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

Version:	1.3.1
Last revised:	08.05.2012
Status:	draft

Publication details

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

File name	Document number	Document name
CPS_T-TeleSec_GlobalRoot_Class_3_V1 3 1_EN_draft.docx	1.3.6.1.4.1.7879.13.24	Certification Practice Statement, CPS

Version	Last revised	Status
1.3.1	08.05.2012	draft

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

Contact	Telephone	E-mail
Service desk	Tel: +49 (0) 1805 268 204 (landlines: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute) Fax: +49 (0) 2151 36607972	telesec_support@t-systems.com

Summary
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	Sep. 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.08,2012	L. Eickholt, C. Dahlenkamp	Section 1.4.1.3 inserted, Section 1.4.2 updated, Section 4.9.9 expanded, Glossary updated
1.3.1	May.08,2012	C. Dahlenkamp	Clarification: No external Sub-CAs allowed Updated Sections 1.3.1, 1.3.3, 1.3.3.1, 1.4.1.3, 4.1.2.1. Deleted Sections 1.3.2.1, 1.3.3.1

Contents

List of Figures

List of Tables

1 Introduction

The Trust Center is operated by the Group unit T-Systems International GmbH ("T-Systems"). Hereinafter it will be referred to as **"T-Systems Trust Center"**.
The T-Systems Trust Center operates a number of different certification authorities under different root CAs. The certification authorities for 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 as well as the organizational infrastructure meet the strict requirements of the German Digital Signature Act (Signaturgesetz, SigG). 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 T-TeleSec Public Key Service (PKS) which covers the process of issuing qualified certificates in accordance with the German Digital Signature Act.

1.1 Overview

This document is the Certification Practice Statement (CPS) for the PKI of the "T-TeleSec GlobalRoot Class 3" 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.

1.2 Document identification

Name:	Certification Practice Statement for the T-Systems Trust Center Public Key Infrastructure of the "T-TeleSec GlobalRoot Class 3" Root CA
Version:	1.3.1
Date	08.05.2012
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 CA certificates for its own products and services only. Issuing of external sub CA certificates is not offered under this 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 under this hierarchy. The root CA only signs certificates from direct sub CA authorities.
The structure is schematically represented in the diagram below:

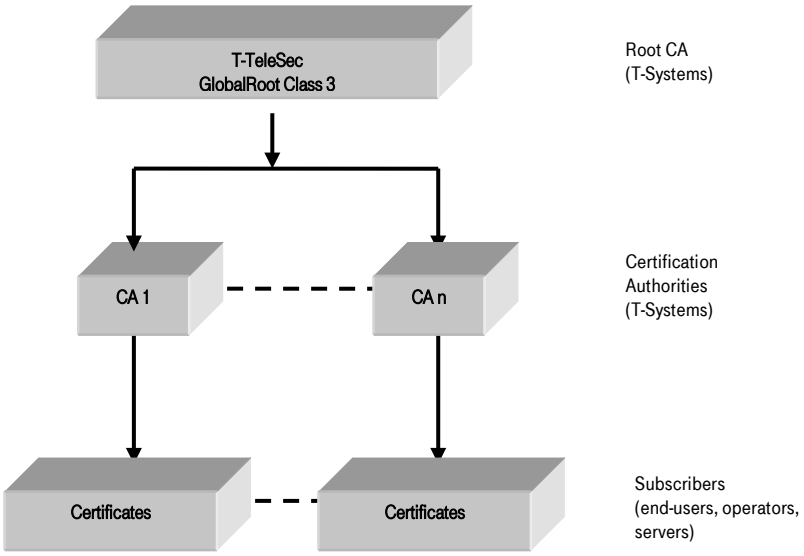

Figure 1: Certification authorities under the "T-TeleSec GlobalRoot Class 3" root CA.

Each certification authority operates one or more service and CA certificates issued by the relevant higher-level CA. Those certificates are re-issued in regular intervals.
All certification authorities shown above are operated by T-Systems and are 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 holders

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 use

1.4.1 Permitted use of certificates

1.4.1.1 Use for natural persons

Certificates are used for authentication purposes, the 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 Signature	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 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 1.4.1.3.

1.5 Policy administration

1.5.1 Responsibility for the policy

This Certificate Practice Statement (CPS) is published by T-Systems International GmbH, ICTO-CSS Deutschland – PSS - Trust Center Services.

1.5.2 Contact

Address:

T-Systems International GmbH
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 Responsibility for recognizing a CPS

The authority named in Section 1.5.1 as responsible for this statement is also responsible for certifying that the CPS of a certification authority is compatible with this statement.

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

The URL is:
http://pki.telesec.de/rl/GlobalRoot_Class_3.crl

2.2 Publication of 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 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 2.2is not subject to access control for certificate holders and certificate users of a certification authority.
Write access to all information listed in Sections 2.1and 2.2is only used by 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 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.

3.1.2 Meaningful names

The name must clearly identify the certificate holder.

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, 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

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 certificate holder'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 certificate holder himself is responsible for these checks. If a certification authority is notified of a violation of such rights, the certificate is revoked.

3.2 Identity check 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. Please refer to Section 3.2.4.

3.2.3 Authentication of a natural person

The authentication of natural persons is subject to the following requirements.

3.2.3.1 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 information

The information required for the authentication is checked, see Section 3.2. Other information will not be checked.

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.

3.3 Identification and authentication for follow-up orders

For follow-up orders the identity check for 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 must be used for the revocation:
Telephone: +49 (0) 1805 -268204 (landlines: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute)
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 in the meaning of Sections 3.2.2 and 3.2.5 can order certificates.

4.1.2 Registration process

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.
Order Management phone number: +49 (0) 271 708-1500
Fax: +49 (0) 1805 3344900091
PC fax: +49 (0) 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 (available for internal services only - see 1.3.1Certification 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 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 orders

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 by specifying the reasons.

4.2.3 Processing time

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 Other checks by the certification authority

The certification authority normally receives orders 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 order regarding the technical formats and character sets permitted. Following this, the certificate is created. There must be a 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

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

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 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)

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. It is not planned to renew CA certificates.

4.6.1 Conditions for re-certification

Re-certification is only permitted before the existing certificate has expired.

4.6.2 Who may order a re-certification?

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

4.6.3 Expiry of the re-certification

The regulations in Section 3.3 apply.

4.6.4 Notification of the certificate holder

The regulations in Section 4.3.1 apply.

4.6.5 Acceptance of a re-certification

The regulations in Section 4.4.1 apply.

4.6.6 Publication of re-certification

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 4.6 apply analogously.

4.8 Amendment of certificate data

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

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 non-verified end-user 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 compromised or a compromise is suspected to have occurred,
- Considerable payment default beyond the payment periods agreed in the contract,
- The details in the certificate (except for non-verified information) is 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 precondition for issuing the certificate has neither been fulfilled nor its fulfillment been waived,
- The certification authority terminates operations,
- Legal requirements or court judgments,
- The certificate holder is no longer authorized to use the certificate.

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 certificate holder,
- 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 order

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

4.9.5 Deadlines for the certification authority

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 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 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 Availability of online 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 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

Trusting third parties must check the status of a certificate to find out whether a certificate that they want to trust 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 Compromising private keys

If a private key is compromised, the relevant certificate must be revoked without delay.

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 for 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

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

4.11 Termination by the certificate holder

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 Structural and organizational 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.
The following statements apply for 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 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 by observing 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 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 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 environment), 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 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 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 as well as in other selected rooms. The supply air and exhaust air of the air conditioning devices in the individual rooms is being 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 Staff measures

The reliability of the personnel working at the T-Systems Trust Center is checked by an independent organization. The staff attends training courses in regular intervals.
A division of roles for critical processes is defined. 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 order (successful / failed processing and enclosed documents)
- Re-certification
- 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 change 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 Discontinuation of operations

Termination 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 termination 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 termination plan may include the following regulations:

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

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

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 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 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

The key length for CA certificates of high security level must be at least 2048 bits. Key lengths for the T-Systems GlobalRoot Class 3 and CA certificates are 2048 bits. They are based on the latest technology developments.

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

Not relevant.

6.1.7 Key usage

The key usage of the root CA and CA certificates is 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 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 usage of private keys is protected by a divided authentication process (Trusted Path Authentication with Key) only known to the persons responsible for it.

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 7.1.1).

7 Profiles for certificates and revocation lists

7.1 Certificate profile

7.1.1 Certificate profile of the root certificate

7.1.1.1 Certificate profile of “T-TeleSec GlobalRoot Class 3”

Certificate field	Contents		Comments
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	

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.

7.2 Revocation list profiles

7.2.1 Revocation list profiles of the certification authorities

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

- [RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- [X.509] Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, Recommendation X.509 (08/05), Recommendation X.509 (2005) Corrigendum 1 (01/07)

Authority Revocation List (ARL) T-TeleSec GlobalRoot Class 3

Version		2 (0x1)
Signature Algorithm		sha1WithRSAEncryption
Issuer		C=DE/O=T-Systems Enterprise Services GmbH/OU=T-Systems Trust Center/CN=T-TeleSec GlobalRoot Class 3
Last update		Last update GMT
Next update		Last update + 6 months
CRL extensions		
	X509v3 Authority Key Identifier	B5:03:F7:76:3B:61:82:6A:12:AA:18:53:EB:03:21:94:BF:FE:CE:CA
	X509v3 CRL Number	Serial number of CRL
Revoked Certificates		
	Serial Number	Serial number of certificate
	Revocation Date	Revocation date of certificate
CRL entry extensions		
	X509v3 CRL Reason Code	Reason of revocation

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 additional audits.

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 authority 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 Prices

Prices are governed by the certification authority's General Terms and Conditions (GT&C) applicable to the relevant service or by individual agreement.
Liability is determined in the relevant General Terms and Conditions (GT&C) of the certification authority. In individual cases, liability may also be agreed separately or set forth in an individual agreement.

9.2 Financial responsibilities

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

9.3 Confidentiality of business data

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 pertinent statutory provisions and other regulations concerning data protection.

9.4 Protection of personal data (data protection)

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.
As part of the data review, only the identity of the certificate holder 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 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 Liability limitations

The certification authority will have unlimited liability for damage arising out of 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 for the relevant service or by individual agreement.

9.7 Compensation

9.8 Entry into force and cancelation

9.9 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 on +49 (0) 1805 268 204 or via e-mail to telesec_support@t-systems.com.

9.10 Mutual notification and communication by subscribers

The subscribers communicate with each other.

9.11 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.
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.

9.11.1 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. Amendments enter into force immediately upon publication.

9.11.2 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.

9.12 Provisions on dispute resolution

Any disputes will be settled by the parties in due consideration of the concluded agreements, regulations and applicable laws.

9.13 Applicable law

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

10 Glossary

AICPA	American Institute of Certified Public Accountants
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	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.
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.
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 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	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.
Mail request	Variant of a certificate request where the data is transmitted to the certification authority by e-mail.
MitM	Man-in-the-Middle
OCSP	The Online Certificate Status Protocol makes it possible to query the validity of certificates online.
PIN	Personal Identification Number. Secret code as it is 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	Entirety 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.
RA	Registration Authority. See Registration Authority.

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 the digital signature and for the secure transmission of keys that is named after the three cryptographs 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., each 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 it used, a revocation list should be used to check whether it may still be used. Is also referred to as 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.
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. Certificates of version X.509v3 are supported in all common public key infrastructures.
Certificate	See digital certificate.

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 (Bundesdatenschutzgesetz), Federal Law Gazette (Bundesgesetzblatt) I 2003 p.66
[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
[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), BGB1 (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