.3 Algorithm Object Identifiers

Not defined.

7.1.4 Name Forms

Not defined.

7.1.5 Name Constraints

Not defined.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 End Entity Certificates

Publicly-trusted device certificates issued by a sub CA chaing to the Root CA „Deutsche Telekom Root CA 2“ must contain at least one policy OID in the certificate's certificatePolicies extension that indicates adherence to and compliance with the [CAB-BR] during it's life cycle. This policy OID shall be defined and documented in the issuing sub CA's Certificate Policy or Certification Practice Statement.

Affilates of the „Deutsche Telekom Root CA 2“ shall 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. Upon customer request an additional policy identifier may be included.

For a Sub CAs that is not an Affilate of the „Deutsche Telekom Root CA 2“ it must be negotiate which policy identifier the sub CA will use to indicate its adherence to the [CAB-BR].

7.1.6.2 Subordinate CA Certificates

This section applies to sub CA certificates issued from the Root CA „Deutsche Telekom Root CA 2“ after 01.07.2012 only:

A Sub CA certificate that is not an Affilate of the „Deutsche Telekom Root CA 2“ must contain a policy identifier indicating the sub CA's compliance with the [CAB-BR] during its life cycle. It must not contain the “anyPolicy” OID (2.5.29.32.0). An affiliate sub CA may contain this policy OID.

Affiliate sub CAs must contain either the policy OID of 2.23.140.1.2.1 (DV) or 2.23.140.1.2.2 (OV) defined by the CA/Browser Forum to indicate the sub CA's compliance with the [CAB-BR]. Upon customer request an additional policy identifier may be included.

Under all circumstances it must be ensured that at least one of the used policy OIDs is included within the publicly-trusted device certificates as well as in the signing sub CA certificate.

The requirements set forth in this section applies to all hierarchy levels chaining to the Root CA „Deutsche Telekom Root CA 2“, i.e. these apply to concatenated sub CAs also.

7.1.7 Policy Identifier defined by the Baseline Requirements

The CA / Browser Forum has defined policy OIDs ,for which the requirements set forth in the [CAB-BR] applies as stated below. All sub-CAs chaining to the Root CA „Deutsche Telekom Root CA 2“ must adhere to these requirements:

1. Policy-OID 2.23.140.1.2.1
   If the Certificate asserts the policy identifier of 2.23.140.1.2.1, then it must not include information in one of the following Subject field:
   - organizationName
   - streetAddress
   - localityName
   - stateOrProvinceName
   - postalCode

2. Policy-OID 2.23.140.1.2.2
   If the Certificate asserts the policy identifier of 2.23.140.1.2. 2 (OV), then it must also include information in all of the following Subject fields:
   - organizationName
   - localityName
   - stateOrProvinceName (if applicable)
   - countryName

7.2 Revocation list profiles

7.2.1 Revocation list profiles of the certification authorities

Authority Revocation List (ARL) Deutsche Telekom Root CA 2:

Version		2 (0x1)
Signature Algorithm		sha1WithRSAEncryption
Issuer		/C=DE/O=Deutsche Telekom AG/OU=T-TeleSec Trust Center/CN=Deutsche Telekom Root CA 2
Last update		Sep 12 09:46:56 2006 GMT
Next update		Mar 13 21:46:56 2007 GMT (last update + 6 months)
CRL extensions		
	X509v3 Authority Key Identifier	DirName:/C=DE/O=Deutsche Telekom AG/OU=T-TeleSec Trust Center/CN=Deutsche Telekom Root CA 2 Serial:26
	X509v3 CRL Number	10
Revoked Certificates		
	Serial Number	25
	Revocation Date	Jul 9 12:07:00 1999 GMT
CRL entry extensions		
	X509v3 CRL Reason Code	Cessation Of Operation
Signature Algorithm		sha1WithRSAEncryption

8 Audits and other assessment criteria

An annual Webtrust program for certification authorities 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

Audits will be carried out at least once every year in accordance with the requirements, unless specific events require an additional audit.

8.2 Identity/ qualification of the auditor

A recognized, reputable audit company will be commissioned to establish compliance with the Webtrust program for certification authorities.

8.3 Relationship of the auditor to the entity to be audited

A recognized, reputable and independent audit company will be commissioned to establish compliance with the Webtrust program for certification authorities.

8.4 Audit areas covered

The design of the annual Webtrust program for certification authorities or an equivalent audit covers the key life cycle, control of key management, disclosure of the infrastructure as well as administration and business practices.

8.5 Measures for rectifying any defects or deficits

If an audit of T-Systems detects defects or faults, a decision will be made as to what corrective measures are to be taken. The Head of the Trust Center and the auditor jointly decide on suitable measures. The Head of the Trust Center is responsible for developing an action plan. The measures must be implemented within a period that is economically suitable. In the event of serious security-critical defects, a correction plan must be developed within 30 days and the deviation must be rectified within a period that is economically suitable. In the event of less serious deficits, the Head of the Trust Center will decide on the rectification timeframe.

9 Other business and legal affairs

9.1 Fees

Fees are determined in the relevant General Terms and Conditions (GT&C) of the certification authorities.

9.2 Financial responsibilities

Financial responsibilities are determined in the relevant General Terms and Conditions (GT&C) of the certification authorities or in individual agreements.

9.3 Confidentiality of business data

Data of legal persons and organizations as subscribers is recorded and verified to an extent as is required for issuing the subscriber certificates and to guarantee that these certificates can be trusted.

Personal information is protected in accordance with the Federal Data Protection Act (Bundesdatenschutzgesetz) and §14 of the German Digital Signature Act. Personal data is only made available to third parties if this becomes necessary as a result of legal requirements.

9.4 Data protection of personal data

Personal data of subscribers is recorded and verified to an extent as is required for issuing the subscriber certificates and to guarantee that these certificates can be trusted.

As part of the data review, only the identity of the subscriber is determined but not his trustworthiness, credit rating or credit worthiness.

Personal information is protected in accordance with the Federal Data Protection Act (Bundesdatenschutzgesetz) and §14 of the German Digital Signature Act. Personal data is only made available to third parties if this becomes necessary as a result of legal requirements.

9.5 Intellectual property rights

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 Disclaimer

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

9.7 Liability limitations

Liability vis-à-vis the certification authority is unlimited for damages resulting from injury to life, limb and health as well as for damages that are attributable to intentional breach of obligations.

Otherwise, liability for damages attributable to negligent breach of obligations is limited or excluded vis-à-vis the certification authority in individual contracts within the framework of legal feasibility.

9.8 Compensation

9.9 Entry into force and cancelation

9.10 Individual communications and agreements with subscribers

The relevant applicable contact information (address, e-mail, etc.) is communicated in relation to individual communications and agreements with the certification authorities. It is also possible to make contact via the service desk (+49 (0) 1805 268 204 or telesec_support@t-systems.com).

9.11 Mutual notification and communication by subscribers

The subscribers communicate with each other.

9.12 CPS amendments

In order to respond to changing market requirements, security requirements and legislation etc., T-Systems International GmbH reserves the right to amend or adjust this CPS. Changes to the CPS will be valid from the moment the CPS enters into force. The CPS enters into force within six weeks of publication of the amendments (see Section 2.2) unless the publication intends a different period.

If the T-Systems Change Advisory Board believes that significant (e.g., security-relevant) amendments are required immediately, the new document version will enter into force as soon as it is published.

9.12.1 Amendment procedures

Amendments to the CPS can only be made by the T-Systems Change Advisory Board. A new version number and date is created for every amendment to the CPS.

9.12.2 Notifications

Subordinate certification authorities will be notified of amendments and are given the opportunity to object within six weeks. If no objections are made, the new document version enters into force after the end of this period. Any claims beyond this for individual end users to be notified are explicitly excluded.

9.13 Provisions on dispute resolution

In the event of disputes, the Parties must follow an escalation procedure.

9.14 Governing law

The law of the Federal Republic of Germany shall apply exclusively. The place of performance and the exclusive place of jurisdiction is Frankfurt / Main, Germany.

10 Glossary

Area of responsibility	Sub-area in the CA administration hierarchy that is administrated by an RA operator.
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	See digital certificate.
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 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.
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 called a smartcard. Smartcards can also be used for cryptographic applications.
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.
CP	See Certificate Policy.
CPS	See Certification Practice Statement.
CRL	Certificate Revocation List. See Revocation List.
Cryptography	Science dealing with the encryption of data and related issues (such as digital signatures).
CV certificate	Card verifiable certificate: certificate in a day/value format (not an X.509 format)
Device Certificate	X.509 certificate containing a hostname or an IP address in either at least one subjectAlternativeName extension and/or the subject's commonName field.
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.
Digital signature	A checksum created with a special mathematical procedure. Guarantees the authenticity of the signatory and the integrity of the data.
Directory service	Database that enables certificates and information about certificates (especially revocation lists) to be called up.
Distinguished Name	Format with which unique names can be specified according to the X.500 standard. A digital certificate must contain a DN.

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.
DN	See Distinguished Name.
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 not using the basic constraint extension “Certificate Authority” and therefore not allowed to sign certificates.
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 an overall 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	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.
Key Recovery	Mechanism for recovering keys. This can be necessary if users lose their key (such as through a damaged file).
LDAP	See Lightweight Directory Access Protocol.
LDAP server	Server that saves the information that can be called up via LDAP.
Lightweight Directory Access Protocol	Protocol for querying directories that has displaced the clearly more complicated Directory Access Protocol (DAP) in many areas. LDAP offers 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.
MitM	Man-in-the-Middle
Mail request	Variant of a certificate order where the data is transmitted to the certification authority by e-mail.
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. There is a difference between Certificate Policy (CP) and Certification Practice Statement (CPS).
PSE	Personal Security Environment. All 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 used for 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.
Publicly-Trusted Device Certificate	Device certificate issued by a sub-CA within the CA hierarchy chaining to a public root certificate.
RA	See Registration Authority.
Registration Authority	Component with which a person or a system must communicate to obtain a digital certificate.
Revocation Authority	Component that revokes the certificates.
Revocation List	List of digital certificates that have been revoked. Before a digital certificate it used, a revocation list should be used to check whether it may still be used. It is also referred to as Certificate Revocation List (CRL).
Root CA	See root certification authority.
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.
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.
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.
SCEP	Simple Certificate Enrollment Protocol. Protocol for ordering and loading certificates in IPSec devices.
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)
Signature	See digital signature.
SigV	German Digital Signature Regulation (Signaturverordnung)
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.
SSL	See Secure Socket Layer.
Subscriber	Person or object using a certificate and the corresponding private key.

Web request	Variant of a certificate request where the data is transmitted to the certification authority via a web form.
X.509	Standard, whose most important element is a format for digital certificates. Certificates of version X.509v3 are supported in all common public key infrastructures.

11 References

BDSG]	Federal Data Protection Act (Bundesdatenschutzgesetz), Federal Law Gazette (Bundesgesetzblatt) I 2003 p.66
[CAB-BR]	The at all times then-current version of the document "Baseline Requirements for the Issuance and Management of Publicly-Trusted published by the CA/Browser Forum on http://www.cabforum.org/documents.html.
[EU-DIR]	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
[RFC2527]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 1999
[RFC3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003
[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), BGBl. (German Civil Code) I p. 3074, November 21, 2001
[TSYSROOTSIGN]	T-Systems Root Signing Service Specification
[X.509]	Information technology - Open Systems Interconnection - The Directory: authentication framework, Version 3, ITU, 1997