TRUSTCENTER
Identity Verification Services

TC TrustCenter GmbH Certification Practice Statement and Certificate Policy for Qualified Certificates

Version 1.0 of June 11th, 2007

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 [RFC2527]).

TC TrustCenter
Certification Practice Statement and Certificate Policy for Qualified Certificates

Version 1.0 of June 11th, 2007

1 Introduction

Doing business and communicating across public and private networks becomes more and more important in electronic commerce.. One requirement of such electronic communication is the ability to identify the originator of electronic information in the same way that documents are signed using a hand-written signature. Technically this can be achieved by electronic signatures. The value of electronic signatures increases significantly if the assignment of an electronic signature to an individual is done by an independent and reliable third party. This third party is commonly called a Certification Service Provider (CSP) or Certification Authority (CA). A Certification Authority issues certificates binding a public key to the entity named in the certificate and holding the corresponding private key.

For users of electronic signatures to have confidence in the authenticity of the electronic signatures they need to have confidence that the CA has properly established procedures and protective measures in order to minimize the operational and financial threats and risks associated with the issuance of certificates.

The Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures [EU-DIR] identifies a special form of electronic signature which is based on a "qualified certificate". Annex I of this Directive specifies requirements for qualified certificates. Annex II of the Directive specifies requirements on Certification Service Providers issuing qualified certificates (i.e. Certification Authorities issuing **qualified** certificates).

This document specifies the practices of the operation and management of TC TrustCenter's CAs issuing qualified certificates in accordance with the Directive 1999/93/EC, in accordance with the German Signature Act, and in accordance with the European Telecommunications Standards Institute's Technical Specification 102 456 (ETSI TS 101 456): Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.

It is common practice for a CA to have two documents in place:

- a CPS describing the practices which a Certification Authority employs in managing certificates (application, issuance, use, and revocation)
- a Certificate Policy (CP) describing the vetting processes and allowing an estimation of the trustworthiness and reliability of certificate contents based on the extent of verification steps undertaken to verify the contents of certificates.

This document considers qualified certificates only. Because all qualified certificates underlie the same regulations and requirements defined in the Directive 1999/93/EC and in the German Signature Act both above mentioned documents (CPS and CP) have been merged into one single document, this CPS/CP.

This CPS/CP in combination with TC TrustCenter's organization, processes, and procedures has been assessed by independent auditors to be compliant to the standard „ETSI TS 101 456 – Policy requirements for certification authorities issuing qualified certificates", Version 1.4.1 of the European Telecommunications Standards Institute (ETSI).

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 technique 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.

A certificate is, in essence, a digitally signed public key. It always contains the name of 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 signatures might be forged.

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 it is signed by the CA.

TC TrustCenter offers several certificate classes that are described in the corresponding Certificate Policy Definitions (CPD). These certificates are so-called advanced certificates; they can be used for digital signatures as well as for encrypting data. They may be issued to individuals as well as to electronic devices. There is no governmental regulation on how and for which purposes these certificates may be used.

In contrast to the above mentioned advanced certificates qualified certificates issued in compliance with [EU-DIR] and [GSA] produce electronic signatures which are legally considered as being equivalent to handwritten signatures. As a natural consequence qualified certificates may be issued to individual persons only.

To allow an estimation of the trustworthiness of issued qualified certificates and to prove compliance the "Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures" in combination with the German Signature Act, and in compliance with the requirements of ETSI TS 101 456 TC TrustCenter publishes this CPS/CP describing the procedures used for the issuance of qualified certificates as well as a description how the verification of data contained in a certificate is done.

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

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

As mentioned above, for qualified certificates these two documents have been merged into one single document.

This CPS/CP describes the structure and practices of TC TrustCenter. it does neither constitute a declaration of self-escrow, nor does it state legally binding warranties.

This CPS/CP 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 Glossary (Chapter 10). The glossary also provides the definitions of some important terms not appearing elsewhere in this text that relate to the areas mentioned above.

1.2 Identification

TC TrustCenter GmbH of Sonninstrasse 24-28, 20097 Hamburg, Germany (referred to as "TC TrustCenter" in this CPS/CP), is an international Certification Authority and Certification Services Provider (CSP). TC TrustCenter issues a wide variety of certificates, such as X.509 and WTLS certificates. These can be used with a number of applications and for a wide variety of purposes, such as secure e-mail, software signing and secure server connections, for both standard Web servers and mobile WAP servers. TC TrustCenter issues certificates under its own policies, as defined in the Certificate Policy Definitions, under policies of third parties that use TC TrustCenter as their CSP, such as Identrus Level One Participants, and under the regulations of the German Signature Act.

This CPS/CP supports the certificates issued by TC TrustCenter under the regulations of the German Signature Act available from http://www.bundesnetzagentur.de.

This Certification Practice Statement and Certificate Policy is available upon request by e-mail. It may also be retrieved from http://www.trustcenter.de/cps.

1.3 Community and Applicability

This CPS/CP adheres to the structure laid out in [RFC2527], "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", © 1999 by the Internet Society, in order to facilitate comparison with other Certification Practice Statements and to ease interoperability between the certificates issued by different CAs, thereby promoting electronic commerce.

This CPS/CP is intended for qualified certificates which

a) meet the requirements laid down in annex I of the Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures,

b) are issued by a CA who fulfils the requirements laid down in annex II of the Directive 1999/93/EC,

c) are for use only with secure signature creation devices (SSCD) which meet the requirements laid down in annex III of Directive 1999/93/EC

d) are issued to the public.

Qualified certificates issued under this CPS/CP may be used to support electronic signatures which "satisfy the requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper based data", as specified in article 5.1 of the Directive 1999/93/EC.

1.3.1 Certification authorities

TC TrustCenter operates a Certification Authority. 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 Signature Act. TC TrustCenter provides information about other subsidiary or cooperating CAs upon request.

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 fulfil the requirements of the superior CA. When registering applicants; Sub-CAs are allowed to perform additional or more extensive checks.

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 as well 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 on of the RO certificates will be accepted by the CA system. As the supervising governmental authority the Federal Network Agency will be informed about all subsidiary RAs becoming operational.

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 Ident Points®, or

(2) German Post Offices, or

(3) Authorized identification points in organizations.

A TC TrustCenter Ident Point® provides the service of personal identification on behalf of and exclusively for TC TrustCenter. This results in a more efficient handling of registering end users. The post offices offer identification services in compliance with the German Signature Act to all certificate service providers. Identification points in organizations may be installed if an organization intends to equip several of its employees with certificates.

Personal identification of end users applying for a certificate may also be performed by mobile identification officers operating on behalf of TC TrustCenter.

1.3.3 End entities

In the context of this document, end entity (or end user) is a synonym for subscriber (or person). It refers to natural persons who use qualified certificates issued by TC TrustCenter.

1.3.4 Applicability

Technically, all applications in the areas of electronic signatures and secure Internet communication are suitable for use with qualified certificates issued under the terms of this CPS/CP.

This CPS/CP supports certificates:

a) which meet the requirements laid down in annex I of [EU-DIR];

b) are issued by TC TrustCenter in compliance with the requirements laid down in annex II of [EU-DIR];

c) which are for use only with secure signature creation devices which meet the requirements annex III of [EU-DIR];

d) are issued to the public.

Qualified certificates issued under this CPS/CP may be used to support electronic signatures which "satisfy requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper based data", as specified in article 5.1 of [EU-DIR].

1.4 Contact details

1.4.1 Specification administration organization

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

1.4.2 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

1.4.3 Person determining CPS suitability

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

2 General Provisions

For the purposes of the service, the repository and the binding legal rules TC TrustCenter refers to the German Law. Under binding consumer protection laws it is not possible to agree with an end user on such a long document like this CPS. Any arising questions which are not covered by this CPS/CP are to be answered by binding codified German law.

Furthermore, for digital certification services offered by TC TrustCenter under the German Signature Act, the provisions of the German Signature Act may be treated as a certification policy of this regulated service and the German Signature Ordinance as a certification practice statement.

In no event, this CPS/CP shall be treated, understood, agreed or regarded as warranty, representation, reassurance or assurance of quality in relation or respect to the GTC.

2.1 Obligations

2.1.1 CA obligations

TC TrustCenter provides its certification services for qualified certificates in compliance with this CPS/CP and in compliance with the German Signature Act.

TC TrustCenter implements measures and procedures for providing certification services for qualified certificates as described in §§ 4 and 5 of this CPS/CP.

TC TrustCenter has the responsibility for conformance with the procedures prescribed in this policy, even when the CA functionality is undertaken by sub-contractors.

The primary purpose of any Certification Authority is to provide Certificate management services (generation, operational use, Revocation and Expiry) for customers within their respective policy domain(s).

Each of TC TrustCenter's CAs uses its own key pairs. The private keys of CA certificates are used to sign certificates to subscribers.

The CA's keys for the issuance of qualified certificates are generated on a secure signature creation device in a physically secure facility at TC TrustCenter's premises.

TC TrustCenter's CA for qualified certificates performs the following functions:

1. Generate its own keys.
2. Operate the Certification Authority in an efficient and trustworthy manner and in accordance with this CPS/CP and the German Signature Act.
3. Establish subordinate Registration Authorities if necessary.
4. On the receipt of a authenticated certificate application, issue qualified certificates that meet the X.509 certificate standard, the ETSI TS 101 456 requirements, and the requirements of the request.
5. Ensure that the certificates are free from data entry errors and factually correct based on the information known to the CA at the time of issuance.
6. Inform the applicant of the measures needed to increase the security of qualified electronic signatures and to test them reliably.
7. Remind the applicant that data with a qualified electronic signature may have to be signed again as soon as the security value of the current signature is reduced due to the passing of time.

8. Inform the applicant that a qualified electronic signature has the same effect in legal transactions as a handwritten signature unless otherwise specified by law.
9. Revoke certificates on receipt of authenticated revocation requests, or in compliance with § 3.4 or § 4.5 of this CPS/CP
10. Post Revocation information to its directory services or OCSP responders or issue CRLs
11. Promptly notify the owner of the certificate about the revocation
12. Conduct regular security audits to prove compliance with ETSI TS 101 456.

In addition, TC TrustCenter reserves the right to investigate compromise and suspected compromises of private keys, non-compliance or suspected non-compliance with the stipulations of this CPS/CP in order to protect the integrity of the community of all subscribers, and take actions it deems appropriate based on its findings.

Investigations may include, but are not limited to:

1. Interviews with operational staff of RAs
2. A review of applicable system logs, operational records and other related files or documents, including e-mails
3. An audit of operational procedures
4. An audit of security controls, procedures, and measures
5. Request for information.

These rights and obligations may be addressed in greater detail in contractual agreements with Subscribers.

2.1.2 RA obligations

An RA is associated with one or more CAs and acts on behalf of its CAs. 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 and certificate revocation to the CA
- Identification and authentication of appliants and third parties
- Information of subscribers about the proper use of qualified certificates
- Handing over smart cards to applicants and activating certificates
- Tracking logistics of certificate lifecycle
- Validation of revocation requests.

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

An RA Officers must not use his/her private RA keys for any other purpose than those associated with its RA function without the express permission of TC TrustCenter. The RA must comply with the provisions in this CPS/CP, those in ETSI TS 101 456, and those in the German Signature Act; this includes, but is not limited to: ensuring that the requirements specified in § 4 CPS/CP are met, and that the controls defined in §§ 5 and 6 CPS/CP are provided; keeping subscriber information confidential according to § 2.8 CPS/CP; and performing the authentication procedure as defined in § 3 CPS/CP.

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 TC TrustCenter must not be publicly accessible, and 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 by TC TrustCenter.

2.1.3 Subscriber obligations

The obligations of the subscribers can be derived from the German Signature Act.

It is recommended that subscribers use signature-application components that clearly indicate the production of a qualified electronic signature and enable the subscriber to identify the data to which the signature refers. To check signed data signature-application components are needed that will show

- To which data the signature refers
- Whether the signed data are unchanged
- To which signature-code owner the signature is assigned to
- The contents of the qualified certificate on which the signature is based, and
- The results of the subsequent validity check of certificates.

2.1.4 Relying party obligations

A relying party shall

- verify the validity or revocation of the certificate using current revocation status information
- take account of any limitations on the usage of the certificate indicated to the relying party in the certificate
- take any other precautions prescribed in agreements or elsewhere.

2.1.5 Repository obligations

TC TrustCenter will update its repository, consisting of the relevant policies, the directory of downloadable certificates, and the status checking service, within a reasonable amount of time, at least once in 24 hours, to reflect new information concerning the validity and reliability of the certificates issued.

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.

TC TrustCenter protects the integrity and authenticity of all systems providing certificate status information.

In compliance with the German Signature Act revocation status information for qualified certificates is available from TC TrustCenter for at least 5 years after a certificate has expired.

Status information for qualified certificates issued by TC TrustCenter's accredited CA is available for at least 30 years after a certificate has expired.

2.2 Liability

2.2.1 CA liability

As a certification services provider issuing qualified certificates to the public TC TrustCenter is liable as specified in § 11 of the German Signature Act.

As a certification services provider under the German Signature Act TC TrustCenter is obliged to make appropriate cover provisions to ensure to be able to meet the statutory obligations for reimbursement of damages caused by an infringement.

2.2.2 RA liability

Like TC TrustCenter, the RA is only liable for matters that lie in its 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 because

> (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.

2.3 Financial responsibility

2.3.1 Indemnification by relying parties

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

2.3.2 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.

2.3.3 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.

2.4 Interpretation and Enforcement

2.4.1 Governing law

The law of the Federal Republic of Germany is applicable, expressly excluding international private law and the UN Treaty on International Sale of Goods.

Regulations for providing certification services for qualified certificates are especially defined in the German Signature Act [GSA] and in the German Signature Ordinance [GDSO].

2.4.2 Severability, survival, merger, notice

2.4.2.1 Severability

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

2.4.2.2 Survival

Despite the fact that this CPS/CP may eventually no longer be in effect, the following obligations and limitations of the CPS/CP shall survive: § 2.1 (Obligations), § 2.2 (Liability), § 2.3.3 (Administrative processes), § 2.4 (Interpretation and Enforcement) and § 2.8 (Confidentiality).

2.4.2.3 Merger

Any modification of the provisions of this CPS/CP directly affecting TC TrustCenter's rights and obligations must be published as a digitally signed message or document, except as provided elsewhere in this CPS/CP.

2.4.2.4 Notice

Whenever any party wishes to or has to notify any other party with respect to this CPS/CP, 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 be addressed 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.

2.4.3 Dispute resolution procedures

It is in the interest of TC TrustCenter as a Certification Authority and trusted third party to resolve any dispute promptly and efficiently. Therefore, any party intending to make claims should contact TC TrustCenter first, regardless of the nature of the claim.

Dispute resolution procedures relating to disputes between TC TrustCenter and Customers can be set forth in the agreements between the parties. Dispute resolution procedures relating to disputes between TC TrustCenter and Subscribers can be set forth in contractual agreements with Subscribers.

In any case of dispute, claim, or controversy in connection with or relating to this CPS/CP or any qualified certificate issued by TC TrustCenter TC TrustCenter can be contacted by e-mail to dispute@trustcenter.de.

Disputes may also be reported to:

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

2.5 Fees

TC TrustCenter charges fees for the use of certain services that TC TrustCenter offers to its Subscribers. An up-to-date list of current fees is available from TC TrustCenter's product pages: http://www.trustcenter.de/en/produkte/index.htm.

2.6 Publication and Repository

2.6.1 Publication of CA information

TC TrustCenter will publish this CPS/CP at http://www.trustcenter.de/repository.

TC TrustCenter's issuer (root) certificates, which may also be used for on-line certificate status inquiries, are accessible from the repository as well.

The directory of all accessible and downloadable qualified certificates issued by TC TrustCenter is available at http://dir.trustcenter.de.

Qualified certificates are accessible for download only if the certificate holder has agreed to the publication of the certificate.

Certificate Revocation Lists (CRLs) for qualified certificates are currently not publicly available.

TC TrustCenter offers an OCSP service for certificate status requests.

2.6.2 Frequency of publication

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

The database providing status information for qualified certificates is updated every time a certificate is released or revoked. Any other information listed in § 2.6.1 is updated every time it is modified.

2.6.3 Access controls

Only authorized personnel is able to publish or modify any information referred to in § 2.6.1.

2.6.4 Repositories

For the location of the certificate repository and the CPS/CP please refer to § 2.6.1.

The TC TrustCenter support center is available at the following URL: http://www.trustcenter.de/support.

2.7 Compliance audit

TC TrustCenter is subject to regular external audits. These include audits pursuant to the German Signature Act, TC TrustCenter acting as a CSP for IdenTrust Level One Participants, an audit for MBA/SISAC compliance, and an ETSI TS 102 042 as well as an ETSI TS 101 456 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 for the issuance of qualified certificates only.

This CPS/CP specifies the practices of the operation and management of TC TrustCenter's CAs issuing qualified certificates in accordance with the European Telecommunications Standards Institute's Technical Specification 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

All of these audits require demonstration of a maximum level of security and conformity to documented policies and practices. The respective provisions supplement each other and serve to enhance the overall security controls.

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.

2.8 Confidentiality

TC TrustCenter keeps information confidential.

TC TrustCenter's directory of certificates transmits the data stated in the certificate to all requesting entities. Qualified certificates can be retrieved only if the certificate holder has agreed to the publication of the certificate.

TC TrustCenter collects, processes, and utilises the personal and organisation-related data only as appropriate and necessary for the issuance of a qualified certificate.

TC TrustCenter will not transmit data contained in certificates to third parties for advertising purposes. TC TrustCenter does not make any further commercial use of the data obtained in connection with an application for a certificate.

TC TrustCenter protects all personal and organisation-related data which is not included in the certificate against unauthorised access. TC TrustCenter reserves its right to mention an organisation as a customer.

2.9 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/CP is the intellectual property of TC TrustCenter.

3 Identification and Authentication

3.1 Initial Registration

In order to obtain a qualified certificate, any subscriber must apply for a certificate, and identify and authenticate himself to TC TrustCenter.

TC TrustCenter ensures that subscribers are properly identified and authenticated; and that subject certificate requests are complete, accurate, and duly authorized.

Before a qualified certificate is issued TC TrustCenter informs the subscriber of the terms and conditions regarding use of the certificate as regulated in § 7.3.4 of Directive 1999/93/EC, annex II (k)), and § 6 of the German Signature Act. This information is communicated by TC TrustCenter through a durable (i.e. with integrity over time) means of communication and in readily understandable language. It may be transmitted electronically.

Details of the identification are regulated by the Directive 1999/93/EC and the German Signature Act. Submitted documents may be in the form of either paper or electronic documentation.

TC TrustCenter verifies at time of registration by appropriate means and in accordance with German law the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued.

3.1.1 Types of names

All names specified in X.509 certificates must be expressed as X.509 Distinguished Names (DNs).

3.1.2 Need for names to be meaningful

TC TrustCenter will determine the subscriber's DN to make it compliant with common standards, practices and other regulations.

The name 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.

However, the German Signature Act demands that the applicant can choose a pseudonym instead of the clear name in the qualified certificate. TC TrustCenter will issue such pseudonymized certificates; the use of a pseudonym is indicated by the suffix ":PN" in the Common Name field of the certificate.

3.1.3 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.

3.1.4 Uniqueness of names

Any DN in a qualified certificate issued by TC TrustCenter must uniquely identify a single entity among all of TC TrustCenter's subscribers of qualified certificates. 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.

3.1.5 Name claim dispute resolution procedure

TC TrustCenter is not responsible for resolving name claim disputes among subscribers. TC TrustCenter may add, at its own discretion, additional information to a name in order to make it unique among the names of certificates issued by TC TrustCenter.

3.1.6 Recognition, authentication and role of trademarks

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

3.1.7 Method to prove possession of private key

Key generation takes place in the secure signature creation device (SSCD) and can be initiated by TC TrustCenter only.

The SSCD is initialized and personalized by TC TrustCenter and then delivered to the subscriber. The subscriber has to confirm the receipt of the SSCD before the activation data is sent to the subscriber.

3.1.8 Authentication of organization identity

If the applicant is a person who is identified in association with a legal person or other organizational entity in addition to the data in § 3.1.9 evidence shall be provided of its existence. This verification may be carried out by a presentation of a copy 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).

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.

The documentation must include

- full name and legal status of the associated legal person or other organizational entity
- relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.

3.1.9 Authentication of individual identity

The authentication of an individual entity is performed in compliance with Directive 1999/93/EC and the German Signature Act.

Evidence of the identity of an applicant is checked against an official ID document in combination with the personal appearance of the applicant. TC TrustCenter may use, with the applicant's consent, personal data collected at an earlier date. The ID document must contain

- full name (including surname and given names)
- date and place of birth

– a serial number or other attributes which may be used to distinguish the person from others with the same name.

It is also permitted to check the identity of the applicant indirectly using means which provide equivalent assurance to physical presence (for example if the applicant already possesses a qualified certificate, which implies that the applicant has been identified with personal presence).

If the applicant is a person who is identified in association with a legal person or other organizational entity in addition to the data in § 3.1.8 evidence shall be provided of:

– evidence that the subject is associated with the legal person or other organizational entity

– authorization from the legal person or other organizational entity to act for the the legal person or other organizational entity.

3.2 Routine Rekey

Rekey means changing the public key for an existing certificate by issuing a new certificate with a *different* 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].) Renewal for qualified certificates is not supported.

The standard procedure for rekey is the same as for the initial issuance of a qualified certificate. The entire registration process has to be repeated.

Alternatively a subscriber may send a new application in electronic form. If this electronic application is signed with a valid qualified certificate issued to the subscriber the identity of the requesting entity is proven by the qualified signature. TC TrustCenter may issue a new qualified certificate without repeating the identification process.

If the new certificate is to contain additional data about an organization the validity of this data has to be verified in the same manner as for an initial application.

3.3 Rekey after Revocation

After a certificate has been revoked, the subscriber must reapply for a new certificate in accordance with § 3.1, since the revoked key pair is ineligible to sign and authenticate a rekey request (see § 3.2).

3.4 Revocation Request

There are several ways to submit a revocation request:

1. The subscriber or an authorized third party may call TC TrustCenter by phone and authenticate itself by using the revocation password chosen when submitting the initial certificate application. For this purpose a revocation hotline is installed. The revocation hotline is available 24 hours per day, 7 days per week.
2. The subscriber or an authorized third party may request a certificate to be revoked by writing a letter to TC TrustCenter stating this request. Authentication is then provided by the handwritten signature or by the revocation password.
3. An authorized third party may request a certificate to be revoked by sending a revocation request in electronic form to TC TrustCenter. Authentication is then provided by the third party's qualified electronic signature or by the revocation password. If a revocation re-

quest is signed with a qualified certificate the certificate to be revoked must be different from the certificate on which the qualified signature is based.

TC TrustCenter confirms a request for revocation by e-mail or sends a written confirmation, within reasonable amount of time, no later than twenty-four hours after receiving the request.

4 Operational Requirements

4.1 Certificate Application

A subscriber submits a certificate application to TC TrustCenter and follows the procedure described in this CPS/CP or in TC TrustCenter's descriptions for certificate applications.

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

The key pair and the certificate are generated by TC TrustCenter.

Key generation then takes place in a secure environment. Keys for qualified electronic signatures are always created in secure signature creation devices which are approved to be used for such purposes Private key are not exportable from such devices.

4.2 Certificate Issuance

TC TrustCenter verifies the accuracy and validity of all data necessary for the issuance of a qualified certificate (compare § 3.1.8 and § 3.1.9).. TC TrustCenter will verify the data contained in the application according to the German Signature Act. TC TrustCenter will either issue the subscriber's certificate upon successful completion of this process and send the certificate on the secure signature creation device to the subscriber, or inform the subscriber about any problems or inconsistencies.

The qualified certificate will be valid for no more than five years from the date of issuance, with a default validity period of three years.

TC TrustCenter generates qualified certificates using the appropriate certificate format, and sets validity periods and extension fields in accordance with relevant standards and legal regulations.

4.3 Certificate Acceptance

After a qualified certificate has been issued and stored on the appropriate secure signature creation device the SSCD is delivered to the subscriber. The subscriber has to confirm the receipt of his SSCD. After the subscriber confirmed the receipt of his SSCD the SSCD activation data will be sent to the subscriber.

4.4 Certificate Dissemination

TC TrustCenter makes qualified certificates available to subscribers by sending the SSCD by personal mail to the subscriber. The subscriber may also collect the SSCD directly at the premises of TC TrustCenter. Alternatively, the subscriber may arrange another way of delivery.

Qualified certificates are made available for retrieval from TC TrustCenter's certificate repository by third parties only if the subscriber has declared his consent.

4.5 Certificate Suspension and Revocation

A qualified certificate can not be suspended.

If the private key has been compromised or lost, or if subscriber data represented in the certificate has changed substantially, the certificate must be revoked.

The subscriber or an authorized third party can revoke a certificate at any time and for any reason.

If the certificate is revoked, it becomes invalid as soon as TC TrustCenter has processed the revocation request. The certificate's serial number and time of revocation will be included in TC TrustCenter's status information service, and subsequent status inquiries to the certificate status service will result in a response citing the certificate as invalid.

4.5.1 Circumstances for revocation

A certificate is revoked in case:

1. The subscriber or an authorized third party has submitted a revocation request as described in § 3.4;
2. TC TrustCenter has learned about false information having been supplied in the certificate application that invalidate the certificate;
3. The supervising authority (Bundesnetzagentur, Federal Net Agency) instructs TC TrustCenter to revoke a certificate in accordance with § 19 of the German Signature Act.;
4. TC TrustCenter ceases operation and no other certification service provider continues TC TrustCenter's certification services.

4.5.2 Who can request revocation

The subscriber or his substitute can request revocation.

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

Any entity or third party that confirmed any information contained in a certificate has the right to revoke the affected certificate.

Everybody can inform TC TrustCenter about the fact that information in a certificate is not or no longer correct. TC TrustCenter will then check whether a revocation in accordance with § 4.5.1, 2 is adequate.

The Federal Net Agency can instruct TC TrustCenter to revoke one or more certificates in accordance with § 19 of the German Signature Act.

4.5.3 Procedure for revocation request

The procedure for revocation is described in § 3.4.

4.5.4 Revocation request grace period

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

4.5.5 Circumstances for suspension

Qualified certificates can not be suspended.

4.5.6 Who can request suspension

Qualified certificates can not be suspended.

4.5.7 Procedure for suspension request

Qualified certificates can not be suspended.

4.5.8 Limits on suspension period

Qualified certificates can not be suspended.

4.5.9 CRL issuance frequency (if applicable)

CRLs for qualified certificates issued by TC TrustCenter are not publicly available.

4.5.10 CRL checking requirements

No stipulation.

4.5.11 On-line revocation / status checking availability

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

Please see TC TrustCenter's Web Site for other means of checking a certificate's status (e. g. OCSP).

4.5.12 On-line revocation checking requirements

It is the responsibility of the relying party to check the revocation status on-line.

In order to check an on-line revocation status response a relying party may need to obtain the appropriate response signing certificate. This certificate may differ from the certificate of the issuer of the certificate being checked, and if so, it is available from TC TrustCenter's Web Site or upon request by e-mail.

4.5.13 Other forms of revocation advertisements available

No stipulation.

4.5.14 Checking requirements for other forms of revocation advertisements

No stipulation.

4.5.15 Special requirements regarding key compromise

Depending on whether the subscriber suspects or knows for sure that his private key has been compromised, he is required to request revocation as soon as possible. A subscriber is not relieved from his obligations as a subscriber until he has been notified by TC TrustCenter of the revocation of the certificate.

5 Physical, procedural, and personnel security controls

TC TrustCenter is committed to establishing and maintaining state of the art security controls required from CAs and RAs. This chapter provides an outline of such a security controls framework, which reflects the provisions of the German Signature Act, the IdenTrust System, the SISAC standard (Secure Identity Services Accreditation Corporation, a subsidiary of the Mortgage Bankers Association of America, "MBA/SISAC"), and the "ETSI TS 101 456 Policy requirements for certification authorities issuing qualified certificates". The respective provisions supplement one another and serve to enhance the overall security controls, which are audited regularly by independent third parties. All of them require the highest standards of security controls.

For security reasons, however, TC TrustCenter will not disclose any specific details about the specific measures taken. The documents describing TC TrustCenter's implementation of security controls are considered non-public.

5.1 Physical Controls

Several layers of physical security controls restrict access to TC TrustCenter's sensitive hardware and software systems used for 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 can access them.

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 certificate status responses are not vulnerable to physical penetration. These keys are stored in tamper-resistant secure signature creation devices which are confirmed to fulfill the requirements of the German Signature Act. 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 with regard to 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.

All CA systems have industry standard power and air conditioning systems to provide a suitable operating environment. All CA systems have reasonable precautions taken to minimize the impact of water exposure. All CA systems have industry standard fire prevention and protection mechanisms in place.

Off-site backups are stored in a physically secure manner by a bonded third-party storage company.

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 the RA's physical security controls must match those of TC TrustCenter.

An RA never stores subscriber key information.

5.2 Procedural Controls

TC TrustCenter's operating procedures are documented and maintained. Procedural controls ensure that no single person acting by him/herself will be able to circumvent the security measure taken.

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 performing certain essential tasks requires multiple individuals. This "dual control" prevents single persons from being able to forge a certificate.

Development and testing facilities are physically 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 and threats to systems or services. System documentation is protected from unauthorized access.

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

5.3 Personnel Controls

TC TrustCenter ensures that all personnel involved in issuing, managing, suspending and revoking qualified certificates, and managing related data and information is integer, trustworthy, and loyal. 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. All personnel 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.

No unauthorized users have access to systems storing sensitive data. All systems storing such data are located inside a protected area. In addition, access to rooms inside the protected area is controlled by an Access Control System; access to systems is permitted for authorized persons only.

Employees sign a confidentiality (nondisclosure) agreement as part of their initial terms and conditions of employment. All employees of the organization and, where relevant, third-party users 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.

5.4 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. These include, but are not limited to: issuance of certificates, CRLs, time stamps, notification of key comprise, revocation of certificates, establishment of trusted roles and actions of trusted personnel, changes to CA keys.

In addition, system access and use is monitored and recorded in audit logs or written down in event journals. Thus all CA personnel is 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.

As part of the scheduled system back up procedures, audit trail files are backed up to WORM media. Audit trail files are archived by the system administrator on a regular (at least) weekly basis. Event journals are reviewed at least on a weekly basis by the internal auditors.

No single person may modify or even delete audit trails or system log files, and access to them is strictly restricted. These provisions are implemented using the features of a secure B1 operating system requiring the simultaneous login of two persons.

For further details upon internal and external audit requirements and procedures, see § 2.7.

5.5 Records Archival

Audit trails and system log files (see § 5.4) are backed up regularly on WORM (write once, read multiple) media and archived in a safe facility. Archived audit data concerning qualified certificates are retained as required by the German Signature Ordinance [GDSO] for a period defined in § 8 (3) in combination with § 4 (1) of [GDSO].

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. In general, records are archived for at least five years; records concerning qualified certificates are retained as long as required by the German Signature Ordinance [GDSO]. No single person is able to modify or even destroy archived material, and access to it is strictly restricted.

5.6 Key changeover

Upon the end of the CA's private key's lifetime, a new CA signing key pair is generated and all subsequently issued certificates are signed with the new private signing key.
Upon the end of the lifetime of the CA's private key, which is used for certificate status information signing, a new signing key pair for status information is generated and all subsequently published status information is signed with the new private signing key.
Changing CA keys enables TC TrustCenter to adjust key parameters and cryptographic algorithms, taking into account the suitability of algorithms and parameters as defined by the Federal Network Agency in order to compensate advances in science and / or technology.

Any new CA key is available by request via e-mail or from TC TrustCenter's repository at http://www.trustcenter.de/ root_certificates.htm.

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 tolerated outage time depends on the requirements on the availability of a specific service and may range from one hour up to 72 hours.

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.

5.8 CA Termination

The CA can only be terminated by the Federal Network Agency or by the Board of Directors of the CA. TC TrustCenter will inform subscribers of valid certificates (i. e., neither revoked nor expired) in as much advance as circumstances permit, and attempt to provide alternative sources of interoperation.

As required by the German Signature Act TC TrustCenter will make a reasonable effort to transfer the records of the CA and the certificate repository to another issuer of qualified certificates. TC TrustCenter will also attempt to establish an acceptable procedure for subscribers and relying parties for switching to a different provider of 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. All relevant documentation will be transferred to the Federal Network Agency as required in § 13 of the German Signature Act.

Subscribers will be notified of such action taken by TC TrustCenter.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

Any private CA key used for issuing qualified certificates is generated on a SSCD evaluated as "E4 high" according to ITSEC criteria (or equivalent) and confirmed to be compliant with the German Digital Signature Act by an independent third party and the Federal Net Agency.

The entire key generation 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.

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

Software generation and/or usage of keys are not supported in connection with the issuance of qualified certificates.

No copy of any private key is kept permanently on magnetic media in unencrypted form. No private key material is temporarily stored on magnetic media because keys for qualified certificates are generated inside the SSCD.

6.1.1.2 Subscriber key pair generation

Currently subscriber key pair generation is not supported.

6.1.2 Private key delivery to entity

Private keys are generated by SSCDs and delivered to the subscriber by certified personal mail with return receipt. Alternatively, the subscriber may collct his SSCD with the private key at TC TrustCenter's office.

On subscriber's request the SSCD may also be delivered by any other acceptable form of secure delivery.

6.1.3 Public key delivery to certificate issuer

Not applicable.

6.1.4 Public key delivery to users

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

The subscriber's public key is delivered on the SSCD used for storing the subscriber's key pair.

If the subscriber has agreed to his certificate being published in TC TrustCenter's certificate directory, it is available for download as well.

6.1.5 Key sizes

Any key generated on a smartcard and used for a qualified certificate is currently at least 1024 bit in size. As soon as such cards are available TC TrustCenter will support smartcards with larger keys. TC TrustCenter will then cease to issue qualified certificates with 1024 bit keys.

After December 31st,2007 1024 bit keys are no longer supported for qualified certificates.

6.1.6 Public key parameters generation

Permissible key parameters for key pairs used for qualified certificates are published by the Federal Net Agency. TC TrustCenter uses only such key parameters for qualified certificates that are defined by the Federal Net Agency to be adequate.

All current CA keys for the issuance of qualified certificates are RSA keys with 1024 bit and use the hash algorithm SHA-1.

As soon as available all keys will be 2048 bit using a hash algorithm from the SHA-2 family (SHA-224 to SHA-512).

6.1.7 Parameter quality checking

Not applicable. There is no possibility for the subscriber to choose key parameters.

6.1.8 Hardware / software key generation

Not applicable. Keys are generated by TC TrustCenter, not by the subscriber.

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

Qualified certificates issued by TC TrustCenter must be used according to the X.509 v3 key usage field as set by TC TrustCenter (see also § 7.1). Qualified certificates may be used for electronic signatures.

6.2 Private Key Protection

TC TrustCenter keeps its private keys in a trusted computer system not connected to TC TrustCenter's local area network or any public network. The computer system is kept in a secure physical facility. Access to both the facility and the private keys is protected by access control mechanisms. The private keys can only be activated by two persons and are stored in a SSCD. They are never written to any permanent or magnetic storage media.

6.2.1 Standards for cryptographic module

For issuing qualified certificates a SSCD is used.

For storing other types of keys TC TrustCenter uses cryptographic hardware modules. These hardware modules are certified to be FIPS 140-1 level 3 compliant. Physical access to the cryptographic module is restricted by an access control system. The hardware module must be activated by two persons simultaneously (dual login). The HSM is used in the FIPS 140-1 level 3 mode.

Two persons are required to activate the SSCDs that hold the private CA keys used for issuing qualified certificates.

Unencrypted private keys can not be extracted from the hardware module or the SSCD at any point.

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

The private CA keys are stored on a SSCD which meets the requirements of the [GDSO] and the [GSA]. In order to activate the private CA keys, two persons are required (see § 6.2.1). 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 signature keys for qualified certificates.

For certificates issued in compliance with the German Signature Act any form of key escrow is explicitly prohibited.

6.2.4 Private key backup

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

6.2.5 Private key archival

Private key archival is not possible because keys generated and stored on a SSCD cannot be extracted from the smart card.

However, the SSCDs holding CA keys may be archived after the operational period of the CA key. Archived 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.

6.2.6 Private key entry into cryptographic module

Private CA keys are generated and stored in a SSCD.

6.2.7 Method of activating private key

Activating private CA keys used for issuing qualified certificates 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.

6.2.8 Method of deactivating private key

The private CA key is automatically deactivated after issuing certificates has been completed and the certification application exits or closes the connection to the SSCD. Before it can be used again, the SSCD must be reactivated.

6.2.9 Method of destroying private key

The destruction of any private CA key must be authorized by the management. It is done under dual control, and it is witnessed and signed off by a third person not involved in the actual destruction of the key.

The CA's private key is stored on an SSCD. The SSCD is destroyed by physically destroying the smart card.

There are no copied or fragments of key material which need to be destroyed because the use of an SSCD guarantees that private keys can never be exported from the SSCD.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

Any qualified certificate issued by TC TrustCenter is stored in the certificate repository and on backup media of the systems that host the certificate repository. In addition, any qualified certificate issued by TC TrustCenter is stored on the CA system and on the audit files crated for the CA system.

TC TrustCenter does not offer any other public key archival service.

6.3.2 Usage periods for the public and private keys

Qualified certificates may be used for as long as the certificate and/or the repository indicate. Once a certificate has expired, it is no longer valid.

The [GDSO], § 14 (4), restricts the validity of qualified certificates to at most five years. This restriction pertains to CA certificates as well as subscriber certificates.

6.4 Activation Data

Business requirements for access control are defined and documented in an access control policy which includes identification and authentication process for each user, segregation of duties, and number of persons required to perform specific CA operations (meaning, 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 are required to follow defined policies and procedures in the selection and use of passwords.

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 § 8.1) ensures 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.

6.6 CA Cryptographic Hardware Life Cycle Controls

Policies and procedures require that CA cryptographic hardware be sent from the manufacturer via registered mail using tamper evident packaging. In the context of qualified certificates, this mainly concerns SSCDs. The SSCD's manufacturer may define different delivery procedures, which then have to be laid down in the product specification and the product confirmation in compliance with § 17 (4) [GSA].

Upon the receipt of CA cryptographic hardware other than SSCDs, authorized CA personnel inspect the tamper evident packaging to determine whether the seal is intact. This is followed by acceptance testing and verification of firmware settings.

The cryptographic hardware is then added to an inventory list. To prevent tampering, CA cryptographic hardware is stored in a secure site, with access limited to authorized personnel. Each piece of cryptographic hardware is tracked during it 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 CA cryptographic hardware is performed in the presence of no less than two trusted employees. The same controls apply to service or repair being performed on the CA site. CA cryptographic hardware is never serviced or repaired off-site and subsequently put back into production.

Audit processes and procedures are in place to verify the effectiveness of the controls

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 Cryptographic Module Engineering Controls

SSCDs used for storing key material are certified according to ITSEC, level “E4 high” and confirmed by an authorized third party (§ 18 [GSA]) to be compliant with the legal requirements (§17 (4) [GSA]).

The Hardware Security Modules used for storing other CA key material are certified to be FIPS 140-1 level 3 compliant (see § 6.2.1).

7 Certificates and CRL Profiles

7.1 Certificate Profile

7.1.1 Version number(s)

TC TrustCenter issues qualified certificates in compliance with X.509 version 3.

7.1.2 Certificate extensions

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

For X.509 certificates compliant to the German Signature Act, TC TrustCenter uses the appropriate X.509v3 extensions:

`KeyUsage` is a critical extension and has the value `nonRepudiation`.

`BasicContraints` is a critical extension and has the value `false`.

`SubjectAltName` will be used if the subscriber wishes to include information such as his postal address.

`AuthorityKeyIdentifier` identifies the CA certificate that must be used to verify the subscriber’s certificate. It contains serial number and issuer DN of the issuing CA certificate.

`ICCSN` contains the serial number of the SSCD that holds the subscriber’s private key or key pair (if applicable).

7.1.3 Algorithm object identifiers

For qualified certificates TC TrustCenter only supports such hash function/digital signature algorithm combination which has been approved by the Federal Net Agency as being permissible for the use in qualified certificates.

Permissible key parameters for key pairs used for qualified certificates are published by the Federal Net Agency.

All current CA keys for the issuance of qualified certificates are RSA keys with 1024 bit and use the hash algorithm SHA-1.

As soon as available all keys will be 2048 bit using a hash algorithm from the SHA-2 family (SHA-224 to SHA-512).

7.1.4 Name forms

See § 3.1.

7.1.5 Name constraints

See § 3.1.

7.1.6 Certificate policy Object Identifier

No stipulation.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical certificate policy extension

If this extension is critical, the certificate path validation software must be able to interpret this extension (including the optional qualifier), or must reject the certificate.

7.2 CRL Profile

TC TrustCenter currently does not publish CRLs.

Status information is provided via OCSP.

7.2.1 Version number(s)

TC TrustCenter currently does not publish CRLs.

7.2.2 CRL and CRL entry extensions

TC TrustCenter currently does not publish CRLs.

8 Specific administration

Contact information:

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

8.1 Specification change procedures

TC TrustCenter's Policies and Practices board has final authority and responsibility for specifying and approving certification policies, this Certification Practice Statement (CPS/CP) and the General Terms and Conditions (GTC). It is responsible for performing a (continuous) assessment to evaluate business risks and determine the security requirements and operational procedures to be included in the applicable certificate policy, Certification Practice Statement and/or General Terms and Conditions.

TC TrustCenter makes available its public Certification Practice Statement (CPS/CP) to all appropriate subscribers and relying parties. Revisions to this CPS/CP or to the GTC that have significant impact on the users of this CPS/CP must not be made retroactively and shall be published at least two weeks prior to coming into effect.

Revisions to this CPS/CP which are considered to have minimal or no impact on subscribers and relying parties using certificates and and certificate staus information issued by TC TrustCenter may be made and posted to the repository without notice to users of the CPS/CP and without changing the version number or date of this CPS/CP.

This version of the CPS/CP is dated June 11th, 2007.

8.2 Publication and notification policies

Any time this CPS/CP (or related documents such as the GTC) is amended, and the modified version is approved by TC TrustCenter's Policies and Practices Board, it is posted to the repository.

8.3 CPS approval procedures

The CPS/CP and the General Terms and Conditions are reviewed by and accredited by TC TrustCenter's Policies and Practices Board before being published in the repository.

9 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

[ETSI] ETSI TS 101 456: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates

[EU-DIR] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[GSA] Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations, published 2001
(http://www.bundesnetzagentur.de/media/archive/1850.pdf)
In combination with First Amendment to the German Signature Act (2005)

[GDSO] Ordinance on electronic Signatures (Signaturverordnung, SigV)

http://www.bundesnetzagentur.de/media/archive/3613.pdf

[RFC2459] Internet X.509 Public Key Infrastructure

Certificate and CRL Profile

ftp://ftp.isi.edu/in-notes/rfc2459.txt

[RFC2527] Internet X.509 Public Key Infrastructure

Certificate Policy and Certification Practices Framework.

ftp://ftp.isi.edu/in-notes/rfc2527.txt

[RFC2828] Internet Security Glossary.

ftp://ftp.isi.edu/in-notes/rfc2828.txt

[RFC3280] Internet X.509 Public Key Infrastructure

Certificate and Certificate Revocation List (CRL) Profile

ftp://ftp.isi.edu/in-notes/rfc3280.txt

[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.

10 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 liberalisation 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 is a public key that is signed by a Certification Authority. It 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

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. While a CPS is prepared by a Certification Authority, any organization may define a Certificate Policy.

CERTIFICATE POLICY DEFINITIONS

The TC TrustCenter Certificate Policy Definitions (CPD) is a document describing a set of certificate policies that TC TrustCenter supports for the issuance of advanced certificates. 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 contained in 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.

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.

CIPHER

A cipher is a cryptographic algorithm used for encryption.

CONFIRM

To ascertain through appropriate inquiry and investigation.

CONVENTIONAL ALGORITHMS

See symmetric algorithms.

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 signed data to provide authenticity and integrity. The digital signature is checked using the sender's public key.

DIGITAL SIGNATURE ACT

The German Signature Act (GSA) and the German Signature Ordinance (GSO) 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. A revision that reflects the experiences gained thus far, and implements Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, is expected to be enacted in the second quarter of 2001.

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=jdoe@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.

GTC

See General Terms and Conditions.

H

HASH FUNCTION

A hash function generates a short extract of fixed length (MD5: 128 bits = 16 characters, SHA-1: 160 bits = 20 characters), 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. 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 make use of their respective advantages, higher speed (symmetric) and easier key exchange (asymmetric).

I-J

IDEA

IDEA (International Data Encryption Algorithm) is a 64 bit block cipher that uses a 128 bit key. IDEA is considered to be one of the most secure encryption algorithms. It is used (among others) by PGP. Commercial users of PGP that use IDEA as the symmetric cipher have to pay a license fee to the Swiss company ASCOM; non-commercial use is free of charge.

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, SHA-1 is 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

QUALIFIED CERTIFICATE

A qualified certificate is a certificate issued in compliance with the Directive 1999/93/EC of the European Parliament and of the Council and in compliance with the German Signature Act. A signature produced using a qualified certificate is deemed to be legally equal to a handwritten signature.

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.

REVOCATION

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 certificate policy definition 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.