



TC TrustCenter GmbH

Certification Practice Statement

Version 1.9.3 of January 27th, 2010

NOTE: The information contained in this document is the property of TC TrustCenter GmbH. This Certification Practice Statement is published in conformance with international practices (see [RFC3647]). This document may not be copied, distributed, used, stored or transmitted in any form or by any means, whether in part or as a whole, without the prior written consent of TC TrustCenter GmbH.

TABLE OF CONTENTS

1	Introduction.....	8
1.1	Overview.....	8
1.2	Document name and identification	9
1.3	PKI participants.....	10
1.3.1	Certification authorities.....	10
1.3.2	Registration authorities.....	11
1.3.3	Subscribers	13
1.3.4	Relying parties	13
1.3.5	Other participants.....	13
1.4	Certificate usage.....	14
1.4.1	Appropriate certificate uses	14
1.4.2	Prohibited certificate uses	14
1.5	Policy administration	14
1.5.1	Organization administering the document	14
1.5.2	Contact person.....	14
1.5.3	Person determining CPS suitability for the policy	14
1.5.4	CPS approval procedures	14
1.6	Definitions and Acronyms	14
2	Publication and Repository Responsibilities.....	15
2.1	Repositories.....	15
2.2	Publication of certification information	16
2.3	Time or frequency of publication	16
2.4	Access controls on repositories.....	16
3	Identification and Authentication	16
3.1	Naming	16
3.1.1	Types of names.....	16
3.1.2	Need for names to be meaningful.....	16
3.1.3	Anonymity or pseudonymity of subscribers	17
3.1.4	Rules for interpreting various name forms	17
3.1.5	Uniqueness of names.....	17
3.1.6	Recognition, authentication, and role of trademarks.....	17
3.1.7	Name claim dispute resolution procedure.....	17
3.2	Initial identity validation	17
3.2.1	Method to prove possession of private key.....	18
3.2.2	Authentication of organization identity	18
3.2.3	Authentication of individual identity.....	18
3.2.4	Non-verified subscriber information	19
3.2.5	Validation of authority.....	19
3.2.6	Criteria for interoperation.....	20
3.3	Identification and authentication for re-key requests	20
3.3.1	Identification and authentication for routine re-key	20
3.3.2	Identification and authentication for re-key after revocation	20
3.4	Identification and authentication for revocation request.....	20
4	Certificate Life-cycle Operational Requirements	20
4.1	Certificate Application	20
4.1.1	Who can submit a certificate application.....	21
4.1.2	Enrolment process and responsibilities	21
4.2	Certificate application processing.....	21
4.2.1	Performing identification and authentication functions	21
4.2.2	Approval or rejection of certificate applications.....	21
4.2.3	Time to process certificate applications.....	21

4.3	Certificate issuance.....	22
4.3.1	CA actions during certificate issuance.....	22
4.3.2	Notification to subscriber by the CA of issuance of certificate.....	22
4.4	Certificate acceptance.....	22
4.4.1	Conduct constituting certificate acceptance.....	22
4.4.2	Publication of the certificate by the CA.....	22
4.4.3	Notification of certificate issuance by the CA to other entities.....	23
4.5	Key pair and certificate usage.....	23
4.5.1	Subscriber private key and certificate usage.....	23
4.5.2	Relying party public key and certificate usage.....	23
4.6	Certificate renewal.....	23
4.6.1	Circumstance for certificate renewal.....	24
4.6.2	Who may request renewal.....	24
4.6.3	Processing certificate renewal requests.....	24
4.6.4	Notification of new certificate issuance to subscriber.....	24
4.6.5	Conduct constituting acceptance of a renewal certificate.....	24
4.6.6	Publication of the renewal certificate by the CA.....	24
4.6.7	Notification of certificate issuance by the CA to other entities.....	24
4.7	Certificate re-key.....	24
4.7.1	Circumstance for certificate re-key.....	24
4.7.2	Who may request certification of a new public key.....	25
4.7.3	Processing certificate re-keying requests.....	25
4.7.4	Notification of new certificate issuance to subscriber.....	25
4.7.5	Conduct constituting acceptance of a re-keyed certificate.....	25
4.7.6	Publication of the re-keyed certificate by the CA.....	25
4.7.7	Notification of certificate issuance by the CA to other entities.....	25
4.8	Certificate modification.....	25
4.8.1	Circumstance for certificate modification.....	25
4.8.2	Who may request certificate modification.....	26
4.8.3	Processing certificate modification requests.....	26
4.8.4	Conduct constituting acceptance of a modified certificate.....	26
4.8.5	Publication of the modified certificate by the CA.....	26
4.8.6	Notification of certificate issuance by the CA to other entities.....	26
4.9	Certificate revocation and suspension.....	26
4.9.1	Circumstances for revocation.....	26
4.9.2	Who can request revocation.....	27
4.9.3	Procedure for revocation request.....	27
4.9.4	Revocation request grace period.....	28
4.9.5	Time within which CA must process the revocation request.....	28
4.9.6	Revocation checking requirement for relying parties.....	28
4.9.7	CRL issuance frequency (if applicable).....	28
4.9.8	Maximum latency for CRLs (if applicable).....	29
4.9.9	On-line revocation/status checking availability.....	29
4.9.10	On-line revocation checking requirements.....	29
4.9.11	Other forms of revocation advertisements available.....	29
4.9.12	Special requirements re key compromise.....	29
4.9.13	Circumstances for suspension.....	29
4.9.14	Who can request suspension.....	29
4.9.15	Procedure for suspension request.....	30
4.9.16	Limits on suspension period.....	30
4.10	Certificate status services.....	30
4.10.1	Operational characteristics.....	30
4.10.2	Service availability.....	30
4.10.3	Optional features.....	30

TC TrustCenter's Certification Practice Statement

Version 1.9.3 of January 27th, 2010

4.11	End of subscription	30
4.12	Key escrow and recovery	30
4.12.1	Key escrow and recovery policy and practices	30
4.12.2	Session key encapsulation and recovery policy and practices.....	31
5	Facility, Management, and Operational Controls	31
5.1	Physical controls	31
5.1.1	Site location and construction.....	31
5.1.2	Physical access.....	31
5.1.3	Power and air conditioning	32
5.1.4	Water exposures	32
5.1.5	Fire prevention and protection.....	32
5.1.6	Media storage	32
5.1.7	Waste disposal.....	32
5.1.8	Off-site backup.....	32
5.2	Procedural controls	32
5.2.1	Trusted roles	33
5.2.2	Number of persons required per task	33
5.2.3	Identification and authentication for each role.....	33
5.2.4	Roles requiring separation of duties	33
5.3	Personnel controls	34
5.3.1	Qualifications, experience, and clearance requirements.....	34
5.3.2	Background check procedures	34
5.3.3	Training requirements	34
5.3.4	Retraining frequency and requirements.....	34
5.3.5	Job rotation frequency and sequence.....	35
5.3.6	Sanctions for unauthorized actions.....	35
5.3.7	Independent contractor requirements	35
5.3.8	Documentation supplied to personnel	35
5.4	Audit logging procedures	35
5.4.1	Types of events recorded.....	35
5.4.2	Frequency of processing log	35
5.4.3	Retention period for audit log	36
5.4.4	Protection of audit log.....	36
5.4.5	Audit log backup procedures	36
5.4.6	Audit collection system (internal vs. external).....	36
5.4.7	Notification to event-causing subject	36
5.4.8	Vulnerability assessments	36
5.5	Records archival	36
5.5.1	Types of records archived	37
5.5.2	Retention period for archive	37
5.5.3	Protection of archive.....	37
5.5.4	Archive backup procedures	37
5.5.5	Requirements for time-stamping of records.....	37
5.5.6	Archive collection system (internal or external).....	37
5.5.7	Procedures to obtain and verify archive information	38
5.6	Key changeover	38
5.7	Compromise and disaster recovery	38
5.7.1	Incident and compromise handling procedures	38
5.7.2	Computing resources, software, and/or data are corrupted	38
5.7.3	CA private key compromise procedures	38
5.7.4	Business continuity capabilities after a disaster.....	39
5.8	CA or RA termination	39
5.8.1	CA Termination	39
5.8.2	RA Termination	40

6	Technical Security Controls	40
6.1	Key pair generation and installation	40
6.1.1	Key pair generation	40
6.1.2	Private key delivery to subscriber	41
6.1.3	Public key delivery to certificate issuer	41
6.1.4	CA public key delivery to relying parties	42
6.1.5	Key sizes.....	42
6.1.6	Public key parameters generation and quality checking	42
6.1.7	Key usage purposes (as per X.509 v3 key usage field)	42
6.2	Private Key Protection and Cryptographic Module Engineering Controls	43
6.2.1	Cryptographic module standards and controls.....	43
6.2.2	Private key (n out of m) multi-person control	43
6.2.3	Private key escrow	43
6.2.4	Private key backup.....	43
6.2.5	Private key archival	44
6.2.6	Private key transfer into or from a cryptographic module	44
6.2.7	Private key storage on cryptographic module	44
6.2.8	Method of activating private key	44
6.2.9	Method of deactivating private key	44
6.2.10	Method of destroying private key.....	44
6.2.11	Cryptographic Module Rating	45
6.3	Other aspects of key pair management.....	45
6.3.1	Public key archival.....	45
6.3.2	Certificate operational periods and key pair usage periods.....	45
6.4	Activation data	45
6.4.1	Activation data generation and installation	45
6.4.2	Activation data protection	46
6.4.3	Other aspects of activation data	46
6.5	Computer security controls	46
6.5.1	Specific computer security technical requirements	47
6.5.2	Computer security rating	47
6.6	Life cycle technical controls	47
6.6.1	System development controls	47
6.6.2	Security management controls	48
6.6.3	Life cycle security controls.....	48
6.7	Network security controls	49
6.8	Time-stamping	49
7	Certificate, CRL, and OCSP Profiles.....	49
7.1	Certificate profile.....	49
7.1.1	Version number(s).....	49
7.1.2	Certificate extensions	49
7.1.3	Algorithm object identifiers	50
7.1.4	Name forms.....	50
7.1.5	Name constraints	52
7.1.6	Certificate policy object identifier	52
7.1.7	Usage of Policy Constraints extension	52
7.1.8	Policy qualifiers syntax and semantics	52
7.1.9	Processing semantics for the critical Certificate Policies extension	52
7.2	CRL profile.....	52
7.2.1	Version number(s).....	53
7.2.2	CRL and CRL entry extensions	53
7.3	OCSP profile.....	53
7.3.1	Version number(s).....	53
7.3.2	OCSP extensions.....	53

TC TrustCenter's Certification Practice Statement

Version 1.9.3 of January 27th, 2010

8	Compliance Audit and other Assessments.....	54
8.1	Frequency or circumstances of assessment	54
8.2	Identity/qualifications of assessor.....	54
8.3	Assessor's relationship to assessed entity	54
8.4	Topics covered by assessment.....	54
8.5	Actions taken as a result of deficiency	54
8.6	Communication of results.....	55
9	Other Business and Legal Matters.....	55
9.1	Fees.....	55
9.1.1	Certificate issuance or renewal fees.....	55
9.1.2	Certificate access fees	55
9.1.3	Revocation or status information access fees.....	55
9.1.4	Fees for other services.....	55
9.1.5	Refund policy	55
9.2	Financial responsibility	55
9.2.1	Insurance coverage.....	56
9.2.2	Other assets.....	56
9.2.3	Insurance or warranty coverage for end-entities.....	56
9.3	Confidentiality of business information	56
9.3.1	Scope of confidential information.....	56
9.3.2	Information not within the scope of confidential information.....	56
9.3.3	Responsibility to protect confidential information	56
9.4	Privacy of personal information	56
9.4.1	Privacy plan.....	56
9.4.2	Information treated as private.....	56
9.4.3	Information not deemed private.....	57
9.4.4	Responsibility to protect private information	57
9.4.5	Notice and consent to use private information	57
9.4.6	Disclosure pursuant to judicial or administrative process.....	57
9.4.7	Other information disclosure circumstances	57
9.5	Intellectual property rights	57
9.6	Representations and warranties.....	57
9.6.1	CA representations and warranties	57
9.6.2	RA representations and warranties	58
9.6.3	Subscriber representations and warranties	58
9.6.4	Relying party representations and warranties.....	58
9.6.5	Representations and warranties of other participants.....	59
9.7	Disclaimers of warranties	59
9.8	Limitations of liability	59
9.9	Indemnities	59
9.10	Term and termination.....	59
9.10.1	Term	59
9.10.2	Termination.....	60
9.10.3	Effect of termination and survival.....	60
9.11	Individual notices and communications with participants.....	60
9.12	Amendments.....	60
9.12.1	Procedure for amendment.....	60
9.12.2	Notification mechanism and period.....	61
9.12.3	Circumstances under which OID must be changed	61
9.13	Dispute resolution provisions	61
9.14	Governing law.....	61
9.15	Compliance with applicable law	61
9.16	Miscellaneous provisions	61
9.16.1	Entire agreement.....	61

TC TrustCenter's Certification Practice Statement
Version 1.9.3 of January 27th, 2010

- 9.16.2 Assignment61
- 9.16.3 Severability61
- 9.16.4 Enforcement (attorneys' fees and waiver of rights)61
- 9.16.5 Force Majeure62
- 9.17 Other provisions62
 - 9.17.1 Fiduciary relationships62
 - 9.17.2 Administrative processes62
- 10 References63
- 11 Glossary64

1 Introduction

1.1 Overview

Certificates are used with public key encryption, which is a technique where any participating entity has a key pair. One of these keys is private and must be kept secret; the other is public and is made available for retrieval from a public key directory, much like telephone numbers in a public phone book. Anything encrypted with the private key can only be decrypted with the corresponding public key (and vice versa). This can be used to implement digital signatures: The sender encrypts data using his private key, and any recipient is able to verify its integrity by using the corresponding public key available from a public key directory. The sender may also encrypt the data using the recipient's public key, ensuring that only the intended recipient is able to decrypt it using the corresponding private key.

A certificate is, in essence, a digitally signed public key. It always contains the name or another unequivocal reference to the holder of the corresponding private key, who is called the subscriber. Since anyone can create a public key with any given name, it is essential to verify that a certificate retrieved from a directory actually belongs to the subscriber named therein, because otherwise digital signatures might be forged and confidential data might be decrypted by unauthorized persons.

A Certification Authority acts as a trusted third party that binds certificates to the indicated entity. A certificate issued by a CA contains the subscriber's name, the name of the CA, the subscriber's public key, and is digitally signed by the CA.

TC TrustCenter offers several certificate classes that are described in the corresponding Certificate Policy Definitions (CPDs) and referenced in this CPS (see section 1.2), each indicating a different level of trust that may be placed in the reliability and strength of this bond by a relying party. This is also called the "assurance level" or "level of trust" of a certificate.

To allow an estimation of the trustworthiness of issued certificates a CA publishes a CPS which describes the procedures used for the issuance of certificates as well as a description how the verification of data contained in a certificate is performed.

A Certification Practice Statement is a statement of the practices which a Certification Authority (CA) employs in issuing certificates to a subscriber. This includes certificate application, use and revocation or suspension of certificates.

A Certificate Policy Definition (CPD) describes the vetting processes and allows estimation of the trustworthiness and reliability of the certificate contents based on the extent of the verification steps undertaken to verify the contents of the certificates.

TC TrustCenter's services are provided on the basis of TC TrustCenter's General Terms and Conditions on Digital Certificates (GTCDC), which are available from the repository.

This CPS describes the structure and practices of TC TrustCenter, in order to enable customers of TC TrustCenter to evaluate TC TrustCenter's services.

This CPS complies with the Internet Request for Comment (RFC) 3647.

This CPS supports all the types of certificates issued by TC TrustCenter (device certificates, individual certificates, certificates for teams, code signing certificates etc.) for all classes of certificates (i.e. TC Class 0 to TC Class 4).

This Certification Practice Statement in combination with TC TrustCenter's organization, processes, and procedures has been assessed by independent auditors to be compliant to the standard „ETSI TS 102 042 – Policy requirements for certification authorities issuing public key certificates“, Version 2.1.1 of the European Telecommunications Standards Institute (ETSI). All

certificates issued under TC TrustCenter's Class 2 Root or higher fulfill at least the requirements of the "Lightweight Certificate Policy" (LCP) of ETSI TS 102 042.

This CPS is not applicable to qualified certificates issued in compliance with the German Electronic Signature Act ([SIGG]). The Electronic Signature Act regulates the issuance of individual signature certificates only; it does not cover other types of certificates.

This CPS neither constitutes a declaration of self-escrow, nor does it state legally binding warranties. Any legally binding statements by TC TrustCenter are made in the General Terms and Conditions or in specific contracts between TC TrustCenter and other parties.

This CPS makes extensive use of the vocabulary related to the field of digital signatures and certificates, cryptography and public key encryption, which is referenced in the Definitions and Acronyms (Section 1.6) or in the Glossary (section 11). The glossary also provides the definition of some important terms not appearing elsewhere in this text that relate to the areas mentioned above.

1.2 Document name and identification

This CPS does not apply to certificates issued under the regulations of the German Digital Signature Act. For certificates issued in compliance with the German Digital Signature Act, so called "Qualified Certificates", TC TrustCenter uses a dedicated CPS, the "Certification Practice Statement and Certificate Policy for Qualified Certificates".

TC TrustCenter's Root and CA certificates are identifiable through their Subject Distinguished Name containing the Organization field "TC TrustCenter for Security in Data Networks GmbH" or "TC TrustCenter GmbH".

Except for the above mentioned Qualified Certificates this CPS applies to every certificate issued by TC TrustCenter regardless of whether this CPS is expressly listed in such a certificate. In particular, this CPS may not be listed in Root certificates.

This CPS also applies to TC TrustCenter's Universal Roots "TC TrustCenter Universal CA I" and "TC TrustCenter Universal CA II", though these Roots do not explicitly refer to a specific certificate class.

The assurance levels expressed in this CPS are TC Class 0 to TC Class 4 as defined in this CPS and in TC TrustCenter's CPDs.

The policies OIDs are registered in the Internet Assigned Numbers Authority (IANA) Objects Registry using the following structure, where the variable x denotes the certificate class x:

```
{ TC TrustCenter (1.2.276.0.44) policies (1) certificate-policies (1) customer-policies (1)
  tc_lot_x_ca(x) }
```

This CPS supports the following OIDs:

Class 0: (1.2.276.0.44.1.1.1.0)

Class 1: (1.2.276.0.44.1.1.1.1)

Class 2: (1.2.276.0.44.1.1.1.2)

Class 3: (1.2.276.0.44.1.1.1.3)

Class 4: (1.2.276.0.44.1.1.1.4)

If a certificate issued by TC TrustCenter asserts one or more of these OIDs it does so in one of the following ways:

- 1) By listing one of the object identifiers of this CPS (see below) in the *certificatePolicies* field, as defined in section 4.2.1.5 of [RFC 3280]

2) By listing the URL of the applicable version of this CPS in the certificate's *cpsURI* subfield of its *certificatePolicies* field, as defined in section 4.2.1.5 of [RFC 3280].

1.3 PKI participants

1.3.1 Certification Authorities

A PKI Root is a special type of CA. A Root serves as a trust anchor for a PKI and its associated CAs by issuing certificates to these (subordinate) CAs. In general, the Root of a PKI is self signed but it may be cross certified with other Roots or CAs.

TC TrustCenter operates several Certification Authorities. It provides certification services for external third parties and issues certificates under its own certificate policies. TC TrustCenter also issues qualified certificates in compliance with the German Electronic Signature Act. TC TrustCenter provides information about other subsidiary or cooperating CAs upon request.

TC TrustCenter's Certification Authorities are organized in a hierarchical structure, i.e. CAs may issue certificates to other certificate issuing entities. Such a Subordinate CA (Sub-CA) must at a minimum fulfill the requirements of the superior CA. This applies especially to the requirements on identification and authentication: when registering applicants, Sub-CAs are allowed to perform additional or more extensive checks than the superior CA; they must not drop below the requirements of the respective superior CA.

Where this CPS refers to a "CA," that term shall be interpreted as TC TrustCenter's Root CAs, and TC TrustCenter's CAs. TC TrustCenter's CAs are issued by one of TC TrustCenter's Roots. Where this CPS refers to a "Root CA," that term shall be interpreted as one of TC TrustCenter's Root CAs.

Currently TC TrustCenter's Root Certificates are:

TC Class 0:

Common Name (CN)	<Empty>
OrganizationName (O)	TC TrustCenter AG
Organizational Unit (OU)	TC TrustCenter Class 0 CA
CountryName (C)	DE
SerialNumber (SN)	00 ad 55 00 00 00 02 b7 f9 b8 f4 f3 12 34 af

TC Class 1:

Common Name (CN)	<Empty>
OrganizationName (O)	TC TrustCenter for Security in Data Networks GmbH
Organizational Unit (OU)	TC TrustCenter Class 1 CA
CountryName (C)	DE
SerialNumber (SN)	03:E9

TC Class 2:

Common Name (CN)	<Empty>
OrganizationName (O)	TC TrustCenter for Security in Data Networks GmbH
Organizational Unit (OU)	TC TrustCenter Class 2 CA
CountryName (C)	DE
SerialNumber (SN)	03:EA
Common Name (CN)	TC TrustCenter Class 2 CA II
OrganizationName (O)	TC TrustCenter GmbH
Organizational Unit (OU)	TC TrustCenter Class 2 CA
CountryName (C)	DE
SerialNumber (SN)	2E:6A:00:01:00:02:1F:D7:52:21:2C:11:5C:3B

TC TrustCenter's Certification Practice Statement

Version 1.9.3 of January 27th, 2010

TC Class 3:

Common Name (CN)	<Empty>
OrganizationName (O)	TC TrustCenter for Security in Data Networks GmbH
Organizational Unit (OU)	TC TrustCenter Class 3 CA
CountryName (C)	DE
SerialNumber (SN)	03:EB
Common Name (CN)	TC TrustCenter Class 3 CA II
OrganizationName (O)	TC TrustCenter GmbH
Organizational Unit (OU)	TC TrustCenter Class 3 CA
CountryName (C)	DE
SerialNumber (SN)	4A:47:00:01:00:02:E5:A0:5D:D6:3F:00:51:BF

TC Class 4:

Common Name (CN)	<Empty>
OrganizationName (O)	TC TrustCenter for Security in Data Networks GmbH
Organizational Unit (OU)	TC TrustCenter Class 4 CA
CountryName (C)	DE
SerialNumber (SN)	03:EC
Common Name (CN)	TC TrustCenter Class 4 CA II
OrganizationName (O)	TC TrustCenter GmbH
Organizational Unit (OU)	TC TrustCenter Class 4 CA
CountryName (C)	DE
SerialNumber (SN)	05:C0:00:01:00:02:41:D0:06:0A:4D:CE:75:10

TC TrustCenter Universal CA I

Common Name (CN)	TC TrustCenter Universal CA I
OrganizationName (O)	TC TrustCenter GmbH
Organizational Unit (OU)	TC TrustCenter Universal CA
CountryName (C)	DE
SerialNumber (SN)	1D:A2:00:01:00:02:EC:B7:60:80:78:8D:B6:06

TC TrustCenter Universal CA II

Common Name (CN)	TC TrustCenter Universal CA II
OrganizationName (O)	TC TrustCenter GmbH
Organizational Unit (OU)	TC TrustCenter Universal CA
CountryName (C)	DE
SerialNumber (SN)	19:33:00:01:00:02:28:1A:9A:04:BC:F2:55:45

TC TrustCenter Universal CA III

Common Name (CN)	TC TrustCenter Universal CA III
OrganizationName (O)	TC TrustCenter GmbH
Organizational Unit (OU)	TC TrustCenter Universal CA
CountryName (C)	DE
SerialNumber (SN)	63:25:00:01:00:02:14:8d:33:15:02:e4:6c:f4

This CPS does not explicitly list all of TC TrustCenter's CAs. New CAs may be added or existing CAs may be terminated; and it is not intended to modify this CPS whenever a CA is added or terminated.

A current list of TC TrustCenter's Roots and CAs can be found at TC TrustCenter's website: http://www.trustcenter.de/infocenter/root_certificates.htm

1.3.2 Registration Authorities

A Registration Authority (RA) works on behalf of a CA. TC TrustCenter operates an in-house Registration Authority but may also make use of external service providers as subsidiary RAs

responsible for verifying both business information and personal data contained in a subscriber's certificate.

Any subsidiary RA is contractually bound to TC TrustCenter. A subsidiary RA is registered as registration service provider. The Registration Officers of such a subsidiary RA are individually identified; they are equipped with special Registration Officer (RO) certificates. Only data signed by an RA is accepted by the CA system.

An RA is responsible for registering applicants. It performs identity proofing and the verification of all certificate data.

In particular the tasks of an RA are:

- Forwarding checked and complete data for Certificate issuance, suspension, termination of suspension and revocation to the CA
- Identification and authentication of subjects and subscribers
- Handing over smart cards to applicants and activating certificates
- Tracking logistics of certificate lifecycle.
- Validation of suspension and revocation requests.

Personal identification of applicants for a certificate may take place at any of the subsidiary RAs used for this purpose. Mobile RA Officers may identify and authenticate persons at the customer's premises.

An RA must not use the private RA keys for any other purpose than those associated with its RA function. An RA must comply with the provisions in this CPS; this includes, but is not limited to: ensuring that the requirements and controls specified in section 5 and section 6 are provided; keeping subscriber information confidential according to sections 9.3 and 9.4; and performing the authentication procedure as defined in section 3.2 of this CPS, TC TrustCenter's CPDs, and TC TrustCenter's RA guidelines. TC TrustCenter's RA guidelines are for internal use only; these guidelines will not be published.

Any RA must have properly qualified and trustworthy employees that are authorized to perform the RA duties. The workstation used for submitting registration information to the CA system must not be publicly accessible. For external RAs the communication via insecure channels must be properly protected.

TC TrustCenter reserves the right to prohibit performing RA services on behalf of TC TrustCenter, if an RA does not conform to the provisions set forth in this CPS.

Personal identification of end users applying for a certificate may take place at TC TrustCenter or at any of the subsidiary RAs used for this purpose. The latter fall into one of three categories: (1) TC TrustCenter IdentPoints[®], or (2) German Post Offices, or (3) authorized identification points in organizations.

A TC TrustCenter IdentPoint[®] provides the service of personal identification on behalf of TC TrustCenter. This results in more efficient handling of end user registration. The German Post offices offer their identification service to different companies, most notably banks. Identification points in organizations may be installed if an organization operates an internal PKI which issues certificates only to members of that organization.

TC TrustCenter may also authorize individual persons to act as representatives of TC TrustCenter. These representatives, called "Trusted Agents" are then authorized to perform the identity verification.

1.3.3 Subscribers

In the context of this document, end entity (or end user) is a synonym for subscriber (or person). It refers to natural persons and legal entities which are able to perform legal acts, and who use certificates issued by TC TrustCenter.

In addition, end users may also be groups of persons or technical devices.

1.3.4 Relying Parties

A Relying Party uses a Subscriber's Certificate to verify the integrity of a digitally signed message, to identify the creator of a message, to authenticate a Subscriber, or to establish confidential communications with the Subscriber.

1.3.5 Other participants

TC TrustCenter may require the services of other security, community, and application authorities. This section of the CPS identifies the parties, defines the services, and designates the mechanisms used to support these services. Examples of other participants include Trusted Agents (TAs), Machine Operators, and Local Registration Authorities (LRA).

1.3.5.1 TC TrustCenter's Policies and Practices Board (PPB)

TC TrustCenter's Policies and Practices Board consists of a group of TC TrustCenter executives and has the responsibility for review, maintenance, clarification, approval, and updates to this CPS.

TC TrustCenter's PPB is responsible for the approval of this CPS for the CAs asserting policy OIDs identified in section 1.2 of this CPS.

TC TrustCenter's PPB is also responsible for the approval of cross-certifications with other CAs.

1.3.5.2 Local Registration Authority (LRA)

The duties of a LRA are similar to the duties of the RA. The LRA may service a limited population (e.g. an organization) as authorized by the RA. An LRA collects and verifies each end entities' identity and information for inclusion in the certificate. The requirements for LRAs are set forth in this document.

Any LRA must be contractually bound to its CA. The CA registers any LRA as local registration service provider. These LRAs are equipped with special Registration Officer (RO) certificates. Only data signed by one of the RO certificates is accepted by the CA system.

1.3.5.3 Trusted Agent (TA)

The TA collects and verifies an applicant's identity in support of the subscriber registration. The TA works closely with an RA or LRA to support registration of applicants. The requirements for TAs are set forth elsewhere in this document.

1.3.5.4 Machine Operator

A Machine Operator serves as the representative of a technical device to an RA or LRA in order to register the technical device.

1.3.5.5 Centralized Credential Server (CCS)

If the private keys for multiple subscribers are stored on a single system, such a system is called a "Centralized Credential Server", or "CCS". A CCS must be based on either a hardware security module (HSM) interfaced to a server, or a software-protected set of private keys in a controlled server environment. A CCS permits the subscribers to access their credentials from multiple

workstations and locations. For the purposes of this CPS, any centralized aggregation of subscriber private keys must comply with the requirements for a CCS as specified in this CPS.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Except for the provisions applying to the different assurance levels (see section 3.2.3), this CPS supports all applications in the areas of electronic commerce and secure Internet or Intranet communication that are suitable for using digital certificates.

1.4.2 Prohibited certificate uses

TC TrustCenter does not prohibit certain uses of certificates as long as they are in compliance with the applicable provisions of a respective agreement with TC TrustCenter. Moreover, it is in the sole responsibility of each Subscriber and/or End User to use certificates in compliance with any and all laws and provisions applicable in the respective jurisdiction.

Certificates must not be used for signatures or authentication after expiry or revocation.

SSL certificates must not be installed on systems with a visible name that differs from the name in the certificate.

1.5 Policy administration

1.5.1 Organization administering the document

This CPS is administered by TC TrustCenter's Policies and Practices Board.

1.5.2 Contact person

Certification Practice Administrator
TC TrustCenter GmbH
Sonninstrasse 24-28
20097 Hamburg
Germany
Phone: +49 (0)40 808026-0
Fax: +49 (0)40 808026-126
E-Mail: certificate@trustcenter.de

1.5.3 Person determining CPS suitability for the policy

TC TrustCenter's Policies and Practices Board consisting of TC TrustCenter executives determines the CPS's suitability.

1.5.4 CPS approval procedures

This CPS, the Certificate Policy Definitions and the General Terms and Conditions on Digital Certificates are under continuous review by the TC TrustCenter Policies and Practices Board and are approved before being published in the repository.

1.6 Definitions and Acronyms

This section addresses some of the acronyms and abbreviations used in this CPS.

CA	Certification Authority
CRL	Certificate Revocation List

DN	Distinguished Name
DSS	Digital Signature Standard
EU	European Union
FIPS PUB	(US) Federal Information Processing Standard Publication
GTCDG	General Terms and Conditions on Digital Certificates
http	Hypertext Transfer Protocol
https	SSL for http
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LRA	Local Registration Authority
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKIX	Public Key Infrastructure X.509
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
SSL	Secure Sockets Layer
TA	Trusted Agent
TLS	Transport Layer Security
UPS	Uninterruptable Power Supply
URL	Uniform Resource Locator
WWW	World Wide Web

2 Publication and Repository Responsibilities

Because root certificates and CA certificates are important reference points for verifying the authenticity of other certificates (see section 1.3.1), it is important that they are available throughout the public key infrastructure(s) that TC TrustCenter provides to participants.

2.1 Repositories

TC TrustCenter's roots and CAs operate repositories to support their PKI operations.

TC TrustCenter ensures interoperability with common standards so that Relying Parties may obtain certificates and CRLs from or through that repository.

The repository shall be available as required by the certificate information posting and retrieval stipulations of this CPS.

Certificate and revocation status information is publicly and internationally available 24 hours per day, 7 days per week. Upon system failure, service, or other factors which are not under the control of TC TrustCenter, TC TrustCenter makes best efforts to ensure that the revocation status service is not unavailable for longer than inevitable.

Certificate and revocation status information is available from TC TrustCenter for at least as long as the certificate's expiry date indicates.

2.2 Publication of certification information

TC TrustCenter publishes this CPS, the Certification Policy Definitions, and the GTCDC in its repository at <http://www.trustcenter.de/repository>. The directory of all certificates issued by TC TrustCenter and TC TrustCenter's issuer (including root) certificates, which may also be used for on-line certificate status inquiries, is accessible from the repository as well. The Certificate Revocation Lists are available from <http://www.trustcenter.de/crl>. TC TrustCenter may also offer an OSCP service for certificate status requests.

2.3 Time or frequency of publication

This CPS and any subsequent changes are made publicly available within one week of approval.

The CRLs are updated at least daily. Details can be found in section 4.9.7. The certificate database is updated every time a certificate is issued. Any other information listed in section 2.2 is updated every time it is modified.

2.4 Access controls on repositories

TC TrustCenter protects the integrity and authenticity of all systems providing certificate status information. The repository is subject to access control mechanisms to protect its availability and information as described in later sections.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

All names specified in X.509 certificates must be expressed as non-null subject Distinguished Names (DNs) complying with the X.500 standard. Details may be found in the certificate profiles set forth later in this CPS.

Certificate names in other formats (such as WTLS certificates) should follow the X.509 conventions for specifying a meaningful name.

The applicable CPDs provide examples for proper certificate names.

3.1.2 Need for names to be meaningful

Names used in the certificates shall identify the person or technical device to which they are assigned.

When DN's are used, the common name shall observe name space uniqueness requirements.

Names shall never be misleading. This does not preclude the use of pseudonymous Certificates as defined in section 3.1.3.

If the subscriber's key pair is generated by TC TrustCenter or one of its cooperating CAs (see section 6.1), TC TrustCenter will determine the subscriber's DN to make it compliant with common standards, practices, and other regulations.

If the subscriber generates his own key pair, the subscriber should choose names to be meaningful; i. e. the name form should have commonly understood semantics (first and last name, company's name, Internet e-mail address) for the relying party to determine identity of the person and / or organization. TC TrustCenter will check subscriber DN's for compliance with common standards, practices, and other regulations, and may, at its own discretion, alter a subscriber DN accordingly.

Names shall never be misleading. This does not preclude the use of pseudonymous certificates as defined in Section 3.1.3.

Please check the applicable CPD for examples.

This section does not apply to TC Class 0 certificates. Class 0 certificates are intended to be used for testing and demonstration purposes; their content is not verified in any way (see section 3.2.3). Therefore, TC TrustCenter can not guarantee that the content of a Class 0 certificate adheres to the requirements of this section.

3.1.3 Anonymity or pseudonymity of subscribers

TC TrustCenter does not issue anonymous certificates. TC TrustCenter may issue pseudonymous certificates to its subscribers to support their operations. However, it is required that the CN of a pseudonymous certificate is an unambiguous name uniquely identifying the subject in the records of TC TrustCenter. Such a name may not be meaningful to anyone but TC TrustCenter and the subscriber.

TC TrustCenter will usually add a suffix to pseudonymous certificates (e.g. “:PN”) to distinguish pseudonymous certificates from other certificates.

3.1.4 Rules for interpreting various name forms

Any X.509 certificate issued for private use will have empty Organization and Organizational Unit fields. If one (or both) of these fields are present, the certificate is either intended for commercial use or sponsored by that organization.

Accordingly, any certificate in any other format, such as WTLS, containing an organization's name (except for e-mail addresses) is intended for commercial use or sponsored by that organization.

3.1.5 Uniqueness of names

Any subscriber DN in a X.509 certificate issued by TC TrustCenter must uniquely identify a single entity among all of TC TrustCenter's subscribers. If necessary, TC TrustCenter may append additional numbers or letters to an actual name in order to ensure the name's uniqueness. The same entity may have different certificates all bearing the same subject DN, but no two separate entities may share a common DN (and be issued by the same CA). In any case, there must not be two X.509 certificates having the same issuer DN and serial number.

The same holds true for other certificate formats, such as WTLS certificates.

3.1.6 Recognition, authentication, and role of trademarks

TC TrustCenter will honor trademark claims that are documented by a subscriber.

TC TrustCenter will make reasonable efforts to resolve any name collisions or disputes regarding certificates brought to its attention. Any dispute resolution shall be in accordance with section 3.1.7.

3.1.7 Name claim dispute resolution procedure

TC TrustCenter shall not be responsible for resolving name claim disputes among subscribers. TC TrustCenter's CAs may add, at their own discretion, additional information to a name in order to make it unique among the names of certificates issued by the CAs covered under this CPS.

3.2 Initial identity validation

In order to obtain a certificate, any applicant must apply for a certificate, and identify and authenticate themselves to TC TrustCenter.

TrustCenter groups the certificates into "certificate classes". The higher the certificate class, the more extensive are the identification verifications that are being used as a basis for the issuance of the certificate. The certificates themselves contain information regarding the class of the certificate for anyone who wishes to rely on the certificate.

Within the context of classification into certificate classes a distinction is made between individuals and organizations.

Certificates for individuals who do not provide information about their affiliation to an organization do not contain statements about the subject's organizational affiliation.

Organizational certificates always contain a statement regarding an organization. These certificates may either be attributed to an organization (such as device certificates which cannot be attributed to natural persons) or they may be attributed to a member of an organization, such as an employee of a company. Information about an organization must be entered into all organizational certificates.

Certificates not containing the name of an individual person (e.g. SSL certificates containing the full qualified domain name of a web server or Team-certificates identifying a group of persons) are always assigned to an organization.

This section covers these topics in a general fashion. Please see the Certificate Policy Definitions (CPDs) for further details.

3.2.1 Method to prove possession of private key

In order to prove a subscriber's possession of the private key corresponding to the public key contained in a certificate application, any certificate request submitted as part of a certificate application must be self-signed.

3.2.2 Authentication of organization identity

A corporate organizational entity must provide a proof of its existence. This verification may be carried out by the presentation of a document, which proves the existence of the organization (current extract of a competent official register in which the organization is listed or a comparable document). For Class 2 certificates copies of such documents are sufficient, Class 3 and above require the presentation of original documents or notarized copies. Further details, especially additional requirements on the validity of such documents can be found in TC TrustCenter's CPDs for the certificate class under consideration.

Alternatively, data provided by reputable third party vendors of business information will be accepted as well.

Governmental or administrative authorities must supply documents which reflect their relationship to the next higher entity (e.g. a superior authority) with official letterhead, stamped with an official stamp or seal, and signed by an authorized officer.

Other organizational entities must provide proper proof of existence/registration that is comparable to the above.

3.2.3 Authentication of individual identity

The authentication of an individual entity depends on the certificate class.

Class 0: These certificates are issued for testing and demonstration purposes. They are valid for a short period of time only. Data contained in a Class 0 certificate is not verified by TC TrustCenter in any way!

Class 1: These certificates always contain an e-mail address. They confirm that the e-mail address stated in the certificate existed at the time of application and that the owner of the public

key had access to this e-mail address. Class 1 certificates provide very little evidence of the identity of the certificate holder. Except from the existence and the accessibility of the e-mail address, no data contained in the certificate is being checked.

Class 2: These certificates contain data about the certificate owner. E-mail addresses are verified in the same way as for class 1 certificates. To verify the correctness of additional data contained in a class 2 certificate (e.g. name and affiliation) the applicant must present copies of documents proving the correctness of this data.

Class 3: These certificates may contain the same data as class 2 certificates. E-mail addresses are verified in the same way as for class 1 certificates. To verify the correctness of additional data contained in a class 3 certificate (e.g. name and affiliation) the applicant must present original documents proving the correctness of this data. Original documents may be replaced by notarized copies.

Class 4: These certificates are issued based on the requirements of Extended Validation Certificates: Guidelines for the Issuance and Management of Extended Validation certificates, Version 1.1, CA/Browser Forum, <http://www.cabforum.org>.

TC TrustCenter will not issue EV Certificates before having undergone and passed an annual

- (i) WebTrust Program for CAs audit and
- (ii) WebTrust EV Program audit, or
- (iii) an equivalent audit for both (i) and (ii) as approved by the CA/Browser Forum.

TC TrustCenter's CPDs define the authentication of individual entities in more detail. The CPDs can be found at <http://www.trustcenter.de/cpd>.

3.2.4 Non-verified subscriber information

Class 0 certificates are issued for testing and demonstration purposes. They are valid for a short period of time only. Data contained in a Class 0 certificate is not verified by TC TrustCenter in any way!

Class 1 certificates always contain an e-mail address. They confirm that the e-mail address stated in the certificate existed at the time of application and that the owner of the public key had access to this e-mail address. Class 1 certificates provide very little evidence of the identity of the certificate holder. Except from the existence and the accessibility of the e-mail address, none of the data contained in the certificate has been verified.

Information that is not verified will not be included in TC Class 2, TC Class 3, and TC Class 4 certificates.

Information about subscriber's internal details (e.g. name of Organizational Unit (OU in the Distinguished Name of the certificate) must be provided by the applicant and has to be approved by the organization. Verification of the OU through a third party is not performed.

3.2.5 Validation of authority

TC Class 2, TC Class 3, and TC Class 4 certificates that contain explicit or implicit information about the applicant's affiliation are issued only after ascertaining that the applicant has the authorization to act on behalf of the organization in the asserted capacity.

There is no validation of authority for TC Class 0 and TC Class 1 certificates.

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

Re-key means changing the public key for an existing certificate by issuing a new certificate with a *different* (usually new) public key. The certificate name stays the same. It is different from renewal, which means issuing a new certificate, with an extended validity period, for the *same* public key. (See [RFC2828].)

Certificate re-key may be performed in case the existing key can no longer be used. Examples are:

- The key is compromised and the certificate has to be revoked,
- The existing certificate has expired.

Re-key is possible for all types of certificates.

3.3.1 Identification and authentication for routine re-key

Subscribers shall identify themselves through the use of their current signing key whose certificate has not yet expired or by using the initial identity-proofing process described above.

3.3.2 Identification and authentication for re-key after revocation

After a certificate has been revoked, the subscriber must generate a new key pair and re-apply for a new certificate in accordance with section 3.2, since the revoked key pair is ineligible to sign and authenticate a rekey request (see section 3.3.1).

3.4 Identification and authentication for revocation request

Revocation requests shall be authenticated.

There are several ways to submit a revocation request:

1. If the subscriber is still in possession of the private key, requests to revoke a certificate may be signed using the private key and authenticated using that certificate's public key, regardless of whether or not the associated private key is compromised.
2. If the private key has been lost or is inaccessible for any reason, the subscriber or an authorized representative may call TC TrustCenter or the responsible RA by phone and authenticate by using a revocation password chosen when submitting the initial certificate application. Revocation passwords may not be supported for all types of certificates.
3. The subscriber may request the certificate to be revoked by writing a letter to TC TrustCenter stating this request. Authentication is then provided by the subscriber's signature.
4. Other methods for revocation may be agreed upon.

4 Certificate Life-cycle Operational Requirements

4.1 Certificate Application

TC TrustCenter provides an online interface for certificate applications. The website for online applications is available 24 hours a day, 7 days a week.

A subscriber fills out the online application form and submits this certificate application to TC TrustCenter. During the online application the subscriber follows the procedure described in this CPS or in TC TrustCenter Certificate Policy Definitions:

- complete a certificate application and provide the required information

- generate a key pair in accordance with 6.1.1,
- deliver the public key to TC TrustCenter in accordance with section 6.1.3,
- demonstrate pursuant to CPS section 3.2.1 possession of the private key corresponding to the public key delivered to TC TrustCenter.

Completed certificate applications are then submitted to TC TrustCenter for processing, the result being either approval or denial.

4.1.1 Who can submit a certificate application

Generally, there is no restriction on a certificate application. However, TC TrustCenter will make reasonable efforts to exclude persons and organizations listed on denied persons list in the EU and/or the U.S. and/or applicants from respective embargo countries from the certification process.

4.1.2 Enrolment process and responsibilities

When applying for a certificate the applicants are responsible for providing accurate information in their application for certification.

After receiving the application TC TrustCenter checks the application for errors and omissions.

TC TrustCenter then initiates the identification and authentication process as described in section 3.2.

Pursuant to section 3.2.1, the TC TrustCenter performs the proof of possession of the private key (e.g., verify digital signature on the self-signed certificate request) and performs the authentication of the applicant as described in sections 3.2.2, 3.2.3, and 3.2.5 as applicable.

4.2 Certificate application processing

Having received an application TC TrustCenter begins to process the application. This includes the verification of accuracy and correctness of all relevant data.

4.2.1 Performing identification and authentication functions

The identity-proofing for subscribers must meet the requirements specified in this CPS as specified in sections 3.2 and 3.3, as applicable.

Only TC TrustCenter's in-house RA, an associated LRA, a TC TrustCenter IdentPoint, or a Trusted Agent as defined in section 1.3.2 is authorized to perform identity-proofing for TC TrustCenter's CAs.

4.2.2 Approval or rejection of certificate applications

TC TrustCenter will either approve the application and issue a certificate upon successful completion of the identity-proofing process or reject the application and inform the applicant about any problems or inconsistencies.

If in doubt LRAs, IdentPoints, and Trusted Agents may contact TC TrustCenter's internal RA.

If TC TrustCenter's internal RA is in doubt it may have to contact TC TrustCenter's Policies and Practices Board which will then accept or reject the application in question.

4.2.3 Time to process certificate applications

Maximum process times can be agreed upon by entering into service level agreements. Customers without service level agreement may not claim for a maximum process time.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

TC TrustCenter verifies, as set forth in section 3.2.1, that the applicant is in possession of the private key and that the certificate request has the proper contents, for example a server certificate request must state the fully qualified server and domain name in the "Common Name" field.

TC TrustCenter verifies the data contained in the request according to this CPS and according to the applicable CPD.

TC TrustCenter's CAs generate certificates using the appropriate certificate format, and set validity periods and extension fields in accordance with relevant standards, such as X.509. Certificates are checked to ensure that all fields and extensions are properly populated.

For certificate renewals, CAs generate and sign a new instance of the certificate, differing from the previous certificate only by the validity period.

End entity certificates have a validity period of no more than five years from the date of issuance.

After generation, verification, and acceptance, TC TrustCenter's CAs post the certificate as set forth in section 4.4.2 and publish it in the repository.

4.3.2 Notification to subscriber by the CA of issuance of certificate

TC TrustCenter's CAs either issue the subscriber's certificate upon successful completion of the vetting process and notifies the subscriber about the issuance of the certificate, or informs the subscriber about any problems or inconsistencies.

After a certificate has been issued TC TrustCenter informs the subscriber that the certificate is available and notifies the subscriber about the means for obtaining the certificate.

Certificates are made available to subscribers either by allowing them to download the certificates from a web site or via a message containing the certificate. For example, TC TrustCenter may send an URL describing where the subscriber can obtain the certificate. The certificate may also be sent to the subscriber in an e-mail message.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Downloading a certificate or installing a certificate from a message constitutes the subscriber's reception of the certificate.

Usage of the private key and the corresponding certificate by the subscriber is deemed to be acceptance of the certificate. It is then usable in any application requiring the use of a digital certificate of that type and available from the certificate repository for verification.

By accepting a certificate the subscriber warrants that all information provided by the subscriber (and by its organization, where applicable) that is included in the certificate, and all representations made by the subscriber (and by its organization, where applicable) as part of the application and identification process, are true and not misleading.

4.4.2 Publication of the certificate by the CA

As specified in section 2.2, TC TrustCenter publishes validation information for issued certificates in a publicly accessible repository immediately after certificate issuance. This includes TC TrustCenter's CA certificates and Root certificates.

Certificates may be made available for retrieval from TC TrustCenter's certificate repository by third parties only if the subscriber has declared his consent.

4.4.3 Notification of certificate issuance by the CA to other entities

There is no explicit notification to other entities. Certificates are published as specified in section 4.4.2.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers shall protect their private keys from access by any other party. Subscribers' private keys shall be protected in accordance with common best practices.

Certificates issued under the terms of this CPS may be used with all applications in the areas of electronic commerce and secure Internet and Intranet communication.

If applicable, restrictions for the use of certificates are defined in subscriber agreements.

4.5.2 Relying party public key and certificate usage

Certificates may specify restrictions on use through certificate extensions. Certificates issued under this CPS conform to the profiles provided in this CPS.

TC TrustCenter's CAs issue information specifying the current status of all unexpired certificates.

Relying Parties must process and comply with this information (e.g., CRL, OCSP responses) before relying on a certificate.

4.6 Certificate renewal

Certificate renewal consists of issuing a new certificate with a new validity period and a new serial number while retaining all other information in the original certificate including the public key.

Certificate renewal is permitted for certificates issued to physical devices, e.g. for SSL certificates. A simplified certificate renewal process (i.e. without re-submitting the public key) is not supported for certificates issued to natural persons.

Certificate renewal by re-using the subscriber's asymmetric key pair is only allowed in the case where the subscriber's key is not comprised.

Certificate renewal is also permitted for the CA certificates.

The subscriber must submit an authenticated renewal request (i. e., using the private key that corresponds to the certificate that is to be renewed). The subscriber's certificate request must include at least the subscriber's distinguished name, the serial number of the certificate (or other information that identifies the certificate), and the requested validity period. TC TrustCenter processes the request data to verify the identity of the requesting entity and identify the certificate to be renewed.

The Certificate Policy Definitions or contractual agreements may provide stipulations that differ from these general provisions, depending on the certificate class that the certificate was issued under. In particular, TC TrustCenter may stipulate, and reserves the right to demand, that the subscriber is re-registered in accordance with section 3.2.

4.6.1 Circumstance for certificate renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, the subject name and attributes are unchanged, and the subscriber meets the identity proofing requirements specified in Section 3.3.1.

In addition, the validity period of the certificate must not exceed the remaining lifetime of the private key, as specified in sections 4.3.1 and 6.3.2.

4.6.2 Who may request renewal

The subscriber may request renewal of its certificate.

Machine Operators for physical devices may request renewal of machine certificates.

4.6.3 Processing certificate renewal requests

One of TC TrustCenter's RAs or LRAs has to approve certificate renewal.

In all cases, the certificate renewal identity-proofing shall be achieved using one of the following processes:

- Initial registration process as described in section 3.2 or
- Identification and authentication for re-key as described in section 3.3, except the old key can also be used as the new key.

4.6.4 Notification of new certificate issuance to subscriber

Identical to section 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

Identical to section 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

Identical to section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

Identical to section 4.4.3.

4.7 Certificate re-key

Re-keying a certificate consists of creating new certificates with a different public key (and different serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-key is possible for all types of certificates.

4.7.1 Circumstance for certificate re-key

CA certificate re-key may be performed in the case where the existing key can no longer be used. Examples are:

- The key is compromised and the certificate has to be revoked,
- The existing certificate has expired.

A CA may issue a new certificate to the subscriber when the subscriber has generated a new key pair and is entitled to a certificate in accordance with this CPS.

4.7.2 Who may request certification of a new public key

A CA may request re-key of its certificate.

The end-user subscriber (including RA and LRA) or the Machine Operator for a technical device (as applicable) may request re-key of their respective certificates.

4.7.3 Processing certificate re-keying requests

Processing of CA certificate rekey is identical to the process used for the initial application.

For all other certificates certificate re-key identity-proofing is achieved using one of the following processes:

- Initial registration process as described in section 3.2; or
- Identity-proofing for re-key as described in section 3.3.

4.7.4 Notification of new certificate issuance to subscriber

Identical to section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Identical to section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

Identical to section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

Identical to section 4.4.3.

4.8 Certificate modification

Modifying a certificate means creating a new certificate that has the same or a different subject public key and a different serial number, and the new certificate differs in one or more other fields related to the subject (e.g., subject e-mail address in the subject alternative name field), from the old certificate. The old certificate shall not be further re-keyed, renewed, or updated. The old certificate shall be revoked if the subscriber no longer holds one or more of the affiliations explicitly stated in the old certificate.

A RA or other designated agent (as set forth previously) must verify the new updated information in the certificate. For example, if an individual's name changes (e.g., due to marriage), then the proof of the name change shall be validated by an LRA/RA or TA.

The validation process shall be identical to the identity-proofing in section 3.2.

The RA, LRA, or Trusted Agent must securely notify the CA and confirm the validation result prior to the issuance of the modified certificate.

4.8.1 Circumstance for certificate modification

A CA may issue a new certificate to a subscriber when some of the information in the certificate has changed, e.g., name change due to change in marital status, change in subject attributes, etc., and the subscriber continues to be entitled to a certificate in accordance with this CPS.

4.8.2 Who may request certificate modification

A CA may request modification of its certificate.

The end-user subscriber (including RA and LRA) or the Machine Operator for a technical device (as applicable) may request modification of their respective certificates.

4.8.3 Processing certificate modification requests

Processing of CA certificate modification is identical to the process used for the initial application.

For all other certificates certificate modification identity-proofing is achieved using one of the following processes:

- Initial registration process as described in section 3.2; or
- Identity-proofing for re-key as described in section 3.3, except the old key can be re-used as the new key. In addition, the validation of information that has not been in the old certificate is performed in accordance with the initial identity-proofing process as described in Section 3.2.

4.8.4 Conduct constituting acceptance of a modified certificate

Identical to section 4.4.1.

4.8.5 Publication of the modified certificate by the CA

Identical to section 4.4.2.

4.8.6 Notification of certificate issuance by the CA to other entities

Identical to section 4.4.3.

4.9 Certificate revocation and suspension

A certificate can either be suspended or revoked. If it is not certain whether a private key has been lost or compromised, the subscriber must suspend the corresponding certificate until matters have been clarified. If the private key has been compromised or lost for sure, or if subscriber data represented in the certificate has changed substantially, the certificate must be revoked.

If the certificate is revoked, it becomes invalid as soon as the CA has processed the revocation request. The certificate's serial number and time of revocation are included in the Certificate Revocation List, and subsequent status inquiries to the certificate repository will result in a response citing the certificate as invalid.

If the certificate is suspended, it is placed on the Certificate Revocation List, and any status inquiries to the certificate repository while the suspension is in effect will result in a response citing the certificate as invalid.

A certificate revocation may be requested at any time; the maximum delay between the receipt of a revocation request and the change to the revocation status system will not exceed 72 hours.

4.9.1 Circumstances for revocation

A certificate shall be revoked for the following reasons:

1. The certificate holder can be shown to have violated the stipulations of its respective contractual agreements or the stipulations of this CPS;
2. The private key is compromised or is suspected of compromise;
3. The subject named in the certificate has died;

4. TC TrustCenter's Policies and Practices Board suspects or determines that revocation of a certificate is in the best interest of the integrity of the PKI the certificate belongs to;
5. The issuing CA has learned about false information having been supplied in the certificate application that invalidates the certificate;
6. The subscriber or his agent (e.g. in case of a machine certificate) has submitted a revocation request as described in section 4.9.3;
7. The subscriber ends its subscription (see section 4.11);

If cryptographic algorithms or parameters become insecure because of technological progress or new developments in cryptography TC TrustCenter reserves the right to revoke certificates that are issued using these algorithms or parameters.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on a CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire. Revoked certificates shall appear on at least one CRL.

TC TrustCenter shall respond to all plausible notices that a signed software object containing Suspect Code verifies with a Code Signing certificate that it has issued by revoking that certificate. In the Subscriber Agreement or in its Terms and Conditions TC TrustCenter must give notice that it will revoke certificates issued to Subscribers who use them to digitally sign Suspect Code.

Suspect Code is defined as: Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.

4.9.2 Who can request revocation

Only the subscriber can request revocation, except as noted in section 4.9.1, items 1 to 5.

Any entity or third party that confirmed any information contained in a certificate should inform TC TrustCenter about the fact that this information is not or no longer correct, and request revocation in accordance with section 4.9.1, 4.

If a certificate states that its holder may act on behalf of a third party, this party may also request invalidation of the certificate.

4.9.3 Procedure for revocation request

Any request to revoke a certificate must identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The CA or RA receiving the revocation request has to authenticate the request as well as the authorization of the requester per section 4.9.2.

There are several ways to submit a revocation request:

1. If the subscriber is still in possession of his/her private key, he/she has the option of submitting an authenticated revocation request to TC TrustCenter. The subscriber can use online revocation at TC TrustCenter's revocation page <http://www.trustcenter.de/sperrren>. In this case the subscriber must authenticate at the revocation page using the certificate. After this authentication the certificate can be revoked.
2. If the private key has been lost or is inaccessible for any reason, the subscriber may call TC TrustCenter by phone and authenticate by providing a revocation password chosen when submitting the initial certificate application.

3. For certificates issued under TC Class 2, TC Class 3, and TC Class 4 the subscriber may request the certificate to be revoked by writing a letter to TC TrustCenter stating this request. Authentication is then provided by the subscriber's signature. The subscriber's signature on the revocation request must match the signature provided during the identity proofing process (e.g. signature on facsimile of ID).

If an RA performs the revocation service on behalf of a CA, the RA must send a message to the CA requesting revocation of the certificates. These messages must be digitally or manually signed.

TC TrustCenter confirms the subscriber's request for revocation by e-mail, within reasonable amount of time, no later than twenty-four hours after receiving the request.

4.9.4 Revocation request grace period

There is no revocation grace period. Authorized parties, including subscribers are required to request the revocation of a certificate immediately after the need for revocation comes to their attention.

4.9.5 Time within which CA must process the revocation request

TC TrustCenter processes a revocation request, upon confirming that it originated from the subscriber or an authorized third party, as promptly and efficiently as possible.

4.9.6 Revocation checking requirement for relying parties

Relying Parties are required to comply with common standards for signature validation, which prescribe how certificate status information is to be obtained and used.

Any relying party's reliance on a certificate issued by TC TrustCenter must be reasonable and exercise ordinary business prudence under the circumstances and must conform to the following obligations:

- Validate the certificate (i.e., confirm that it has not expired or been revoked or suspended), by checking the published revocation list;
- Verify that a valid certificate chain is established between the relying party and the subject. A valid chain means that the certificate signatures have been validated back to a final root certificate and the revocation list has been checked to determine the validity of each certificate.

4.9.7 CRL issuance frequency (if applicable)

Certificate status information is made available to all relevant entities through Certificate Revocation Lists (CRLs) which are available from TC TrustCenter's repository. CRLs are also available upon request by e-mail. Each CRL is digitally signed so that entities can validate the integrity of the CRL and the date of issuance, and it includes a monotonically increasing sequence number.

In general, CRLs are issued at least once a day, but they may be updated several times a day, even if no changes have occurred since the last issuance. Each CRL has a maximum validity period of one week. CRLs for CAs issuing very few certificates (e.g. Root CAs) may have a longer validity.

At a minimum, a CRL entry identifying a revoked certificate remains on the CRL until the end of the certificate's validity period. A certificate is also put on the CRL during its suspension period.

CRLs are available from the following URL: <http://www.trustcenter.de/crl>.

4.9.8 Maximum latency for CRLs (if applicable)

TC TrustCenter processes the revocation request, upon confirming that it originated from the subscriber or another authorized entity, as promptly and efficiently as possible. The time needed to revoke the certificate after confirming the request's origin does not exceed twenty-four hours.

4.9.9 On-line revocation/status checking availability

The certificate status can be checked on-line from the certificate repository. Any changes committed to the repository are immediately available to any subscriber and / or relying party.

CAs do not necessarily support OCSP services. If a CA provides revocation information via OCSP, that service is updated at least once every day. OCSP responses have a maximum expiration time identical to the validity of the associated CRL.

4.9.10 On-line revocation checking requirements

It is the responsibility of the relying party to either

- obtain the latest CRL and check the revocation status, or
- check the revocation status on-line.

In order to check a CRL's signature a relying party must be in possession of or obtain the appropriate CRL certificate. This certificate may differ from the certificate of the issuer(s) of any certificate on the CRL, and if so, it is available from TC TrustCenter's Web Site or upon request by e-mail.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements regarding key compromise

Depending on whether the subscriber suspects or knows for sure that the private key has been compromised, it is required to request suspension or revocation, respectively, as soon as possible. A subscriber is not relieved from the obligations as a subscriber until the subscriber has been notified by TC TrustCenter of the revocation of the certificate. Such notifications are submitted to the subscriber (e.g. by e-mail) after a certificate has been revoked or suspended.

4.9.13 Circumstances for suspension

A certificate is suspended in case:

1. The subscriber has informed TC TrustCenter that the certificate must be suspended, for example because the private key might have been compromised or lost;
2. TC TrustCenter or any other entity or third party that confirmed any information contained in a certificate suspects that false information has been supplied in the certificate application that might invalidate the certificate.

4.9.14 Who can request suspension

The subscriber can request suspension.

Any entity or third party that confirmed any information contained in a certification should inform TC TrustCenter about the fact that this information might not or no longer be correct and request suspension in accordance with section 4.9.13, 2.

Other third parties may request suspension of a certificate only for reasons mentioned in section 4.9.13, 2.

4.9.15 Procedure for suspension request

Identical to section 4.9.3.

4.9.16 Limits on suspension period

The period for suspensions requested by the subscriber must not exceed six weeks. A certificate may be suspended twice; a third suspension or exceeding the suspension period will result in the certificate being revoked.

4.10 Certificate status services

No stipulation beyond section 4.9.9.

4.10.1 Operational characteristics

No stipulation.

4.10.2 Service availability

Certificate and revocation status information is publicly and internationally available 24 hours per day, 7 days per week (compare section 2.1).

Upon system failure, service, or other factors which are not under the control of TC TrustCenter, TC TrustCenter makes best efforts to ensure that the revocation status service is not unavailable for longer than inevitable.

Relying Parties are bound to their obligations and the stipulations of this CPS irrespective of the availability of the certificate status service. Especially if the revocation status service is temporarily unavailable Relying Parties shall not rely on the validity of a certificate until the proper functionality of the revocation status service has been re-established.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

TC TrustCenter will not keep end users' private keys or any private key material, unless

- (1) key escrow is explicitly agreed upon in a contract between the subscriber and TC TrustCenter, outlining the liabilities and remedies between the parties, and
- (2) is not prohibited by law, certificate policies, or other applicable provisions or agreements.

Key escrow processes require appropriate controls to assure that the risk doesn't outweigh the benefits, e.g. dual control.

4.12.1 Key escrow and recovery policy and practices

This CPS prohibits third party escrow or recovery of CA, RA, and LRA signing keys used for purposes set forth in this CPS.

TC TrustCenter shall not escrow subscriber private keys solely intended for signing purposes.

Key recovery for decryption keys can be contractually agreed upon between TC TrustCenter and the Subscriber. Such a contractual agreement must then describe the key escrow and recovery procedures and practices.

4.12.2 Session key encapsulation and recovery policy and practices

Procedures for key encapsulation and recovery must be laid down in the contractual agreement mentioned in section 4.12.1.

5 Facility, Management, and Operational Controls

5.1 Physical controls

All CAs and certificate status verification systems are subject to the physical security requirements specified in Section 5.1.2. These requirements also apply to CCSs.

RA and LRA equipment is protected from unauthorized access at any time. The RAs and LRAs have implemented physical access controls to reduce the risk of equipment tampering even when cryptographic equipment is not installed and activated. These security mechanisms are commensurate with the level of threat in the LRA/RA environment.

5.1.1 Site location and construction

Several layers of physical security controls restrict access to TC TrustCenter's sensitive hardware and software systems used in performing critical CA operations, which take place within a physically secure facility. These systems are physically separated from the organization's other systems so that only authorized employees of the CA can access them.

5.1.2 Physical access

TC TrustCenter protects its relevant systems, especially CA and certificate status systems, with physical security mechanisms to:

- Permit no unauthorized access to the hardware;
- Store all removable media and paper containing sensitive plain-text information in secure containers;
- Monitor, either manually or electronically, for unauthorized intrusion at all times;
- Maintain and periodically inspect an access log; and
- Require two person physical access control to all sensitive computer systems and cryptographic equipment as Hardware Security Modules (HSMs).

Physical access to the CA systems is strictly controlled. Only trustworthy individuals with a valid business reason are provided such access. The access control system is always functional and utilizes access cards in combination with passwords for access. A log is maintained, listing all physical entries to restricted areas.

Private keys used for issuing certificates or signing CRLs are not vulnerable to physical penetration. These keys are kept in tamper-resistant hardware modules or smart cards. Any unauthorized access to stored information, possibly resulting in loss, tampering or misuse thereof, is prevented by proper means. Regular security checks are made to ensure that all these controls function properly.

Access to any physical area where information or equipment sensitive to CA operations is located requires at least two authorized persons to access the respective locations. Entering restricted areas using the same authorization token twice (to circumvent the requirement of two *different*

persons having to access the respective location) is prevented by technical means. In addition, sensitive areas are monitored by video cameras.

Any sensitive computer system performing certificate issuance runs a secure B1 operating system and cannot be operated through a LAN or WAN, but only from the console. The computer systems providing the directory and repository services may only be administered from the console or via a secure network protocol. Access to sensitive systems requires two persons to be present (or log on) simultaneously.

Any RA confirming subscriber information and forwarding this information to TC TrustCenter must provide a secure physical facility for storing registration records and tokens needed to access RA components. If an RA keeps confidential subscriber information, such as subscriber key information, the RA's physical security controls must match those of TC TrustCenter.

5.1.3 Power and air conditioning

All CA systems have industry standard power and air conditioning systems to provide a suitable operating environment.

Furthermore, all relevant systems are provided with an uninterruptable power supply sufficient more than six hours operation in the absence of commercial power, to support either a smooth shutdown of the CA operations or to re-establish commercial power.

5.1.4 Water exposure

All CA systems have reasonable precautions taken to minimize the impact of water exposure.

5.1.5 Fire prevention and protection

All CA systems have industry standard fire prevention and protection mechanisms in place.

5.1.6 Media storage

CA media is stored so as to protect it from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains audit, archive, or backup information is duplicated and stored in a location separate from the CAs.

5.1.7 Waste disposal

Sensitive waste material shall be disposed of in a secure fashion.

5.1.8 Off-site backup

Daily full system backups of all CAs are made, sufficient to recover from system failure. These daily backups are stored off-site. The backup site has physical and procedural controls commensurate to those of TC TrustCenter.

5.2 Procedural controls

TC TrustCenter's operating procedures are documented and maintained. Procedural controls ensure that no single person acting individually will be able to circumvent the implemented security measures.

Formal management responsibilities and procedures exist to control all changes to CA equipment, software, and operating procedures. Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorized modification or misuse of information or services. This is achieved, for example, by defining different roles so that the performance of certain essential tasks requires multiple individuals in order to prevent a single person from being able to forge a certificate.

Development and testing facilities are separated from operational facilities. Procedures exist and are followed for reporting software malfunctions. Procedures exist and are followed to ensure that faults are reported and corrective action is taken. Users of CA systems are required to note and report observed or suspected security weaknesses in or threats to systems or services. System documentation is protected from unauthorized access.

Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

Detection and prevention controls to protect against viruses and malicious software and appropriate user awareness procedures are implemented.

A formal reporting procedure exists and is followed, together with an incident response procedure, setting out the action to be taken on receipt of an incident report. Incident management responsibilities and procedures exist and are followed to ensure a quick, effective, and orderly response to security incidents.

5.2.1 Trusted roles

Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorized modification or misuse of information or services. This is achieved by defining different roles so that the performance of certain essential tasks requires multiple individuals from different roles. Examples of roles are: System Operator, System Administrator, CA Manager, CA Operator, CA Administrator, CCS Administrator, CCS Operator, Auditor, and IT-Security Officer.

5.2.2 Number of persons required per task

All activities at one of TC TrustCenter's CAs require (at least) dual control. Backup and activation of CA private keys requires dual control.

The generation of CA and Root keys requires at least participation of three individuals (see section 6.1.1.1).

5.2.3 Identification and authentication for each role

An individual in a trusted role must identify and authenticate before being permitted to perform any actions related to operating a TC TrustCenter root or CA.

5.2.4 Roles requiring separation of duties

The role concept is enforced by the CA system. Especially for activation of HSMs protecting TC TrustCenter's CA and root keys at least two different roles are required.

Individual personnel are specifically designated to the roles.

Individuals may not assume more than one role except for the following exceptions:

- An individual assigned an IT-Security Officer role may also be assigned an Auditor role, and vice versa.
- An individual assigned the CA Operator role may also be assigned a System Operator role, and vice versa.
- An individual assigned the CA Administrator role may also be assigned a System Administrator role, and vice versa.

No individual is assigned more than one identity.

Under no circumstances shall any PKI entity perform its own compliance auditor function.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

All persons filling trusted roles and personnel involved in issuing, managing, and revoking certificates and managing related data and information are citizens of one of the member States of the European Union. RA personnel may be a citizen of the country where the RA is located. All persons in trusted roles are selected on the basis of loyalty, trustworthiness, and integrity.

This includes, but is not limited to; requiring a certificate issued by the police, stating that the individual in question has no criminal record whatsoever. The individual must have proper knowledge and experience related to CA operations and must have demonstrated security consciousness and awareness regarding its duties at TC TrustCenter. Periodic reviews occur to verify the continued trustworthiness of all personnel. Employees have to sign a confidentiality (nondisclosure) agreement as part of their initial terms and conditions of employment.

All employees involved in the operation of the CA systems receive appropriate training in organizational policies and procedures.

A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures. TC TrustCenter's policies and procedures specify the sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems.

Appropriate and timely actions are taken when an employee is terminated so that controls and security are not impaired by such an occurrence.

5.3.2 Background check procedures

Relevant personnel involved in the operation of the CA systems have to pass, at a minimum, a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence;
- Criminal background check; and
- References (if available).

The extent to which these investigations are performed is restricted by the applicable local legislation.

5.3.3 Training requirements

All personnel performing duties with respect to the operation of the CA systems receive comprehensive training. Training is conducted in the following areas:

- CA security principles and mechanisms;
- Use and operation of all PKI associated equipment;
- PKI software;
- All PKI duties an individual is expected to perform.

5.3.4 Retraining frequency and requirements

Individuals responsible for trusted roles regarding TC TrustCenter's CA systems must be aware of changes in the CA's operation. Any significant change to the operations requires the operating staff

to be trained appropriately before the change is implemented. Participation at training is documented. Examples of such changes are software or hardware upgrades, changes in automated security systems, and relocation of equipment.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Appropriate administrative and disciplinary actions are taken against personnel who perform unauthorized actions (i.e., not permitted by this CPS or other policies) involving TC TrustCenter's CA systems, CCS system, the certificate status verification systems, and the repository.

5.3.7 Independent contractor requirements

Contractor personnel employed to perform functions pertaining to CA, certificate status verification systems, RA, LRA, and TA are subject to the same requirements as TC TrustCenter's staff performing similar functions (c.f. section 5.3 and subsections thereof).

5.3.8 Documentation supplied to personnel

TC TrustCenter makes available to its personnel this CPS, applicable system operations documents, operations procedures documents, and any relevant statutes, policies or contracts required to perform their jobs.

5.4 Audit logging procedures

TC TrustCenter keeps audit trails and system log files that document actions taken as part of TC TrustCenter's public certification services. All relevant events related to the security of the CA, certificate status systems, RA, and LRA are logged.

Where possible, the security audit logs are automatically collected. Where this is not possible, a logbook, a paper form, or other physical mechanism is used.

All security audit logs, both electronic and non-electronic, are retained and maintained in accordance with section 5.5.2, *Retention period for archive*.

5.4.1 Types of events recorded

TC TrustCenter keeps audit trails and system log files that document actions taken as part of its services. These include, but are not limited to: issuance of certificates, CRLs, time stamps; notification of key compromise; revocation of certificates; extension of certificates; establishment of trusted roles and actions of trusted personnel; changes to CA and root keys.

In addition, system access and use is monitored and recorded in audit logs or written down in event journals. Thus all CA personnel are accountable for their activities. Events in audit logs are time-stamped and digitally signed. Audits logs and event journals are reviewed regularly and archived to assist in future investigations of security-related incidents.

5.4.2 Frequency of processing log

Audit logs from the CA, certificate status systems, RA, and LRA are reviewed regularly by internal auditors. At a minimum, a statistically significant set of security audit data generated by the component since the last review is examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity.

The analysis must document and explain all significant events in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews are documented.

5.4.3 Retention period for audit log

Records are archived for at least five years.

5.4.4 Protection of audit log

No single person may modify or even delete audit trails or system log files, and access to them is strictly restricted.

System configuration and operating procedures ensure that:

- Only authorized people have read access to the logs;
- Audit logs are not modified.

Procedures are implemented to protect archived data from destruction prior to the end of the audit log retention period. Audit logs are moved to a safe, secure storage location separate from the component which produced the log.

5.4.5 Audit log backup procedures

As part of the scheduled system back up procedures, audit trail and system log files (see section 5.4.1) files are backed up to WORM (write once, read multiple) media and archived in a safe facility.

Audit trail files are archived by the system administrator on a regular (at least) weekly basis.

TC TrustCenter uses internal and external archival to prevent loss of important documents and digital data. The archives are located in separate (internal or external) locations and protected by access-control systems.

5.4.6 Audit collection system (internal vs. external)

The audit log collection system may or may not be external to a component. Audit processes shall be invoked at system start-up, and cease only at system shutdown.

Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the IT-Security Officer (see section 5.2.1) is notified, and the IT-Security Officer shall determine whether to suspend the component operation until the problem is remedied.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

The Auditor or the IT-Security Officer (see section 5.2.1) shall perform vulnerability self-assessments of security controls.

5.5 Records archival

TC TrustCenter's archive records are sufficiently detailed to establish the proper operation of the certification system or the validity of any certificate (including those revoked or expired) issued by one of TC TrustCenter's CAs.

TC TrustCenter uses internal and external archival to prevent loss of important documents and digital data. The archives are located in separate (internal or external) locations and protected by access-control systems. Records are archived for at least five years. No single person is able to modify or even destroy archived material, and access to it is strictly restricted.

5.5.1 Types of records archived

At a minimum, the following data is recorded for archive:

- This CPS
- Contractual obligations
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- Revocation requests
- All certificates issued or published
- Record of CA re-key
- All CRLs issued and/or published
- All Audit Logs
- Documentation required by compliance auditors

5.5.2 Retention period for archive

Records are archived for at least five years.

5.5.3 Protection of archive

Only authorized individuals are permitted to add to or delete from the archive. The archived records may be moved to another medium when authorized by the Auditor.

The contents of the archive shall not be released except as determined by TC TrustCenter's Policies and Practices Board or as required by law.

5.5.4 Archive backup procedures

Archived records in electronic form (see section 5.5.1) are backed up regularly on WORM (write once, read multiple) media and archived in a safe facility. TC TrustCenter's Archival Policy describes how archive records are backed up, and how the archive backups are managed.

5.5.5 Requirements for time-stamping of records

CA archive records related to issuance of certificates, issuance of CRLs, issuance of time stamps, revocation of certificates, and extension of certificates are automatically time-stamped as they are created. TC TrustCenter's Time-Stamp Policy describes how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

Archive information is automatically created by TC TrustCenter's CA systems. Archive information is held on the respective system (e.g. CA system, certificate status verification system, webserver) and, additionally, backed up to WORM media (see section 5.5.4. Archive information is verified in regular intervals as described in section 5.4.2.

5.6 Key changeover

Upon the end of the private key's lifetime, a new CA signing key pair is generated and all subsequently issued certificates and, if applicable, CRLs are signed with the new private signing key. Changing CA keys enables TC TrustCenter to adjust key parameters, taking into account advances in science and / or technology. Any new CA key is available on request via e-mail or from TC TrustCenter's repository at <http://www.trustcenter.de/repository>.

5.7 Compromise and disaster recovery

TC TrustCenter has a business continuity plan to restore its business operations in a reasonably timely manner following interruption to, or failure of, critical business processes. The business continuity plan defines the period of time that is an acceptable system outage time in the event of a major natural disaster or CA private key compromise. This outage time depends on the applicable contractual subscriber agreements that pertain to the certification services related system that has failed.

5.7.1 Incident and compromise handling procedures

Backups of essential business information and CA system software are performed daily. TC TrustCenter tests internal disaster recovery procedures regularly. Documentation concerning details of these procedures is considered confidential.

If a CA detects a potential hacking attempt or other form of compromise of a CA, it performs an investigation in order to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in Section 5.7.3 are followed. Otherwise, the scope of potential damage will be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

If a CCS is compromised or suspected of being compromised, the incident shall be investigated. All certificates associated with the subscriber private keys held in the CCS shall be revoked unless a definitive determination is made that the CCS is not compromised.

5.7.2 Computing resources, software, and/or data are corrupted

TC TrustCenter maintains backup copies of its databases and private keys in order to be able to rebuild the signing capability in case of software and/or data corruption.

When computing resources, software, and/or data are corrupted, TC TrustCenter responds as follows:

- If the affected CA signature keys are not destroyed, operation of that CA will be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in section 4.9.7.
- If a CA signature keys is destroyed, operation of that CA will be re-established as quickly as possible, giving priority to the generation of a new CA key pair.

5.7.3 CA private key compromise procedures

In case of a key compromise of a CA, TC TrustCenter will revoke the CA certificate (which has been issued by one of TC TrustCenter's roots) and publish the revocation information.

Furthermore, the affected CA will request revocation of its certificates from all other root or CAs who have issued it a certificate. These other CAs shall immediately publish the revocation information in the most expedient manner. Subsequently, the CA functionality will be re-established as above.

If one of TC TrustCenter's roots is compromised, the trusted self-signed certificate will be removed from TC TrustCenter's CAs, and a new one will be distributed to the CAs.

If this root has certified other CAs as well, these CAs are informed and advised to remove the self-signed root certificate and to install a new one (distributed via secure out-of-band mechanisms).

Because some of TC TrustCenter's root certificates are distributed as part of most internet browsers, all partners distributing the root certificates will be informed to replace the current root certificate by a new one. A current list of applications, operating systems, and browsers with pre-installed TC TrustCenter Root certificates and CA certificates can be found in TC TrustCenter's FAQ at <http://www.trustcenter.de/infocenter/faq.htm>.

The TC TrustCenter Policies and Practices Board (PPB) will also investigate what caused the compromise or loss of a private key, and what measures have been taken to preclude recurrence.

5.7.4 Business continuity capabilities after a disaster

In the case of a disaster whereby the CA equipment is physically damaged and all copies of a TC TrustCenter Root CA key are destroyed as a result, TC TrustCenter will inform all external CAs which have been certified by the affected Root CA that it will not be able to issue a new CRL with the same CRL signing key as before. The TC TrustCenter Root CA has to generate a new self-signed root key; the affected CAs and their users have to install this new root key and the associated certificate as trust anchor.

If CA equipment is physically damaged and all copies of a TC TrustCenter CA key are destroyed as a result, TC TrustCenter will generate a new CA key and sign it with the appropriate root key.

If CA equipment is damaged or rendered inoperative, but the CA signing keys are not destroyed, operation will be re-established as quickly as possible and in a secure fashion, giving priority to the ability to generate a new CRL.

Directories containing certificates and certificate status information are deployed so as to provide high availability. Features are implemented to provide high levels of directory reliability.

5.8 CA or RA termination

5.8.1 CA Termination

A CA can only be terminated by TC TrustCenter's Board of Directors. TC TrustCenter will inform subscribers of valid certificates (i. e., neither revoked nor expired). They will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought.

TC TrustCenter will make a reasonable effort to archive the records of the CA and transfer them to a specified custodian, and to establish an acceptable procedure for subscribers and relying parties for switching to a different provider of public certification services, in order to minimize the effects of TC TrustCenter ceasing to provide these services by itself

If no alternative certificate provider continues TC TrustCenter's services all certificates that have not expired or have not been revoked by the respective subscribers will be revoked by TC TrustCenter. A final CRL will be published and made available for at least as long as the validity period of the certificate with the longest validity period indicates. Subscribers will be notified of such action taken by TC TrustCenter.

To cover all financial expenses in case of termination TC TrustCenter has made appropriate provisions in form of a Letter of Comfort (a special kind of a letter of credit). It is the intention of such a letter that TC TrustCenter's mother company guarantees that it will be responsible for the debts or duties set out in the letter.

5.8.2 RA Termination

Upon termination of an RA TC TrustCenter will revoke the RA certificate(s) which have been issued to that RA. If the RA has a dedicated archival facility all archived data will be transferred to the relevant archival facility. Otherwise TC TrustCenter's internal RA will archive these documents.

6 Technical Security Controls

Whenever a FIPS 140-1/2 module is used, the module must be validated and must be used in FIPS approved mode.

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

TC TrustCenter generates its key pairs used for signing and verifying certificates:

- In accordance with its operational standards listed in section 5;
- In a procedure documented in a key generation script carried out by TC TrustCenter personnel and archived securely for as long as the corresponding certificate is valid.

Any private CA key used for issuing certificates is generated on a hardware security module (HSM) evaluated as "E4 high" according to ITSEC criteria (or equivalent) e.g. a Smart Card, or using a FIPS 140-1/2 Level 3-compliant HSM, which is tested for proper operation before commencing the key generation procedure. The entire procedure is done under dual control. In addition, the key generation is witnessed and signed off by a third person not involved in the actual key generation.

The private keys are retained either in the hardware security module in which they were generated or are stored in secure hardware tokens to which access is limited to TC TrustCenter personnel. The private keys are also backed up and stored offline in a secure facility.

Immediately after generating a key pair, the hardware security module creates a certificate request and signs it, using the private key just created. A TC TrustCenter Root CA receives and verifies that certificate request, and then issues a certificate –either to itself or to the CA that just generated the request– with the content specified in section 7.1.

At no point during the generation process does the private key leave the HSM in unencrypted form, and no unencrypted private key material leaks out.

Keys initially generated by software are split up into shares by a cryptographic module that meets FIPS 140-1/2 Level 3, or imported into a FIPS 140 Level 3-compliant HSM, if possible. Splitting a key up into parts allows for better control of private key usage, requiring n out of m people (with n and m greater than or equal to 2) to use a key. The key shares are encrypted using the keys that are needed to activate the module (see section 6.2.1). The encrypted shares are transferred to and stored in an HSM.

Software generation and/or usage of keys is only done if no other option is available to issue certificates of the appropriate type. In this case, the passphrase needed to activate the key is split into two or more shares.

No copy of any private key is kept permanently on magnetic media in unencrypted form, and any private key material that was temporarily stored on magnetic media is destroyed by wiping the space once occupied by the respective file(s) multiple times to erase any remaining trace.

6.1.1.2 Subscriber key pair generation

In general, the key pair and the certificate request are generated by the subscriber during the process of applying for the certificate. In most cases this is automatically done by the subscriber's internet browser or server software.

The subscriber may generate his key pair using software that generates certificate requests in any format that TC TrustCenter can process (X.509, WTLS, etc.), like Internet browsers, Web servers, security proxies etc. The key generation may happen during the certificate application, depending on what kind of certificate the subscriber wishes to apply for.

Only on subscriber's request or in special projects will TC TrustCenter generate keys on behalf of the subscriber. Key generation then takes place in a secure environment as described in section 5. This may happen if the secret key is stored on a smart card (see also section 6.1.1.1). In this case, smart cards used will generally be able to autonomously generate the key pair and they will be evaluated as "E4 high" according to ITSEC criteria (or equivalent). TC TrustCenter then merely initiates this process and has no control over or access to private key material.

Other keys may be created in software.

6.1.2 Private key delivery to subscriber

If the subscriber generates the key pair, there is no need for private key delivery to the end user.

If TC TrustCenter generates the key and stores it on a hardware token (such as a smart card), the private key (i.e., the hardware token) and the sealed letter containing the PIN(s) needed to use or enable the private key may either

- (1) be delivered to the end user, upon his request, by certified mail with return receipt or any other acceptable form of secure delivery, or
- (2) be collected by the end user at TC TrustCenter's office or an associated RA or LRA.

Software keys may either

- (1) be delivered to the end user, upon his request, by encrypted email, or
- (2) be downloaded in encrypted form from TC TrustCenter's website.

Private keys are protected from activation, compromise, or modification during the delivery process. When keyed hardware tokens are delivered to subscribers, the delivery is accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subscribers.

Nobody but the subscriber has substantive knowledge of or control over signing private keys after generation of the key. TC TrustCenter does not retain any copy of a private signing key after delivery of the private key to the subscriber.

CAs generate their own key pairs in hardware.

6.1.3 Public key delivery to certificate issuer

If the subscriber generates the key pair, the self-signed public key is submitted to TC TrustCenter during certificate application. The self-signed certificate signing request allows TC TrustCenter to bind the applicant's verified identity to the public key contained in the certificate signing request.

If TC TrustCenter generates the key pair on behalf of the user (see section 6.1.1.2), there is no need for public key delivery to the certificate issuer.

6.1.4 CA public key delivery to relying parties

The CA public keys are available from the certificate repository and upon request by e-mail.

TC TrustCenter ensures that subscribers receive and maintain CA certificates and/or root certificates in a trustworthy fashion by using acceptable methods for trust anchor delivery only. These methods include but are not limited to:

- A trusted role loading the CA or Root certificates onto tokens delivered to subscribers via secure mechanisms;
- Distribution of CA or Root certificates through secure out-of-band mechanisms;
- Calculation and comparison of CA or Root certificate hash or fingerprint against the hash made available via authenticated out-of-band sources. Fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism;
- Downloading CA or Root certificates from TC TrustCenter's website secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded. In this case certificate securing the website (or at least the root of that certificate) must already be on the subscriber's system via secure means (e.g. as built-in part of the subscriber's browser).

6.1.5 Key sizes

All TC TrustCenter CA keys are at least 1024 bit RSA. All TC TrustCenter CA keys with validity beyond 2013 are at least 2048 bit RSA.

Subscriber's public keys must be between 1024 and 4096 bit in size, with 2048 bit recommended. TC TrustCenter reserves the right to reject requests with smaller key sizes.

All keys generated on smart cards are at least 1024 bit in size.

1024 bit keys in combination with specific hash algorithms will only be used as long as they are declared to be suitable by the ETSI requirements defined in [TS 102 176].

TC TrustCenter may issue 1024 bit SSL certificates and 1024 bit authentication keys provided that the validity of such certificates ends on or before December 31, 2013 and provided that the validity of such certificates is not in conflict with commonly agreed upon requirements as stipulated e.g. in the CA/Browser Forum's "Guidelines For The Issuance And Management Of SSL Certificates".

The key length for Extended Validation (EV) SSL certificates is always 2048 bit.

6.1.6 Public key parameters generation and quality checking

Public key parameters prescribed in the Digital Signature Standard (DSS) are generated in accordance with FIPS 186-2 or equivalent.

Parameter quality checking (including primality testing for prime numbers) is performed in accordance with FIPS 186; additional tests may be specified by TC TrustCenter's Policies and Practices Board.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Certificates issued by TC TrustCenter must be used according to the X.509 v3 key usage field as set by TC TrustCenter (see also section 7.1). Certificates may, in general, be used for any purpose, including web server security and code signing.

Public keys that are bound into certificates are in most cases certified for use in signing or encrypting. The use of a specific key is determined by the key usage extension in the X.509 certificate. In particular, subscriber certificates to be used for digital signatures (including

authentication) shall set the *digitalSignature* and *nonRepudiation (contentComittment)* bits. Subscriber Certificates to be used for encryption shall set the *keyEncipherment* bit.

CA certificates must set the following key usage bits: *cRLSign* and *keyCertSign*.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The relevant standard for cryptographic modules is FIPS PUB 140-1/2, *Security Requirements for Cryptographic Modules*.

The minimum requirement for cryptographic modules storing Root CA keys or other CA keys is Level 3; higher levels may be used.

Physical access to cryptographic modules is restricted by an access control system. The hardware modules must be activated by two persons simultaneously (dual login).

If smart cards are used to store private CA keys these smart cards must be evaluated as "E4 high" according to ITSEC criteria (or equivalent). Also in this case two persons are required to insert and activate the smart cards that hold private CA keys.

Unencrypted private keys cannot be extracted from the hardware modules or smart cards.

6.2.2 Private Key (n out of m) multi-person control

Private CA keys are stored encrypted in a secure physical facility operated by TC TrustCenter. In order to gain access to the private keys, two persons are required (see section 6.2.1) in accordance with the requirements from section 5.2.2. No single person has all the activation data needed for accessing any of the private CA keys.

6.2.3 Private Key escrow

TC TrustCenter will not keep end users' private keys or any private key material, unless

- (1) key escrow is explicitly agreed upon in a contract between the subscriber and TC TrustCenter, outlining the liabilities and remedies between the parties, and
- (2), is not prohibited by law, certificate policies or other applicable provisions or agreements.

Using signing key escrow is strongly discouraged, however, since the risks generally outweigh the benefits.

If CA private signing keys are held in escrow, escrowed copies of the CA private signing keys are subject to the same or greater level of security controls as keys currently in use.

Third party escrow of CA signing keys used to support non-repudiation services is prohibited.

Key escrow for subscriber's private keys intended solely for digital signature is prohibited.

6.2.4 Private Key backup

TC TrustCenter keeps backup copies of its private CA keys in encrypted form. These keys can only be activated under dual control (compare sections 5.2.2 and 6.2.2) in a physically secure site (see section 5.1).

Keys generated and stored on a smart card cannot be extracted from the smart card and are therefore not backed up.

6.2.5 Private Key archival

TC TrustCenter uses the key backup (see section 6.2.4) for archival purposes. The stipulations on private key backup apply.

All archived private CA keys are destroyed at the end of the archive period using dual control in a physically secure site. Archived keys are never put back into production.

Subscribers may archive their own private keys.

6.2.6 Private Key transfer into or from a cryptographic module

Private CA keys are generated in FIPS 140-1/2 Level 3 (or equivalent) compliant Hardware Security Modules or on an ITSEC "E4 high" evaluated smart card and remain in the same HSM, resp. smart card.

Private CA keys may be backed up in accordance with section 6.2.4. Private CA keys generated and stored on smart cards can not be backed up.

6.2.7 Private Key storage on cryptographic module

Hardware cryptographic modules may store private keys in any form as long as the keys are not accessible without a FIPS 140-1/2, Level 2 authentication mechanism.

6.2.8 Method of activating Private Key

Activating CA private keys requires authentication via pass phrases and / or PINs and can only be done under dual control, since the authentication secret is split into two or more shares. Where an HSM is used, activation of the private key additionally requires possession of a hardware token (smart card).

6.2.9 Method of deactivating Private Key

Private CA signing keys are automatically deactivated after issuing certificates has been completed and the certification application exits or closes the connection to the HSM. Before it can be used again, it must be reactivated.

6.2.10 Method of destroying Private Key

CA signing private keys will be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked.

The destruction of any private CA key must be authorized by the management. It is done under dual control. The destruction of a CA signing key is documented and signed off.

Key destruction is achieved by executing a "zeroize" command on the HSM. Physical destruction of hardware cryptographic modules is not required.

If a CA cryptographic device is being permanently removed from service, then any key contained within the device that has been used for any cryptographic purpose is erased from the device by executing a "zeroize" command. If a CA cryptographic device case is intended to provide tamper-evident characteristics and the device is being permanently removed from service, then the case is destroyed.

For private keys used in conjunction with an HSM, the magnetic storage space that carried the private key is wiped multiple times to erase any remaining trace and the hardware token (smart card) needed to activate the key is completely erased or physically destroyed, unless it is needed to activate other private keys. If the storage medium itself is replaced (for example, due to hard disc hardware failure), it is physically destroyed.

For private keys stored on a smart card, the private key is destroyed by physically destroying the smart card.

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All CA public keys are archived as part of the certificate archive process.

Any certificate issued by TC TrustCenter is stored in the certificate repository and on backup media of the systems that host the certificate repository. TC TrustCenter does not offer any other public key archival service.

6.3.2 Certificate operational periods and key pair usage periods

A private key may be used for as long as it is known not to have been compromised and the key parameters are still considered to provide adequate security. Certificates, i. e. signed public keys, may be used for as long as the certificate and / or the repository indicate. Once a certificate has expired, it is no longer valid.

TC TrustCenter's public and private CA keys have a life-time period between 5 and 25 years, depending on the type of key. Root CA keys need a longer validity period to be useful.

The CA private key's life-time period is shorter than that for the corresponding public key, as determined by the validity-period of the certificates that are issued using the CA private key. If end-entity certificates have a validity period of one year, for example, and the life-time period of the CA certificate (and the public key) is five years, the private key's life-time period is at most four years. When the life-time period of the private key ends, key changeover will be initiated (see section 5.6).

End entity certificates will be valid for no more than five years from the date of issuance.

The usage period of a decryption private key is determined by the user because it may be necessary to decrypt messages or documents even if the associated public key certificate is no longer valid.

6.4 Activation data

6.4.1 Activation data generation and installation

The activation data used to unlock TC TrustCenter's CA private keys, in conjunction with any other access control, has a level of strength appropriate for a Root CA (Trust Anchor). It consists of a combination of system generated passwords, user selected passwords, and unique hardware tokens. Activation data is split between at least two disjoint groups of trusted roles.

One group has to present the hardware token to the HSM. Both groups must enter their password share that is associated with the token before the HSM can be activated.

If the activation data –more precisely: splits of activation data– must be transmitted, it has to be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

A CA's activation data has to be changed when the CA re-keys.

6.4.2 Activation data protection

Business requirements for access control are defined and documented. They require an identification and authentication process for each user, segregation of duties, and identification of the number of persons required to perform specific CA operations (m out of n rule). Activation (and access) data for sensitive keys and assets is under dual control and/or split between at least two disjoint groups of employees.

A formal user registration and deregistration procedure for granting access to activation data for CA information systems and services is followed, and the allocation and use of activation data and privileges is restricted and controlled. Users' access rights are reviewed at regular intervals, and the password holders are required to follow defined policies and procedures in the selection and use of their passwords.

Hardware tokens that contain TC TrustCenter's CA activation data are stored in a secure manner under dual control.

Activation data for TC TrustCenter's CAs is split among dedicated trusted roles, such that no single person has knowledge of or access to all activation data.

In general, activation data shall be memorized, not written down. If written down, it has to be secured at the level of the data that the associated cryptographic module is used to protect. Staff involved in the certificate issuance process may write down (its share of) activation data on a sheet of paper, which then has to be kept at all times (e.g. in the briefcase) or, alternatively, activation data may be stored electronically. If stored electronically, the activation data has to be encrypted using appropriate algorithms, parameters, and passwords.

To allow other members of the same trusted role access to activation data, activation data for each trusted role is stored separately in tamper-evident packaging and under dual control in a safe location.

It is prohibited to store activation data with the HSM or the associated hardware token.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

A general information security policy document (security policy) is approved by management, published, and communicated, as appropriate, to all employees. This policy is supplemented by detailed policies and procedures for personnel involved in certificate and key management.

The information security policy contains a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing. It contains a statement of management intent, supporting the goals and principles of information security, and gives an explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization.

The information security policy lists general and specific responsibilities for information security management, including reporting security incidents, and contains references to documentation which supports the policy. Responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined. An authorization process for new information processing facilities exists and is followed.

The Policies and Practices Board (see section 1.3.5.1) ensures that there is clear direction and visible management support for security initiatives. It is responsible for maintaining the security policy and coordinates the implementation of information security measures.

6.5.1 Specific computer security technical requirements

The operating systems used by the CA, status validation systems, RA, and LRA provide the following computer security functions:

- Authenticated logins
- Discretionary Access Control
- Security audit capability
- Access control restrictions to CA services based on authenticated identity
- Trusted path for user identification and authentication
- Operating system self-protection.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

TC TrustCenter's CA systems and certificate status validation systems are infrastructure components that support a range of customer related applications, some of which may manage regulated data. TC TrustCenter's design, installation, and operation are documented by qualified personnel in a qualified manner to support a broad variety of requirements.

TC TrustCenter has developed and produced appropriate documentation establishing that all relevant systems are properly installed and configured, and operate in accordance with their own technical specifications and the technical requirements imposed by business best practice, common standards (e.g. ETSI TS 102 042, ETSI TS 101 456, SAFE-BioPharma Association, etc.) and governmental regulations (e.g. the German Digital Signature Act).

This documentation includes:

- Installation manuals, procedures/scripts/data, acceptance criteria, and results.
- Operation manuals, procedures/scripts/data, acceptance criteria, certifications, and test results.

TC TrustCenter's CA system development process meets the following requirements:

- The CA shall use software that has been designed and developed under a formal, documented development methodology.
- All hardware and software shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase or the vendor uses tamper-evident packaging).
- If a CA develops its own software for the CA system or certificate status validation system, this development shall take place in a controlled environment, and the entire development process shall defined and documented.
- Whenever possible CAs shall use tamper-evident packaging in combination with courier services for shipping or delivery of hardware and software in order to obtain a continuous chain of accountability, from the purchase location to the operations location.
- CA platform (server hardware, operating system software, and CA application software) shall be dedicated to performing CA functions. There shall be no non-CA applications installed on the CA platform.

- Certificate validation system platform (server hardware, operating system software, and certificate validation application software) shall be dedicated to performing certificate validation functions. Applications which are not related to certificate validation shall not be installed on the certificate validation system platform.
- RA system platform (server hardware, operating system software, and RA application software) shall be dedicated to performing RA functions. There shall be no non-RA applications installed on the RA platform.
- CAs shall use centralized as well as host based firewalls in combination with local virus scanning software and intrusion detection/prevention systems to prevent malicious software from being loaded. Applications performing PKI relevant operations shall either have been developed in-house or shall have been obtained from reliable sources authorized by TC TrustCenter's policies.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment. Installation of hardware and software shall be performed by trusted and trained personnel in a defined manner.
- Before CA, certificate validation system, and RA hardware and software is used for the first time it shall be scanned for malicious code and periodically thereafter.
- CAs and certificate status validation systems shall use integrity protection software and automated alarming systems to detect all deviations from a defined state in system configurations and software applications. These mechanisms shall be activated permanently on the CA system and on the certificate status validation system. On all other systems these mechanisms shall be used periodically.

6.6.2 Security management controls

The CA and the certificate status verification systems have been developed in-house under conditions described above in section 6.6.1. TC TrustCenter uses a formal software acceptance procedure defining how and under which circumstances self-developed software is put into production. These procedures require verifications that software to be installed is that supplied from the developer, with no modifications, and the version intended for use. CA software integrity is under permanent control through automatic integrity checking mechanisms for detecting unauthorized modification to TC TrustCenter's CAs software or configuration.

The configuration of TC TrustCenter's CA systems as well as any modifications and upgrades are documented and controlled. A formal configuration management methodology is used for installation and ongoing maintenance of CA systems.

The CRLs are either manually or automatically checked when issued. Since they are signed they can not be altered unnoticed.

6.6.3 Life cycle security controls

Cryptographic hardware may be transported between locations in tamper evident packaging only.

Upon receipt of cryptographic hardware, authorized personnel inspect the tamper evident packaging to determine whether seals are intact. This is followed by acceptance testing.

After acceptance testing the cryptographic hardware is added to an inventory list. To prevent tampering, cryptographic hardware is stored in a secure site, with access limited to authorized personnel.

Each piece of cryptographic hardware is tracked during its life cycle; any change in its state (removal from storage, integration into the production environment, removal from service etc.) is reflected in an event journal.

The handling, installation and removal of cryptographic hardware are performed in the presence of no less than two trusted individuals. The same controls apply to service or repair being performed. TC TrustCenter cryptographic hardware is never serviced or repaired off-site and subsequently put back into production.

CA software is permanently under supervision after installation.

CA and certificate status validation system software development takes place in a secure and controlled environment dedicated for TC TrustCenter's development staff. The entire development process is well defined and documented.

6.7 Network security controls

TC TrustCenter has installed adequate protection from both inside and outside attacks (firewalls, intrusion detection mechanisms, etc.). Computer systems directly involved in issuing certificates have no LAN or WAN connection.

Routing controls are in place to ensure that computer connections and information flows do not breach the access control policy of the organization's business applications.

Access to all servers is subject to authentication. Users are provided direct access only to the services that they have been specifically authorized to use.

6.8 Time-stamping

For the provision of time-stamping services dedicated documents apply:

- TC TrustCenter GmbH Time-Stamping Policy (Time-Stamp Policy, Version 1.1 of January 21, 2008), and
- TC TrustCenter GmbH Time-Stamp Practice Statement (Time-Stamp Practice and Disclosure Statement Version 1.0 of January 31, 2008).

Both documents are available from TC TrustCenter's repository at www.trustcenter.de/repository.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate profile

7.1.1 Version number(s)

TC TrustCenter issues X.509 version 3 certificates. X.509 version 1 certificates can be issued upon request.

TC TrustCenter also issues WTLS certificates.

7.1.2 Certificate extensions

TC TrustCenter uses the standard X.509v3 extensions in accordance with RFC 2459 and RFC 3280.

TC TrustCenter uses the `ISOAuthorityKeyIdentifier` extension to indicate the CA key that was used to sign the certificate. It contains the serial number and distinguished name of that CA key.

Since extensions are only defined for X.509 version 3 certificates, TC TrustCenter does not (and cannot) use any extension with X.509 version 1 certificates.

7.1.3 Algorithm object identifiers

TC TrustCenter currently supports the hash function / digital signature algorithm combinations:

- md5withRSAEncryption,
- sha1withRSAEncryption,
- sha256WithRSAEncryption,
- sha384WithRSAEncryption, and
- sha512WithRSAEncryption.

The subfield *algorithmIdentifier:algorithm* contains the appropriate object identifier (specified in [RFC 3280]) for one of the above algorithms.

The length of the public key in *subjectPublicKey* is not less than 1024 bits.

7.1.4 Name forms

The subject and issuer fields of each X.509 certificate are populated with a unique Distinguished Name (DN) in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by RFC3280.

7.1.4.1 Fields Identifying the Issuer

Certificates issued by TC TrustCenter's CAs contain the following in the *issuer* field:

Identifier Type:	With data content of:	Indicates:
OrganizationName (O)	"TC TrustCenter GmbH"	TC TrustCenter acts as the Issuer
CountryName (C)	"DE"	TC TrustCenter is incorporated in Germany
CommonName (CN)	<Name of CA>, if necessary followed by a numeral	The name of the CA. The numeral indicates that there are several generations of CAs with the same name.

7.1.4.2 Fields Identifying the Subject

A certificate issued by a TC TrustCenter CA identifies its subject in the *subject* field. Root CAs have the same content in the *subject* field as in the *issuer* field (section 7.1.4.1 above) because the subject and the issuer are the same entity.

Certificates issued by TC TrustCenter's CAs contain the following in the *subject* field:

Identifier Type:	With data content of:	Indicates:
CommonName (CN)	Alphanumeric text	An unambiguous name identifying the subject. This name may not be meaningful to anyone but the subject and TC TrustCenter
Organizational Unit (OU)	Alphanumeric text, optional	The organizational unit the subject belongs to
OrganizationName (O)	Alphanumeric text, optional	The company name of the subject
Email (E)	Alphanumeric text, optional	Email address of the subject
LocalityName (L)	Alphanumeric text, Optional	The city or town in which the subject's place of business is located
StateOrProvinceName (ST)	Alphanumeric text, optional	The state or province in which the subject's place of business is located.
CountryName (C)	A standard two-letter	The country in which the subject is located

	abbreviation listed [ISO 3166] for a country, such as "US" for the United States	
--	--	--

7.1.4.3 Other Supported Fields

Certificates issued by TC TrustCenter may also contain the following fields. "Critical" indicates extensions where an application is required to be able to process the content of the field.

It is not applicable ("n/a") for fields that are not extensions. See [ITU-T X.509] and [RFC 3280] for more information about certificate content.

Field Name	Critical?	Data Content Requirements	Significance
version	n/a	V3 only (indicated by the integer "2")	Indicates the version of [ITU-T X.509] to which the certificate conforms
serialNumber	n/a	An integer unique to the certificate among the range of all serial numbers in certificates issued by the same issuer	Certificate serial number. The combination of issuer and serial number comprises a unique identifier for the certificate
signature	n/a	The subfield <i>algorithmIdentifier</i> : <i>algorithm</i> must contain the object identifier (specified e.g. in [RFC 3280]) for SHA-1 with RSA encryption)	Indicates the algorithm used by the issuer to sign the certificate
validity	n/a	The subfields <i>notBefore</i> and <i>notAfter</i> contain dates in the form specified for UTC in [RFC 3280]	<i>NotBefore</i> indicates the date on which the certificate begins to be valid and <i>notAfter</i> indicates when it ceases to be valid. Years are listed as specified in [RFC 3280]
subject	n/a	Contains at least one identifier specified in section 7.1.4.2	As specified in section 7.1.4.2
subjectPublicKeyInfo	n/a	The subfield <i>algorithmIdentifier</i> : <i>algorithm</i> contains the object identifier for hash function and encryption (e.g. SHA-1 with RSA encryption). The length of the public key in <i>subjectPublicKey</i> is not less than 1024 bits	<i>SubjectPublicKey</i> is the subject's public key, and <i>algorithmIdentifier</i> lists the algorithm to use with it.
authorityKeyIdentifier	No	The subfield <i>keyIdentifier</i> contains the SHA-1 hash of the public key by which the issuer's signature on the certificate can be verified	Indicates which public key to use in verifying the authenticity of the certificate
subjectKeyIdentifier	No	The subfield <i>keyIdentifier</i> contains the SHA-1 hash of the public key listed in <i>subjectPublicKeyInfo.subjectPublicKey</i> .	The subfield <i>keyIdentifier</i> labels the public key of this certificate for convenient reference and to prevent confusion with other key pairs the same subject may have.
keyUsage	Yes	As appropriate for the designated purpose of the certificate (e.g.	Indicates to software applications using the key that the key is to be used for authentication and

		<i>digitalSignature, nonRepudiation, keyCertSign, or cRLSign</i>)	certification (see [ITU X.509] and [IETF 3280])
certificatePolicies	No	As stated in section 1.2	As stated in section 1.2
basicConstraints	Yes	As appropriate for the certificate (<i>cA: FALSE</i> for end entity certificates, <i>cA: TRUE</i> for CA certificates).	The subfield CA with a value of "true" indicates that the certificate may be used to issue and verify other certificates. The <i>pathLenConstraint</i> subfield is interpreted as specified in [RFC 3280] section 4.2.1.10. Omission indicates that no limit is imposed
CRLDistribution-Points	No	As appropriate for the certificate, the subfield <i>DistributionPointName</i> contains a URL.	Points to a URL where more information about the post-issuance validity or reliability of a certificate may be available
authorityInfoAccess	No	URL for Sub-CA certificate and/or URL für OCSP	Points to a URL where more information about the post-issuance validity or reliability of a certificate may be available
subjectAlternateName	No	RFC822Name	In most cases an e-mail address can be found here

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

Certificates issued by CAs under this CPS may assert one or more of the OIDs listed in Section 1.2.

7.1.7 Usage of Policy Constraints extension

TC TrustCenter's CAs adhere to the certificate formats described in this CPS.

7.1.8 Policy qualifiers syntax and semantics

Certificates issued under this CPS may contain policy qualifiers such as user notice, policy name, and CPS pointers.

7.1.9 Processing semantics for the critical Certificate Policies extension

Processing semantics for the critical certificate policy extension is in conformance with X.509 certification path processing rules.

7.2 CRL profile

The fields in CRLs are the following:

Field Name	Critical?	Data Content Requirements	Significance
version	n/a	V2 only (indicated by the integer "1")	Indicates the version of [ITU-T X.509] to which the certificate revocation list (CRL) conforms
signature	n/a	Same as specified for certificates in section 7.1.4.1	
issuer	n/a	The distinguished name of the issuer (see section	Identifies the CA that issued the CRL (and the revoked

		7.1.4.1) of the revoked certificate	certificate)
ThisUpdate	n/a	A date and time specified according to section 5.1.2.4 of [RFC 3280] (<i>i.e.</i> in UTCtime)	The date and time when the certificate revocation list was issued
NextUpdate	n/a	A date and time specified according to section 5.1.2.5 of [RFC 3280] (<i>i.e.</i> in UTCtime). In general, the time indicated is seven days from the time listed in <i>ThisUpdate</i>	If this field is present, it indicates the date and time when this CRL becomes invalid The issuer anticipates issuing an update to the current CRL before this date and time.
RevokedCertificates	n/a	If present, this field contains the following subfields: <i>userCertificate</i> contains a subfield containing an integer <i>revocationDate</i> contains a date and time specified as UTCtime	If this field is present, <i>userCertificate</i> indicates the serial number of the unexpired, revoked certificate. <i>revocationDate</i> indicates the time when the certificate was revoked. If this field is absent in a particular CRL a user can infer that no certificates have been revoked as of the issue date of the CRL
authorityKeyIdentifier	No	The subfield <i>keyIdentifier</i> contains the hash of the public key by which the issuer's signature on the CRL can be verified	Indicates which public key to use in verifying the authenticity of the certificate
CRLumber	No	A long integer not exceeding 20 octets in length	The serial number of this CRL in an incrementally increasing sequence of CRLs

7.2.1 Version number(s)

TC TrustCenter's CAs issue X.509 version two (v2) CRLs (version field populated with integer "1").

7.2.2 CRL and CRL entry extensions

If the key used to sign a CRL is different from the one used to issue certificates on the respective CRL, TC TrustCenter uses the `authorityKeyIdentifier` to indicate the key that was used for issuing certificates on the CRL in question by stating issuer distinguished name and serial number of the certificate issuer certificate.

7.3 OCSP profile

If a CA provides OCSP services, requests and responses are in accordance with RFC 2560.

7.3.1 Version number(s)

If a CA provides OCSP services, the version number for request and responses is v1.

7.3.2 OCSP extensions

No stipulation.

8 Compliance Audit and other Assessments

TC TrustCenter is subject to regular external audits. These include audits pursuant to the German Digital Signature Act, TC TrustCenter acting as a CSP for Identrust Level One Participants, an audit for MBA/SISAC compliance, an ETSI TS 101 456, and an ETSI TS 102 042 compliance audit. ETSI TS 102 042 is in many cases accepted as an equivalent to the WebTrust™ program for Certification Authorities. ETSI TS 101 456 is intended for qualified certificates in compliance with the EU Directive 199/93 EC of the European Parliament and of the Council: Community Framework for Electronic Signatures, dated 13 December 1999 [EU-DIR].

All of these audits require demonstration of a maximum level of security and conformity to documented policies and practices. The respective provisions supplement one another and serve to enhance the overall security controls, which are audited regularly by independent third parties.

In addition, TC TrustCenter performs internal self-audits. Topics covered by these audits include checks of proper implementation of TC TrustCenter's certificate policies and extensive checks on key management policies, security controls, operations policy and comprehensive checks on certificate profiles.

The results of these compliance audits are documented and archived. They may be released at the discretion of TC TrustCenter's management.

8.1 Frequency or circumstances of assessment

TC TrustCenter's CAs, status verification systems, and RAs are subject to periodic compliance audits, which are no less frequent than once per year. Audits are conducted to validate ongoing compliance with the standards mentioned in section 8 above.

TC TrustCenter has the right to require periodic and aperiodic compliance audits or inspections of subordinate CA or RA operations to validate that the subordinate components are operating in accordance with the security practices and procedures described in this CPS resp. their own applicable CPS.

8.2 Identity/qualifications of assessor

The auditor performing the above mentioned audits demonstrates competence in the field of compliance audits for security and PKIs. The auditor is thoroughly familiar with requirements for the issuance and management of certificates, and with the requirements of the respective audits.

The compliance auditor performs such compliance audits as a primary responsibility.

8.3 Assessor's relationship to assessed entity

The compliance auditor is a private firm, which is independent from TC TrustCenter (in the role of the technical provider of hosting services).

8.4 Topics covered by assessment

The purpose of a compliance audit is to verify that TC TrustCenter's PKI components are complying with the statements of this CPS as well as with the requirements specified in the audit standard under consideration.

Thus, all applicable aspects of this CPS and all the standards mentioned in section 8 are covered by compliance audits.

8.5 Actions taken as a result of deficiency

TC TrustCenter's PPB (see section 1.3.5.1) may determine that a PKI component is not complying with its obligations set forth in this CPS. When such a determination is made, the PPB may

suspend operation of the affected PKI component (e.g., CA, OCSP Responder, or RA, etc.), or may direct that other corrective actions be taken which allow interoperation to continue.

When the compliance auditor finds a discrepancy between how a component operates and the requirements of this CPS, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify TC TrustCenter,
- TC TrustCenter shall determine what further notifications or actions are necessary pursuant to the requirements of this CPS or applicable Issuer Agreements, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the PPB may decide to halt temporarily operation of a CA, to revoke or request the revocation of the corresponding CA certificate, or take other actions it deems appropriate.

8.6 Communication of results

After an audit, an Audit Compliance Report, including identification of corrective measures taken or being taken, will be provided to TC TrustCenter. Such a report identifies the applicable CPS used in the assessment, including its dates and version numbers. Additionally, where necessary, the results shall be communicated as set forth in section 8.5 above.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Certificate issuance and renewal fees are in accordance with the agreement between TC TrustCenter, TC TrustCenter external CA and RA contractors, and Subscribers.

9.1.2 Certificate access fees

Certificate access fees are in accordance with the agreement between TC TrustCenter, TC TrustCenter external CA and RA contractors, and Subscribers.

9.1.3 Revocation or status information access fees

Revocation or status information fees are in accordance with the agreement between TC TrustCenter, TC TrustCenter external CA and RA contractors, and Subscribers.

9.1.4 Fees for other services

Fees for other services are in accordance with the agreement between TC TrustCenter, TC TrustCenter external CA and RA contractors, and Subscribers.

9.1.5 Refund policy

Refunds from a CA are in accordance with the respective agreement between the Subscriber and TC TrustCenter. If no such agreement exists, either TC TrustCenter's refund policy or statutory regulations apply.

9.2 Financial responsibility

For both contractual and non-contractual relying parties, the regulations of indemnification of German law are binding.

9.2.1 Insurance coverage

TC TrustCenter maintains appropriate insurances.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for End Entities

TC TrustCenter has made appropriate provisions to cover all financial expenses in case of termination.

9.3 Confidentiality of business information

Information pertaining to TC TrustCenter and not requiring protection may be made publicly available at the discretion of TC TrustCenter.

Specific confidentiality requirements for business information are defined in TC TrustCenter's Policies.

TC TrustCenter may disclose confidential information to law enforcement officials or private litigants in order to comply with valid legal processes such as a search warrant, subpoena or court order, to protect the company's rights and property, or during emergencies when TC TrustCenter believes physical safety is at risk.

9.3.1 Scope of confidential information

Confidential information includes any information provided by subscribers for purposes of obtaining certificates. Also, information provided for establishing and maintaining the provisions of subscriber agreements are considered confidential.

9.3.2 Information not within the scope of confidential information

Certificates are designed to circulate widely in technological systems, and restricting their dissemination is impractical. In accordance with standards, most applications include a copy of the relevant certificate with each digital signature or block of encrypted data. Consequently, information in a certificate is not treated as confidential as a practical matter. In addition, expiration and revocation status of a certificate must, by design, be published and is therefore not treated as confidential.

Deviations from this practice may be contractually agreed upon.

9.3.3 Responsibility to protect confidential information

All of TC TrustCenter's PKI components and external CAs and RAs shall be responsible for protecting the confidential information in their possession in accordance with this CPS and in accordance with contractual agreements with subscribers.

9.4 Privacy of personal information

9.4.1 Privacy plan

All Subscriber identifying information as defined by German privacy regulations, as well as the local privacy regulations of the issuing CA, is protected from unauthorized disclosure.

9.4.2 Information treated as private

German statutory data privacy law defines which information must be treated as private.

Further information to be treated as private can be defined in the respective Subscriber and Issuer Agreements, the respective CA's CPS.

9.4.3 Information not deemed private

Any information not specifically identified under section 9.4.2 may be treated as not private. Information included in the certificates is considered not to be private.

9.4.4 Responsibility to protect private information

Any sensitive information must be explicitly identified in the applicable CPS. All information stored electronically on TC TrustCenter's CA equipment and not in the repository, and all physical records are handled as sensitive and in accordance with TC TrustCenter's Operating Policies. Access to this information is restricted to those persons with an official need-to-know in order to perform their official duties. Sensitive information may be released in accordance with other stipulations in section 9.4.

9.4.5 Notice and consent to use private information

Requirements for notice and consent to use private information are defined in the respective contractual agreements.

9.4.6 Disclosure pursuant to judicial or administrative process

Any disclosure will be handled in accordance with German law.

9.4.7 Other information disclosure circumstances

Any disclosure will be handled in accordance with German law.

9.5 Intellectual property rights

Key pairs corresponding to certificates of TC TrustCenter's CAs are the property of TC TrustCenter.

Key pairs corresponding to certificates of subscribers are the property of the subscribers that are named in these certificates.

This CPS, the CPDs and GTCDC are © 2008 by TC TrustCenter GmbH, Germany. (See section 1.2 CPS for full identification information.)

TC TrustCenter will not knowingly violate intellectual property rights held by others.

9.6 Representations and warranties

9.6.1 CA representations and warranties

TC TrustCenter conforms to the stipulations of this document, including:

- Providing a CPS, as well as any subsequent changes, for conformance assessment;
- Conforming its practices and procedures to the stipulations of this CPS;
- Ensuring that registration information is accepted only from RAs or LRAs who understand and are obligated to comply with this CPS;
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in certificates;
- Revoking the certificates of subscribers as described in section 4.9; and

- Operating and providing for the services an on-line repository that satisfies the obligations under Section 9.6.5.

If a CA is acting in a manner inconsistent with these obligations, it will be subject to action as described in Section 8.5.

Any guarantee will be provided only as a result of the issuing of a separate written declaration of guarantee, expressly described as such.

9.6.2 RA representations and warranties

TC TrustCenter's RAs perform registration functions as described in this CPS.

If an RA is acting in a manner inconsistent with these obligations, it is subject to revocation of its RA certificate and RA responsibilities.

LRAs and Trusted Agents are bound to the same obligations as RAs.

9.6.3 Subscriber representations and warranties

Before being issued certificates, Subscribers are required to accept TC TrustCenter's General Terms and Conditions on Digital Certificates or comparable contractual agreements containing the Subscriber's obligation to exercise diligence and co-operation. The GTCDC and the contractual agreements include obligations respecting protection of the Private Key and use of the certificate.

Subscribers shall:

- Accurately represent themselves in all communications with TC TrustCenter;
- Protect their Private Keys at all times, in accordance with this CPS and TC TrustCenter's GTCDC or comparable contractual agreements;
- Notify, in a timely manner, the CA, RA, or LRA that issued their certificates of suspicion that their Private Keys are compromised or lost. Such notification shall be made directly or indirectly through mechanisms consistent with this CPS;
- Abide by all the terms, conditions, and restrictions levied upon the use of their Private Keys and certificates;
- Use certificates in accordance with this CPS.

Machine Operators assume the obligations of subscribers for the certificates associated with their Machine Subscribers.

9.6.4 Relying party representations and warranties

In general, there are no contractual relations between TC TrustCenter and Relying Parties because, when issuing a certificate, TC TrustCenter does not know to whom the certificate will be presented and who will have to rely on the certificate.

Before relying on the certificates issued under this CPS Relying Parties are recommended to adhere to the following provisions:

- Use of the certificate is limited to the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- A check is performed for each certificate for validity prior to reliance;
- Information is preserved for later verification of signature validation.

9.6.5 Representations and warranties of other participants

9.6.5.1 Repository Representations and Warranties

See Section 2.1.

9.6.5.2 Certificate Status Validation System Obligations

TC TrustCenter and its CAs represent and warrant that their Status Validation Systems, which provide revocation status and/or complete validation of certificates, are conformant to the stipulations of this CPS, including:

- Ensuring that certificate and revocation information is accepted only from valid CAs; and
- Publishing only valid and appropriate responses and maintaining evidence that due diligence was exercised in validating the certificate status.

If the Status Validation System is found to have acted in a manner inconsistent with these obligations it shall be subject to action as described in Section 8.5.

9.7 Disclaimers of warranties

Except as expressly provided otherwise in contractual agreements, any reliance on a certificate issued by TC TrustCenter is at the certificate owner's and the relying party's own risk. This CPS describes certain aspects of the public key infrastructure employed in TC TrustCenter's services, but that description is not relevant or applicable to non-participants except as promotional literature to persuade them to sign up and participate in TC TrustCenter's products or services.

Further aspects of TC TrustCenter's liability are described in clause 5 (Liability) of the GTCDC.

9.8 Limitations of liability

TC TrustCenter shall not be liable for failures which are not within their scope of responsibility, especially for technical failures or non availability of the certificate directory or specific certificates.

Like TC TrustCenter, associated RAs are only liable for matters that lie in their sphere of influence and responsibility. Any RA operating on behalf of TC TrustCenter has a contractual agreement with TC TrustCenter. An entity intending to make claims against an RA should first turn to TC TrustCenter, for one of the following reasons:

- (1) A subscriber has a contractual agreement with TC TrustCenter, not with the RA, which only acts on behalf of TC TrustCenter.
- (2) A relying party will, in general, not know the RA that committed the act leading to the claim that is made by the relying party.

TC TrustCenter will investigate facts and, should TC TrustCenter come to the conclusion that no fault can be attributed to TC TrustCenter, refer the party making claims to the relevant RA.

9.9 Indemnities

For both kinds of relying parties, contractual and non-contractual relying parties, the regulations of indemnification of German law are binding.

9.10 Term and termination

9.10.1 Term

This CPS becomes effective when approved by TC TrustCenter's PPB. This CPS has no specified term.

9.10.2 Termination

Termination of this CPS is at the discretion of TC TrustCenter's PPB.

In case of termination TC TrustCenter will inform subscribers with valid certificates (i. e., neither revoked nor expired). They will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought.

If TC TrustCenter terminates its contractual agreements with its subscribers TC TrustCenter will make a reasonable effort to archive the records of its CAs and transfer them to a specified custodian, and to establish an acceptable procedure for subscribers and relying parties for switching to a different provider of PKI services, in order to minimize the effects of TC TrustCenter ceasing to provide these services by itself.

9.10.3 Effect of termination and survival

9.10.3.1 Severability

If parts of any of the provisions in this CPS are inoperative or void, this will not affect the validity of the remaining provisions.

9.10.3.2 Survival

Despite the fact that this CPS may eventually no longer be in effect, the following obligations and limitations of the CPS shall survive: section 9.6 (Representations and warranties), section 9.2 (Financial responsibility), and section 9.3 (Confidentiality of business information).

The fact that this CPS may eventually no longer be in effect has no effect to the survival of the GTCDC.

9.11 Individual notices and communications with participants

Whenever any party wishes to or has to notify any other party with respect to this CPS, such a notice shall be given by digitally signed e-mail or in writing. The latter must be delivered either by certified mail (including return receipt request), or by a courier service confirming the delivery in writing, and it must either be addressed to the entity specified in section 1.5 or to:

TC TrustCenter GmbH
CA Administration
Sonninstrasse 24-28
20097 Hamburg
Germany

Electronic e-mail must be confirmed by the recipient within one week, by digitally signed e-mail. If the sender does not receive a confirmation within the specified time period, the notice must be re-sent in writing as described above.

9.12 Amendments

9.12.1 Procedure for amendment

TC TrustCenter's PPB reviews this CPS in regular intervals. Errors, updates, or suggested changes to this CPS shall be communicated to TC TrustCenter via the address specified in section 1.5. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2 Notification mechanism and period

This CPS and any subsequent changes will be made publicly available within one week of approval.

All policy changes under consideration by TC TrustCenter will be disseminated to subordinate CAs and other parties designated by the PPB.

9.12.3 Circumstances under which OID must be changed

The policy OIDs (see section 1.2) will only change if the change in the CPS results in a material change to the trust by the relying parties, as determined by TC TrustCenter's PPB.

9.13 Dispute resolution provisions

The use of certificates issued by TC TrustCenter is governed by contracts, agreements, and standards set forth in TC TrustCenter's GTCDC and/or dedicated contracts with subscribers. Those contracts, agreements and standards may include dispute resolution procedures that can be employed in any dispute arising from the issuance or use of a certificate governed by this CPS.

9.14 Governing law

The governing law is described in the GTCDC.

The place of jurisdiction is described in the GTCDC.

The GTCDC are available at TC TrustCenter: <http://www.trustcenter.de/en/about/repository.htm>

9.15 Compliance with applicable law

As specified in TC TrustCenter's GTCDC.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Not applicable.

9.16.2 Assignment

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns of the parties. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (e.g. as a result of merger), or otherwise, provided such assignment is undertaken consistent with this CPS's sections on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

9.16.3 Severability

If parts of any of the provisions in this CPS are incorrect or invalid, this shall not affect the validity of the remaining provisions until the CPS is updated. The process for updating this CPS is described in section 9.12.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

TC TrustCenter shall not be responsible for any breach of warranty, delay, or failure in performance under this CPS that result from events beyond its control, such as strike, acts of war, riots, epidemics, power outages, fire, earthquakes, and other disasters.

9.17 Other provisions

9.17.1 Fiduciary relationships

No fiduciary relationship between RA, CA, subscriber or relying party is represented by TC TrustCenter. TC TrustCenter does not represent, or act as agent, fiduciary, or trustee of a subscriber or relying party. TC TrustCenter cannot be bound to any obligation in any way by subscribing or relying parties, and TC TrustCenter shall make no contradicting representation in any way.

9.17.2 Administrative processes

A certified public accountant performs an audit of TC TrustCenter's balance once a year to ensure financial integrity and proper business management.

10 References

- [BSIMDS] BSI Manual for Digital Signatures on the basis of the Digital Signature Act (SigG) and the Digital Signature Ordinance (SigV).
<http://www.bsi.bund.de>
- [TS 101 456] ETSI TS 101 456: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, Version 1.4.3, May 2007, European Telecommunications Standards Institute (ETSI).
- [TS 102 042] ETSI TS 102 042 "Policy requirements for certification authorities issuing public key certificates", Version 2.1.1, May 2009, European Telecommunications Standards Institute (ETSI).
- [TS 102 176] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".
- [EU-DIR] Directive 1999/93/EC, European Parliament and of the Council: Community Framework for Electronic Signatures, dated 13 December 1999
- [RFC2459] Internet X.509 Public Key Infrastructure
Certificate and CRL Profile
<http://www.ietf.org/rfc/rfc2459.txt>
- [RFC3647] Internet X.509 Public Key Infrastructure
Certificate Policy and Certification Practices Framework.
<http://www.ietf.org/rfc/rfc3647.txt>
- [RFC2828] Internet Security Glossary.
<http://www.ietf.org/rfc/rfc2828.txt>
- [RFC3280] Internet X.509 Public Key Infrastructure
Certificate and Certificate Revocation List (CRL) Profile
<http://www.ietf.org/rfc/rfc3280.txt>
- [SIGG] Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations of 16 May 2001 (Federal Law Gazette I, p. 876), last amended by Art. 1 of the First Act Amending the Signature Law (First Signature Amendment Act - 1. SigÄndG) of 4 January 2005 (Federal Law Gazette I, p. 2)
<http://www.bundesnetzagentur.de/media/archive/3612.pdf>
- [SIGV] Ordinance on Electronic Signatures (Signatures Ordinance – SigV) of November 16th, 2001 last amended by Article 2 of the First Act Amending the Signatures Act
<http://www.bundesnetzagentur.de/media/archive/3613.pdf>
- [X509] ISO/IEC 9594-8, Information Technology – Open Systems Interconnection – The Directory: Authentication Framework. Also published as ITU-T X.509 Recommendation. See the edition ITU-T Rec. X.509 (1993 E) or ISO/IEC 9594-8:1995 with Technical Corrigendum 1 and Amendment 1 (Certificate Extensions) applied for X.509v3 certificates.

11 Glossary

A

ACTIVATION DATA

Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e. g., a PIN or a passphrase).

ASYMMETRIC ALGORITHM

Unlike symmetric algorithms, asymmetric (or public key) encryption algorithms use two different keys for encryption and decryption, where either one cannot be computed from the other.

AUTHENTICATION

Authentication refers to the process of confirming either a person's identity or the integrity of information (or both).

B

BLOCK CIPHER

A block cipher is a symmetric algorithm that encrypts larger blocks of text of fixed size, usually 64 bits (equal to eight characters). Examples of block ciphers are IDEA, DES and Triple-DES. See also stream cipher.

BSI

The BSI is the German government authority for Security in Information Technology. Among other things, it publishes provisions regarding the Digital Signature Act.

BUNDESANZEIGER

The Bundesanzeiger is a publication where the German government authorities officially make public announcements and place official notices regarding federal laws, ordinances and related provisions.

BUNDESNETZAGENTUR (BNETZA)

The Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway is a separate higher federal authority within the scope of business of the Federal Ministry of Economics and Labour, and has its headquarters in Bonn. On 13 July 2005 the Regulatory Authority for Telecommunications and Posts which superseded the Federal Ministry of Posts and Telecommunications (BMPT) and the Federal Office for Posts and Telecommunications (BAPT), was renamed Federal Network Agency. Moreover, it acts as the root certification authority as provided for by the Electronic Signatures Act.

The Federal Network Agency's task is to provide, by liberalization and deregulation, for the further development of the electricity, gas, telecommunications and postal markets and, as from 1 January 2006, also of the railway infrastructure market. For the purpose of implementing the aims of regulation, the Agency has effective procedures and instruments at its disposal including also rights of information and investigation as well as the right to impose graded sanctions. (From the BNetzA Web site.)

C

CA

See Certification Authority.

CERTIFICATE

A certificate binds a public key to the entity named in the certificate (the subject) that holds the corresponding private key. A certificate can be thought of as an electronic ID card. It also identifies the Certification Authority that issued the certificate. The certificate formats most widely used today are PGP and X.509.

CERTIFICATE APPLICATION

In the context of this document, the term "certificate application" refers to all the information a subscriber submits to the Certification Authority in applying for a certificate. This information includes, but may not be limited to, the (digital) certificate request, personal data, a photocopy of his ID card etc. See also certificate request.

CERTIFICATE CLASS

TC TrustCenter issues certificates according to different certificate classes, each of which has a different level of subscriber authentication. See also Certificate Policy.

CERTIFICATE POLICY

To allow an estimation of the trustworthiness of issued certificates a CA publishes a Certificate Policy (CP) describing the requirements which a Certification Authority (CA) shall employ in issuing certificates to subscribers. While a CPS is prepared by a Certification Authority, any organization may define a Certificate Policy.

CERTIFICATE POLICY DEFINITIONS

A named set of rules that indicates the applicability of a certificate to a particular community and / or class of applications with common security requirements. The TC TrustCenter Certificate Policy Definitions (CPD) is a document describing a set of certificate rules that TC TrustCenter supports. It is available from the repository.

CERTIFICATE REQUEST

In the context of this document, the term "certificate request" refers to the digitally self-signed public key of the subscriber, which may either be encoded in binary or text form. The certificate request is transformed into a certificate by replacing the owner's signature on the public key with the CA's signature, thereby binding the public key to the entity named in the certificate. See also certificate application.

CERTIFICATE REVOCATION LIST

A list that contains revoked certificates which the CA has issued. If a CA issues certificates under different Certificate Policies, with a different signing key being used for each policy, there will usually be one CRL for each policy, and each of these lists is signed by the private signing key that was used in issuing the certificates on that particular list.

CERTIFICATION AUTHORITY

A Certification Authority is trustworthy institution that certifies public keys, i. e. issues certificates. For this purpose, the information to be related to the public key, in particular the key holder's identity, is verified. TC TrustCenter is an example of a CA.

CERTIFICATION PATH

An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

CERTIFICATION PRACTICE STATEMENT

A statement of the practices which a Certification Authority employs in issuing certificates. See also Certificate Policy and Certificate Policy Definitions.

CERTIFICATION SERVICES PROVIDER

A Certification Services Provider is a third party that manages any of the services that a Certification Authority generally provides, such as issuing certificates, a directory service, an online certificate status responder or end entity registration.

CERTIFY

To digitally sign another entity's public key by using one's own private key.

CONFIRM

To ascertain through appropriate inquiry and investigation.

CORRESPOND

To belong to the same key pair.

CPD

See Certificate Policy Definitions.

CPS

See Certification Practice Statement.

CRL

See Certificate Revocation List.

CRYPTANALYSIS

Cryptanalysis deals with the breaking of encryption algorithms, i. e. decrypting coded messages.

CRYPTOGRAPHY

Cryptography is the science of keeping messages secret.

CRYPTOLOGY

Cryptology is the area of mathematics that combines cryptography and cryptanalysis.

CSP

See Certification Services Provider.

D

DECRYPTION

The process of unscrambling encrypted data.

DES

DES (Data Encryption Standard) is a block cipher developed by IBM in the early 1970s. Initially, the key size used in the algorithm was 128 bits, but the NSA reduced it to 56 bits, which is considered too weak nowadays. A DES variant known as Triple DES offers better security.

DH

See Diffie-Hellman.

DIFFIE-HELLMAN

Diffie-Hellman is a secure public key exchange algorithm invented by Whitfield Diffie and Martin Hellman in 1976. The Diffie-Hellman patent expired in 1997.

DIGITAL CERTIFICATE

See certificate.

DIGITAL SIGNATURE

A digital signature is a small block of data (hash value) that is encrypted using the sender's private key and appended to the original data to provide authenticity and integrity. The digital signature is checked using the sender's public key.

DIGITAL SIGNATURE ACT

The German Digital Signature Act (SigG) and the Digital Signature Ordinance (SigV) aim "to establish general conditions under which digital signatures are deemed secure and forgeries of digital signatures or manipulation of signed data can be reliably ascertained." It came into force on August 1st, 1997. Some revisions that reflect the experiences gained thus far, and implement Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures have been published 2001 and 2004.

DISTINGUISHED NAME

Strictly speaking, a Distinguished Name (DN) is a path through an X.500 directory information tree which uniquely identifies an entity. An X.500 directory tree is a hierarchical structure, and because information like an e-mail address follows no such hierarchy, it should not be part of a DN. Most DNs do, however, contain an e-mail address, and a DN is commonly understood to be comprised of the collection of data fields that make up a standard X.509, i. e., Country (C), State / Province (SP), Locality (L), Organization (O), Organizational Unit (OU), Common Name (CN), and Email. A DN following this scheme might look like the following: /C=US/SP=Washington/L=Seattle/O=My Company, Inc./OU=Internet Services/CN=John [Doe/Email=doe@mycompany.com](mailto:doe@mycompany.com).

DN

See Distinguished Name.

DSA

A public key signature algorithm proposed by NIST for use in DSS that uses a variable key size from 512 to 1024 bits.

DSS

DSS (Digital Signature Standard) is a digital signature standard proposed by NIST. DSS is used, for instance, by PGP version 5.0 and above.

E

ENCRYPTION

The process of scrambling and rendering data useless for anyone other than the intended recipient.

ENTITY

See person.

F

FINGERPRINT

The fingerprint is an extract of the public key (usually 128 or 160 bits in size) that is used to readily verify that one has the correct key, i. e. that the key belongs to the entity named in the certificate, without having to check that the entire key (usually 1024 bits and above) matches exactly. It is computed by applying a hash function to the public key.

G

GENERAL TERMS AND CONDITIONS

TC TrustCenter's services and offers are provided on the basis of the General Terms and Conditions. These are available from the repository.

GTCDC

See General Terms and Conditions on Digital Certificates.

H

HASH FUNCTION

A hash function generates a short extract of fixed length (MD5: 128 bits = 16 characters, SHA-1: 160 bits = 20 characters, SHA-256: 256 bits, etc.), the hash value, from any given data in such a way that the original data cannot be derived from the extract, and that it is infeasible to construct other data that produces the same hash value. However, some hash functions are deemed broken and should not be used any longer. Hash functions are used e.g. to support digital signatures. For example, the hash value derived by applying the hash function to the body (the message text) of an e-mail is then encrypted using the private key in order to digitally sign the e-mail.

HYBRID ALGORITHMS

A hybrid encryption algorithm combines symmetric and asymmetric algorithms in order to make use of their respective advantages, higher speed (symmetric) and easier key exchange (asymmetric).

I-J

IETF

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

ISSUE A CERTIFICATE

The process of a CA signing an end user's public key, thus creating the certificate, and notifying the subscriber of its contents.

K

KEY

A digital code used to encrypt, decrypt, create and verify digital signatures. Keys used for asymmetric algorithms come in pairs, and anything encrypted with either one of them must be decrypted with the other. Symmetric algorithms, however, use the same key for both encryption and decryption, and there is no concept of a digital signature.

KEY PAIR

The set of keys used for asymmetric algorithms. See also: key.

KEY RING

The key ring is the file PGP keeps the public (or private) keys in.

L

LAN

Local Area Network.

LDAP

A protocol for accessing on-line directory services. LDAP was defined by the IETF in order to encourage adoption of X.500 directories. The Directory Access Protocol (DAP) was seen as too complex for simple Internet clients to use. An LDAP directory entry is a collection of attributes with a name, called a distinguished name (DN). The DN refers to the entry unambiguously. Each of the entry's attributes has a type and one or more values. The types are typically mnemonic strings, like

"CN" for common name, or "mail" for e-mail address. The values depend on the type. For example, a mail attribute might contain the value "john.doe@company.com". LDAP directory entries are arranged in a hierarchical structure that reflects political, geographic, and / or organizational boundaries.

M

MD5

MD5 is a 128 bit hash function developed by Ron Rivest. It is widely used, and PGP uses it in conjunction with the RSA algorithm. Since MD5 has been found to have weaknesses, algorithms from the SHA-family are to be preferred, although these weaknesses are hard to exploit in practice.

N

NIST

The NIST (National Institute for Standards and Technology) is a branch of the US Department of Commerce that proposes open interoperability standards.

NSA

The NSA (National Security Agency) is a cryptologic organization of the US government that deals with the development and the cryptanalysis of encryption algorithms.

O

ONE-WAY FUNCTION

See hash function.

P

PASS PHRASE

A pass phrase, just like a pass word, is used to deny unauthorized access to confidential data. A pass phrase consists of several words, punctuation marks and numbers to provide better security than a simple pass word. A pass phrase is used, for instance, to protect the private key.

PEM

PEM (Privacy-Enhanced Mail) is an Internet mail standard that implements protocols for encryption, message integrity, key management and authentication (see digital signature). PEM uses RSA keys ranging from 508 to 1024 bits. PEM certificates are based on the X.509 format.

PERSON

A human being or any organization capable of signing a document, either legally or as a matter of fact.

PGP

PGP (Pretty Good Privacy), developed by Phillip Zimmermann, is a popular and very widely used application for exchanging secure e-mail and encrypting files. Non-commercial use is free, commercial users will have to obtain a license from PGP Inc., now owned by Network Associates Inc.

PIN

Personal Identification Number.

PRIVATE KEY

Of the key pair used in asymmetric algorithms, the private key is the one that must be kept secure by its owner. No one else must have access to this key. Usually, the private key is protected by a pass word or a pass phrase. It is used for decrypting messages sent to the owner of the corresponding public key and for generating digital signatures.

PUBLIC KEY

Of the key pair used in asymmetric algorithms, the public key is the one that is made publicly available, e. g. on a public key server. Its purpose it to encrypt messages sent to the key owner and to verify digital signatures that the latter has made using the corresponding private key. A public key certified by a Certification Authority is a called a certificate.

PUBLIC KEY ENCRYPTION ALGORITHM

See asymmetric algorithm.

PUBLIC KEY EXCHANGE ALGORITHM

A public key method for exchanging session keys. Most public key algorithms are simply used for exchanging secret keys for symmetric encryption algorithms, not for encryption of data. Diffie-Hellman is suitable for key exchange only, while RSA is a public key encryption algorithm.

PUBLIC KEY SERVER

A public key server is a public key directory, much like a public telephone book, which lists user names and their public keys for easy access.

Q-R

RA

See Registration Authority.

REGISTRATION AUTHORITY

An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates, i. e., an RA is delegated certain tasks on behalf of a CA.

RELYING PARTY

A recipient of a certificate who acts in reliance on that certificate and / or digital signatures verified using that certificate.

REPOSITORY

A collection of databases for storing and retrieving certificates, CRLs and any other information related to certificates and digital signatures, for example this CPS.

REVOCAION

Revocation is the process of declaring one's public key as no longer valid. This is normally done because its owner can no longer guarantee that he has sole access, and that his private key has not been compromised. By revoking the corresponding public key one aims to prevent others from doing any damage by pretending to be the key's owner. Revoking the key lets people know that the public key should no longer be used to encrypt any messages or files, and that digital signatures made using this key should no longer be accepted. The revoked key is then placed on a CRL (Certificate Revocation List) by a Certification Authority so that anyone can check whether a public key is still valid.

RSA

RSA is the name of the asymmetric algorithm developed by the US-based company of the same name, RSA Data Security Inc. Its security is based on the fact that it is easy to multiply two large primes (with several hundred decimal digits each) but very hard to factor them out of the product.

The abbreviation RSA refers to the three inventors of the algorithm: Ron Rivest, Adi Shamir und Leonard Adleman.

S

SECRET KEY

See private key.

SECRET KEY ALGORITHM

See symmetric algorithm.

SELF-SIGNED

A public key is referred to as self-signed if it is digitally signed using the corresponding private key.

SESSION KEY

In hybrid algorithms, the key used for the symmetric encryption algorithm and exchanged via the public key algorithm. The session key is randomly generated for each exchange of data, i.e. for each session, while the public key remains the same over a longer period of time.

SET OF PROVISIONS

A collection of practice and / or policy statements, spanning a range of standard topics, for use in expressing a CPD or CPS.

SHA-1

SHA-1 is a 160 bit hash function developed by NIST that is used in the DSS.

SIGG

See Digital Signature Act.

SIGV

See Digital Signature Act.

S/MIME

S/MIME (Secure Multipurpose Mail Extension) is a standard suggested by a group of software developers lead by RSADSI that provides encryption and digital signatures for exchanging secure e-mail. S/MIME certificates are based on the X.509 format.

SSL

SSL (Secure Socket Layer) is a protocol developed by Netscape that aims to provide secure data exchange over the Internet. SSL is supported and used by all modern Internet browsers in order to protect the communication and the transfer of sensitive data on the world wide Web through encryption. Unfortunately, the export versions of these applications that are available outside of the United States are limited to a weak 40 bit encryption (instead of 128 bit) due to export restrictions. SSL certificates are based on the X.509 format.

STEGANOGRAPHY

In contrast to cryptography, steganography aims to conceal that there actually is any secret message by hiding the confidential message in other data (e. g. in a digital image).

STREAM CIPHER

A stream cipher is a symmetric algorithm that encrypts the message character by character. See also block cipher.

SUBSCRIBER

A person that is the subject named in a certificate and holds the private key corresponding to the public key listed in the certificate.

SUSPENSION

Suspension is the process of placing one's certificate on hold, i. e., declaring it as temporarily invalid. This is normally done because the subscriber suspects that his private key has been lost or compromised. By suspending the corresponding public key one aims to prevent others from doing any damage by pretending to be the key's owner. Suspending the key lets people know that, for the time being, the public key should not be used to encrypt any messages or files, and that digital signatures made using this key should not be accepted at the moment. A suspended key must either be revoked upon confirming that the private key has indeed been lost or compromised, when it is placed on a CRL (Certificate Revocation List) by the issuing Certification Authority, or the suspension may be lifted, if, for example, the private key has been recovered (i. e., is not lost).

SYMMETRIC ALGORITHM

In contrast to asymmetric algorithms, the key used for decryption (or encryption) can be computed from the other key in a symmetric (or conventional) encryption algorithm. Most of the time both keys are the same.

T

TIME-STAMP

An indication of (at least) the date and time a document was signed and by whom.

TRIPLE-DES

A variant of the DES algorithm where DES (key size 56 bits) is used three times with three different keys. The effective key size is only 112 bits (and not 168 bits, as one might expect).

U-V

USER ID

A PGP data structure containing the key owner's identity. The commonly used format is "Full name <e-mail address>", e. g. "John Doe <jdoe@company.com>".

W-Z

WAN

Wide Area Network.

X.509

X.509 is a standard certificate format of the ITU-T (International Telecommunication Union-Telecommunication). It contains the name of the issuer, usually a Certification Authority, information about the key owner's identity and the digital signature of the issuer. Both SSL and S/MIME are based on the X.509 format.