



TC TrustCenter GmbH

Certification Practice Statement

Version 1.1 of April 1st, 2001

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]).

This document may not be copied, distributed, used, stored or transmitted in any form or by any means, whether in part or as a whole, without the prior written consent of TC TrustCenter GmbH.

Copyright © 1999-2001 by TC TrustCenter GmbH.

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

1	Introduction	4
1.1	Overview	4
1.2	Identification	4
1.3	Community and Applicability	5
1.4	Contact details	6
2	General Provisions	7
2.1	Obligations	7
2.2	Liability	8
2.3	Financial responsibility	8
2.4	Interpretation and Enforcement	9
2.5	Fees	10
2.6	Publication and Repository	10
2.7	Compliance audit	10
2.8	Confidentiality	11
2.9	Intellectual Property Rights	11
3	Identification and Authentication	12
3.1	Initial Registration	12
3.2	Routine Rekey	13
3.3	Rekey after Revocation	14
3.4	Revocation Request	14
4	Operational Requirements	15
4.1	Certificate Application	15
4.2	Certificate Issuance	15
4.3	Certificate Acceptance	15
4.4	Certificate Suspension and Revocation	15
4.5	Security Audit Procedures	18
4.6	Records Archival	18
4.7	Key changeover	19
4.8	Compromise and Disaster Recovery	19
4.9	CA Termination	19
5	Physical, procedural, and personnel security controls	20
5.1	Physical Controls	20
5.2	Procedural Controls	21
5.3	Personnel Controls	21
6	Technical Security Controls	23
6.1	Key Pair Generation and Installation	23
6.2	Private Key Protection	25
6.3	Other Aspects of Key Pair Management	27
6.4	Activation Data	27
6.5	Computer Security Controls	28
6.6	CA Cryptographic Hardware Life Cycle Controls	28
6.7	Network Security Controls	28
6.8	Cryptographic Module Engineering Controls	29
7	Certificates and CRL Profiles	30

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

7.1 Certificate Profile.....	30
7.2 CRL Profile	31
8 Specific administration	32
8.1 Specification change procedures	32
8.2 Publication and notification policies.....	32
8.3 CPS approval procedures	32
9 References.....	33
10 Glossary	34

1 Introduction

1.1 Overview

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

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

A certificate is, in essence, a digitally signed public key. It always contains the name 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 and confidential data might be decrypted by unauthorized persons.

A Certification Authority acts as a trusted third party that binds certificates to the indicated entity. A certificate issued by a CA contains the subscriber's name, the name of the CA, the subscriber's public key, and is signed by the CA. TC TrustCenter offers several certificate classes that are described in the corresponding Certificate Policy Definitions (CPD) and referenced in this CPS, each indicating a different level of trust that may be placed in the reliability and strength of this bond by a relying party. TC TrustCenter's services are provided on the basis of TC TrustCenter's General Terms and Conditions (GTC), which are available from the repository.

This CPS describes the structure and practices of TC TrustCenter, in order to enable customers of TC TrustCenter to evaluate TC TrustCenter's services. This CPS does neither constitute a declaration of self-escrow, nor does it state legally binding warranties. Any legally binding statements by TC TrustCenter are made in the General Terms and Conditions or in specific contracts between TC TrustCenter and other parties.

This CPS makes extensive use of the vocabulary related to the field of digital signatures and certificates, cryptography and public key encryption, which is referenced in the Glossary (Chapter 10). The glossary also provides the definition of some important terms not appearing elsewhere in this text that relate to the areas mentioned above.

1.2 Identification

TC TrustCenter GmbH of Sonninstrasse 24-28, 20097 Hamburg, Germany (referred to as "TC TrustCenter" in this CPS), is an international Certification Authority and Certification Services Provider (CSP). TC TrustCenter issues a wide variety of certificates, such as X.509, WTLS and PGP certificates. These can be use 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

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

under its own policies, as defined in the Certificate Policy Definitions, and under policies of third parties that use TC TrustCenter as their CSP, such as Identrus Level One Participants.

This CPS supports the certificates issues under TC TrustCenter's Certificate Policy Definitions available from

<http://www.trustcenter.de/cpd>

This Certification Practice Statement is available upon request by e-mail. The TC TrustCenter Certificate Policy Definitions may be retrieved from

<http://www.trustcenter.de/cps>

IMPORTANT NOTE: TC TRUSTCENTER IS NOT A LICENSED CERTIFICATION AUTHORITY IN ACCORDANCE WITH ART. 4 OF THE Digital Signature Act YET.

1.3 Community and Applicability

This CPS 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.

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 provides information about other subsidiary or cooperating CAs upon request.

1.3.2 Registration authorities

A Registration Authority (RA) works on behalf of a CA. TC TrustCenter operates an in-house Registration Authority responsible for verifying both business information and personal data contained in a subscriber's certificate.

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 two categories: (1) TC TrustCenter Ident Points[®] or (2) post offices.

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 the identification service to different companies, most notably banks, and it takes a day or two for the certificate to be issued once the identification process is completed.

Please refer to the TC TrustCenter Certificate Policy Definitions for further details.

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 both natural and juristic persons which are able to perform legal acts, and who use certificates issued by TC TrustCenter.

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

1.3.4 Applicability

Except as noted in the provisions applying to the different policies this CPS supports (see the Certificate Policy Definitions for a description of the certificate policies that are supported by this CPS), all applications in the areas of electronic commerce and secure Internet communication are suitable for use with digital certificates issued under the terms of this CPS.

1.4 Contact details

1.4.1 Specification administration organization

This CPS 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 for the policy

The TC TrustCenter Policies and Practices Board consisting of TC TrustCenter executives determines the CPS suitability for the policy.

2 General Provisions

For the purposes of the service, the repository and the binding legal rules TC TrustCenter refers to its General Terms and Conditions for Digital Certificates (GTC) in this section. The GTC are based on German law. Under binding consumer protection laws it is therefore not possible to agree with an end user on such a long document like this CPS. The only applicable regulation between the customers and TC TrustCenter are the GTC. Any arising questions which are not covered by the GTC are to be answered by binding codified German law.

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

In no event, this CPS 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

The obligations of TC TrustCenter are described in the GTC in the clauses 2 (Certification), 3 (Inquiries) and 5 (Data Transmission).

2.1.2 RA obligations

An RA must not use the 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 and those in the CPD; this includes, but is not limited to: ensuring that the requirements specified in § 4 CPS are met, and that the controls defined in §§ 5 and 6 CPS are provided; keeping subscriber information confidential according to § 2.8 CPS; and performing the authentication procedure as defined in § 3 CPS, the CPD and TC TrustCenter's RA guidelines.

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 are described in clause 4 (Duty of Care and Support) of the GTC.

2.1.4 Relying party obligations

Prior to relying on a certificate issued by TC TrustCenter, a relying party must review the CPS, the Certificate Policy Definitions and the GTC governing the issuance of the certificate as referenced therein and as set forth in this CPS in order to determine its suitability for the application in question. Different applications require different levels of security, and the re-

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

lying party is solely responsible for making the decision to rely on digitally signed data verifiable by the respective certificate in the given application context, and for checking that the certificate is neither invalid nor revoked.

TC TrustCenter will not enter into a single agreement with a relying party who has no other contractual relationship with TC TrustCenter. Certificate holders of TC TrustCenter who act as a relying party will be treated as subscribing customers and must therefore fulfil the obligations of the subscribers as described in clause 4 (Duty of Care and Support) of the GTC.

2.1.5 Repository obligations

TC TrustCenter will update the repository operated by TC TrustCenter, consisting of the directory of certificates and the support center, within a reasonable amount of time to reflect new information concerning the validity and reliability of the certificates issued.

2.2 Liability

2.2.1 CA liability

The liability of TC TrustCenter is described in clause 7 (Liability) of the GTC.

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, for one of the following reasons: (1) A subscriber has a contractual agreement with TC TrustCenter, not with the RA, which only acts as TC TrustCenter's accomplice. (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 governing law is described in clause 1 (General) of the GTC in section 1.4.

The place of jurisdiction is described in clause 1 (General) of the GTC in section 1.5.

2.4.2 Severability, survival, merger, notice

2.4.2.1 Severability

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

The severability of the GTC is described in clause 1 (General) of the GTC in Section 1.6.

2.4.2.2 Survival

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

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

2.4.2.3 Merger

Any modification of the provisions of this CPS 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.

2.4.2.4 Notice

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

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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/products>.

2.6 Publication and Repository

2.6.1 Publication of CA information

TC TrustCenter will publish the CPS, the Certification Policy Definitions and the GTC in the repository at <http://www.trustcenter.de/repository>. The directory of all certificates issued by TC TrustCenter and TC TrustCenter's issuer (root) certificates, which may also be used for on-line certificate status inquiries, is accessible from the repository as well. The Certificate Revocation List is available upon request by e-mail and from <http://www.trustcenter.de/crl>.

2.6.2 Frequency of publication

The CRL is updated at least weekly. The certificate database is updated every time a certificate is issued. 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 and Certificate Policy Definitions, 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 performs internal self-audits at least once a year. The results of these self-audits are documented, archived and submitted to the party that requires the audit report for review, if applicable.

Topics covered by internal self-audits include a sample check 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.

In addition, TC TrustCenter is subject to regular external audits. These include audits with respect to TC TrustCenter acting as a CSP for Identrus Level One Participants, and will, in the future, be extended to include audits for Identrus QuickStart compliance, compliance with the WebTrust program for Certification Authorities, the SET standards for Certificate Processors by VISA and MasterCard, and the German Digital Signature Act.

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

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

2.8 Confidentiality

TC TrustCenter keeps information confidential as it is described in clauses 3 (Inquiries) and 5 (Data Transmission) of the GTC.

2.9 Intellectual Property Rights

This CPS, the CPD and GTC are © 2001 by TC TrustCenter GmbH, Germany. (See § 1.2 CPS for full identification information.)

3 Identification and Authentication

3.1 Initial Registration

In order to obtain a certificate, any subscriber must apply for a certificate, and identify and authenticate himself to TC TrustCenter. This section covers these topics in a general fashion. Please see the Certificate Policy Definitions (CPD) for further details.

3.1.1 Types of names

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

Names specified in PGP certificates do not follow the same strict rules that X.509 imposes since there are no data fields like Organization or Common Name that make up the subject DN. Subscribers must, however, exercise the same care in specifying their name and other relevant data in their certificate to enable others to identify the entity holding that certificate (see the following subsection).

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

The CPD provide examples for proper certificate names.

3.1.2 Need for names to be meaningful

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

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

Please check the CPD for examples.

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.

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

3.1.4 Uniqueness of names

Any subscriber DN in a X.509 certificate issued by TC TrustCenter must uniquely identify a single entity among all of TC TrustCenter's subscribers. The same entity may have different certificates all bearing the same subject DN, but no two separate entities may share a com-

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

mon 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.

PGP does not impose the same restrictions on user IDs pertaining to PGP public keys, and subscribers should provide enough information in a user ID to enable a relying party to uniquely identify the entity holding the certified public key.

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

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

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

3.1.8 Authentication of organization identity

A corporate organizational entity must provide TC TrustCenter with the memorandum that establishes the company and that is required for registration with the national register of corporations, or similar documents.

Governmental organizational entities must supply documents which reflect their relationship to the next higher entity and provide a certificate application confirmed by that entity.

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

3.1.9 Authentication of individual identity

The authentication of an individual entity depends upon the Certificate Policy that is reflected in the different certificate classes TC TrustCenter defines for issuing certificates.

Please see the TC TrustCenter Certificate Policy Definitions for details:

<http://www.trustcenter.de/cpd>

3.2 Routine Rekey

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

The general procedure for rekey and renewal is as follows:

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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

The Certificate Policy Definitions may provide stipulations that differ from these general provisions, depending on the certificate class that the certificate was issued under. In particular, TC TrustCenter may stipulate, and reserves the right to demand, that the subscriber is re-registered in accordance with § 3.1.

3.3 Rekey after Revocation

After a certificate has been revoked, the subscriber must generate a new key pair and reapply to TC TrustCenter 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) Renewal after revocation is not allowed.

3.4 Revocation Request

There are several ways to submit a revocation request:

1. If the subscriber is still in possession of his secret key, he has the option of submitting an authenticated revocation request to TC TrustCenter.
2. If the private key has been lost or is inaccessible for any reason, the subscriber may call TC TrustCenter and authenticate himself by naming the revocation password chosen when submitting the initial certificate application.
3. The subscriber may request his certificate to be revoked by writing a letter to TC TrustCenter stating this request. Authentication is provided by the subscriber's signature.

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

4 Operational Requirements

4.1 Certificate Application

A subscriber submit a certificate application to TC TrustCenter and follow the procedure described in TC TrustCenter Certificate Policy Definitions. The certificate request is either generated by the subscriber during the process of applying for the certificate or prior to completing the application form, or by TC TrustCenter after the application has been received and approved. In the latter case key generation takes place in a secure environment and on a cryptographic hardware token such as a smart card, such that the private key never leaves the token. Examples for the former are PGP keys and certificate requests intended for use with Web servers, most security proxies or Web browsers.

4.2 Certificate Issuance

TC TrustCenter verifies, as set forth in see § 3.1.7, that the applicant is in possession of the private key and that the certificate request has the proper contents, for example, that the common name field states the full server domain name in the case of server certificate requests. TC TrustCenter will verify the data contained in the request according to the Certificate Policy Definitions. TC TrustCenter will either issue the subscriber's certificate upon successful completion of this process and notify the subscriber, or inform the subscriber of any problems or inconsistencies.

The certificate will be valid for no more than five years from the date of issuance, with a default validity period of one year. Once it has expired, the subscriber may either renew his certificate if the maximum validity period has not yet been reached, or must reapply for a new certificate otherwise.

TC TrustCenter generates certificates using the appropriate certificate format, and sets validity periods and extension fields in accordance with relevant standards, such as X.509. For certificate renewals, TC TrustCenter generates and signs a new instance of the certificate, differing from the previous certificate only by the validity period.

4.3 Certificate Acceptance

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

4.4 Certificate Suspension and Revocation

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

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 the Certificate Revocation List, and subsequent status inquiries to the certificate repository will result in a response citing the certificate as invalid.

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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

Certificate suspension may not be supported for all (or any) certificate class(es).

4.4.1 Circumstances for revocation

A certificate is revoked in case:

1. The subscriber or his agent 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 invalidates the certificate.

4.4.2 Who can request revocation

Only the subscriber can request revocation, except as noted in § 4.4.1, 2.: Any entity or third party that confirmed any information contained in a certification should inform TC TrustCenter about the fact that this information is not or no longer correct, and request revocation in accordance with § 4.4.1, 2.

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

4.4.3 Procedure for revocation request

The procedure for revocation is described in § 3.4.

4.4.4 Revocation request grace period

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

4.4.5 Circumstances for suspension

A certificate is suspended in case:

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

4.4.6 Who can request suspension

Only the subscriber can request suspension, except as noted in § 4.4.5, 2.: Any entity or third party that confirmed any information contained in a certification should inform TC TrustCenter about the fact that this information might not or no longer be correct and request suspension in accordance with § 4.4.5, 2.

4.4.7 Procedure for suspension request

There are several ways to submit a suspension request:

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

1. If the subscriber is still in possession of his secret key, he has the option of submitting an authenticated suspension request to TC TrustCenter.
2. If the private key has been lost or is inaccessible for any reason, the subscriber may call TC TrustCenter and authenticate himself by naming the revocation password chosen when submitting the initial certificate application.
3. The subscriber may request his certificate to be suspended by writing a letter to TC TrustCenter stating this request. Authentication is provided by the subscriber's signature.

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

4.4.8 Limits on suspension period

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

4.4.9 CRL issuance frequency (if applicable)

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

CRLs are issued at least once a week, but will in general be updated up to several times a day, even if no changes have occurred since the last issuance. At a minimum, a CRL entry identifying a revoked certificate remains on the CRL until the end of the certificate's validity period. A certificate is also put on the CRL during its suspension period.

CRLs are available from the following URL:

<http://www.trustcenter.de/crl>

4.4.10 CRL checking requirements

It is the responsibility of the relying party to either obtain the latest CRL and check the revocation status, or to check the revocation status on-line.

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

4.4.11 On-line revocation / status checking availability

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

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

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

4.4.12 On-line revocation checking requirements

It is the responsibility of the relying party to either obtain the latest CRL and check the revocation status, or 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.

4.4.13 Other forms of revocation advertisements available

TC TrustCenter offers a push service to interested customers. Any time a certificate is revoked, TC TrustCenter will notify these customers. Details are available upon request from TC TrustCenter.

4.4.14 Checking requirements for other forms of revocation advertisements

No stipulation.

4.4.15 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 suspension or revocation, respectively, 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.

4.5 Security Audit 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 compromise; revocation of certificates; extension of certificates; establishment of trusted roles and actions of trusted personnel; changes to CA keys. In addition, system log files are kept for facilities employed in providing these services.

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.

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

4.6 Records Archival

Audit trails and system log files (see § 4.5) are backed up regularly on WORM (write once, read multiple) media and archived in a safe facility. TC TrustCenter uses internal and external archival to prevent loss of important documents and digital data. The archives are located in separate (internal or external) locations and protected by access-control systems. Records are archived for at least five years. No single person is able modify or even destroy archived material, and access to them is strictly restricted.

4.7 Key changeover

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

4.8 Compromise and Disaster Recovery

TC TrustCenter has a business continuity plan to restore its business operations in a reasonably timely manner following interruption to, or failure of critical business processes. The business continuity plan defines the period of time that is an acceptable system outage time in the event of a major natural disaster or CA private key compromise. This outage time depends on the certificate policy that pertains to the certification services related system that has failed and may range from one hour up to 72 hours.

Copies 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.

4.9 CA Termination

The CA can only be terminated by the Board of Directors of the CA. TC TrustCenter will inform subscribers of valid certificates (i. e., neither revoked nor expired) at least eight weeks in advance of its intention to stop providing certification services. All certificates that have not expired or have not been revoked by the respective subscribers will be revoked by TC TrustCenter once this eight week period has ended. Subscribers will be notified of such action taken by TC TrustCenter.

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

5 Physical, procedural, and personnel security controls

TC TrustCenter is committed to establishing and maintaining state of the art security controls required of CAs and RAs. This chapter provides an outline of such a security controls framework, which reflects the provisions of the Digital Signature Act, the Identrus System, the WebTrust Program for Certification Authorities and the requirements for SET certificate processors. The respective provisions supplement one another and serve to enhance the overall security controls, which are audited regularly by an independent third party. Both the Digital Signature Act and SET practices 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 the TC TrustCenter's implementation of security controls are considered non-public.

Note: Although this chapter is drafted with all of the above requirements in mind, this does not mean that TC TrustCenter has been audited to all of these requirements and approved by an appropriate third-party auditor yet. As of this writing, TC TrustCenter has been approved as a third-party certification services provider to several Identrus Level One Participants, and is preparing to obtain a license as a Digital Signature Act-, WebTrust -, and SET-compliant Certification Authority.

5.1 Physical Controls

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

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 and passwords for access.

A log is maintained, listing all physical entries to restricted areas. Private keys used for issuing certificate or signing CRLs are not vulnerable to physical penetration. These keys are kept in tamper-resistant hardware modules. Any unauthorized access to stored information, possibly resulting in loss, tampering or misuse thereof, is prevented by proper means. A regular security check is 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 persons authorized 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.

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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

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

5.2 Procedural Controls

TC TrustCenter's operating procedures are documented and maintained. Procedural controls ensure that no single person acting by itself 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 to prevent a single person from being able to forge a certificate.

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

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

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

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

5.3 Personnel Controls

TC TrustCenter ensures that the personnel involved in issuing, managing, suspending and revoking 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. It must have proper knowledge and experience related to CA operations and must have demonstrated security consciousness and awareness regarding its duties at TC TrustCenter. Periodic reviews occur to verify the continued trustworthiness of all personnel.

Employees 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

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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.

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

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

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

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

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

6.1.1.2 Subscriber key pair generation

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

The key pair may also be generated by TC TrustCenter or one of its cooperating CA agencies. This may happen, for example, if the secret key is stored on a Smart card (see also § 6.1.1.1). In this case, Smart cards used will generally be able to autonomously generate the key pair and be evaluated as "E4 high" according to ITSEC criteria (or equivalent). TC TrustCenter then merely initiates this process and has no control over or access to private key material.

6.1.2 Private key delivery to entity

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

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

If TC TrustCenter generates the key and stores it on a hardware token (such as a Smart card), the private key (i. e., the hardware token) and the sealed letter containing the PIN(s) needed to use or enable the private key may either (1) be delivered to the end user, upon his request, by certified mail with return receipt or any other acceptable form of secure delivery, or (2) be collected by the end user at TC TrustCenter's office.

6.1.3 Public key delivery to certificate issuer

If the subscriber generates the key pair by himself, his self-signed public key is submitted to TC TrustCenter during certificate application.

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

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 either delivered by e-mail or by means of delivery of the physical hardware token (smart card) used for storing the subscriber's key pair. During certificate generation, the CA system checks that the end entity's certificate can be verified using the issuing CA's public key. 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

The X.509 and WTLS CA keys are 1024 bit, and the PGP CA keys are 2048 bit in size. Subscriber's public keys must be between 512 and 4096 bit in size, with 1024 bit recommended for X.509 and 2048 bit for PGP keys. (The difference in key size is entirely of technical nature: Netscape Internet browsers prior to version 4.x cannot handle keys larger than 1024 bit.)

Any key generated on a Smart card is currently 1024 bit in size.

6.1.6 Public key parameters generation

Public key parameters for key pairs generated by software are determined by the configuration of the generating application. They may include key size, key ID, key type (e. g., Diffie-Hellman or RSA), date of creation, validity period, etc.

Public key parameters for key pairs generated by hardware are determined by the hardware's capability. They are chosen to ensure the best possible security, i. e., the optimal key size and reliable encryption / signature algorithms that are offered by the hardware are used.

All current CA keys are RSA keys and use the MD5 hash algorithm.

6.1.7 Parameter quality checking

The online-application and / or certification mechanisms will check for properly generated certificate requests and their correct format.

6.1.8 Hardware / software key generation

The subscriber may generate his key pair with whatever soft- or hardware is available to him. He should use the strongest type available, and tamper-proof hardware tokens (like Smart cards) are to be preferred for storage of the secret key.

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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

Certificates issued by TC TrustCenter must be used according to the X.509 v3 key usage field as set by TC TrustCenter (see also § 7.1). Certificates may, in general, be used for any purpose, including Web server security and code signing, except as provided in this CPS and the Certification Policy Definitions. Please see the CPD for details.

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, once decrypted using the proper authorization, never written to any permanent or magnetic storage media.

6.2.1 Standards for cryptographic module

For signing X.509 keys, a cryptographic hardware module is used. This hardware module has two modes of operation which meet either FIPS 140-1 level 2 or FIPS 140-1 level 3 criteria. Physical access to the cryptographic module is restricted by an access control system. The hardware module must be activated by two out of four persons using their Smart cards simultaneously. Each person has a security officer certificate stored on a Smart card which indicates which mode of operation (level 2 or level 3) is to be used. Level 2 allows transfer of the private key from the Smart card to the hardware module (and vice versa) unencrypted, while level 3 does not. *The HSM is used in the FIPS 140-1 level 3 mode.*

Another two out of four persons, different from the personnel activating the hardware module mentioned above, are required to insert and activate the Smart cards that hold the private CA keys used for issuing certificates.

The unencrypted private key cannot be extracted from the hardware module at any point.

TC TrustCenter's PGP cryptosystem is based on the commercial version of PGP 5.x or later. As of now, PGP keys may only be stored in software. No hardware interface (e. g. for use with Smart cards) is currently available.

The source code has been published in book form, and may be inspected by anyone interested in confirming that there are no security holes. PGP has, however, had plenty of expert review in recent years and is believed to be unbreakable by today's standards, provided the key size is at least 1024 bit. PGP is a trademark of Pretty Good Privacy Inc., which is now owned by Network Associates Inc. Please see their Web site and the PGP documentation for details on licensing PGP, especially for commercial use.

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

The private CA keys are stored encrypted in a secure physical facility operated by TC TrustCenter. In order to gain access to the private keys, two out of four 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 keys or any private key material, unless (1) key escrow is explicitly agreed upon in a contract between the subscriber and TC TrustCenter.

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

ter, outlining the liabilities and remedies between the parties, and (2), is not prohibited by law, certificate policies or other applicable provisions or agreements. *Using key escrow is strongly discouraged*, however, since the risks generally outweigh the benefits.

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

The Digital Signature Act explicitly prohibits any form of key escrow.

6.2.4 Private key backup

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

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

6.2.5 Private key archival

TC TrustCenter uses monthly backup media (see § 6.2.4) for archival. The stipulations on private key backup apply.

All 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 keys are stored on the CA system in encrypted form. They can only be activated under dual control. Unencrypted keys are kept inside HSM during their usage only, and are never stored on the host in the clear, except where using an HSM is not possible (PGP).

6.2.7 Method of activating private key

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

6.2.8 Method of deactivating private key

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

6.2.9 Method of destroying private key

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

All copies and fragments of the private key are destroyed at the end of the key pair life cycle. If a secure cryptographic device is accessible and known to be permanently removed from service, all private keys stored within the device that have ever been or potentially could be used for any cryptographic purpose are destroyed. If a CA cryptographic device is being permanently removed from service, then any key contained within the device that has been used for any cryptographic purpose is erased from the device. If a CA cryptographic device

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

case is intended to provide tamper-evident characteristics and the device is being permanently removed from service, then the case is destroyed.

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

For private keys stored in encrypted form on the CA system, but which are not protected by an HSM (PGP keys), the magnetic storage space that carried the private key is wiped multiple times to erase any remaining trace. If the storage medium itself is replaced (for example, due to hardware failure), it is physically destroyed.

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

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

6.3.2 Usage periods for the public and private keys

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

TC TrustCenter's public and private keys have a life-time period of at least five years. The private key's life-time period is lower than that for the corresponding public key, as determined by the validity-period of the certificates that are issued using the private key. If end-entity certificates have a validity period of one year under a certificate policy for which the private key is used to issue certificates, for example, and the life-time period of the CA certificate (and the public key) is five years, the private key's life-time period is four years. When the life-time period of the private key ends, key changeover will be initiated (see § 4.7).

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 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.

Upon the receipt of CA cryptographic hardware from the manufacturer, 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 its life cycle; any change in its state (removal from storage, integration into the production environment, removal from service etc.) is reflected in an event journal.

The handling, installation and removal of CA cryptographic hardware is performed in the presence of no less than two trusted employees. The same control 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 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

Smart cards used for storing key material are certified according to ITSEC, level “E4 high”.

The hardware module used for issuing X.509 certificates meets FIPS level 2 or 3, depending on its mode of operation (see § 6.2.1).

7 Certificates and CRL Profiles

7.1 Certificate Profile

7.1.1 Version number(s)

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

TC TrustCenter also issues certificates for PGP keys, both RSA and DH / DSS, and WTLS certificates.

7.1.2 Certificate extensions

TC TrustCenter uses the standard X.509v3 extensions.

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

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

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

`BasicConstraints` 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 Smart card that holds the subscriber's private key or key pair (if applicable).

In addition, TC TrustCenter uses the Microsoft Extensions for Microsoft Authenticode™ (if applicable).

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

7.1.3 Algorithm object identifiers

TC TrustCenter currently supports the hash function / digital signature algorithm combinations of `md5withRSAEncryption` and `sha1withRSAEncryption`.

7.1.4 Name forms

See § 3.1.

7.1.5 Name constraints

See § 3.1.

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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

Each CRL states the issuer of certificates on the list, the date of issuance, the date of expiry and a list of certificate serial numbers and revoke reasons (unless the latter is unspecified), indicating the certificates issued by the named issuer that have been revoked.

7.2.1 Version number(s)

TC TrustCenter issues X.509 version 2 CRLs.

7.2.2 CRL and CRL entry extensions

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

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: certificate@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) 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) to all appropriate subscribers and relying parties. Revisions to this CPS, to the certificate policies supported by this CPS or to the GTC that have significant impact on the users of this CPS must not be made retroactively and shall be published at least two weeks prior to coming into effect.

Revisions to this CPS which are considered to have minimal or no impact on subscribers and relying parties using certificates and CRLs issued by CA, may be made and posted to the repository without notice to users of the CPS and without changing the version number or date of this CPS.

This version of the CPS is dated April 1st, 2001.

8.2 Publication and notification policies

Any time the CPS (or related documents, such as the CPD and the GTC) is amended, and the modified version is approved by the TC TrustCenter Policies and Practices Board, it is digitally signed and posted to the repository.

8.3 CPS approval procedures

The CPS, the Certificate Policy Definitions and the General Terms and Conditions are reviewed by and accredited by the TC TrustCenter CPS 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>
- [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>
- [SIGG] Digital Signature Act (Signaturgesetz - SigG). Article 3 of the Information and Communication Services Act (Informations- und Kommunikationsdienste-Gesetz - IuKDG).
<http://www.iid.de/iukdg/iukdgc.html>
- [SIGV] Digital Signature Ordinance (Signaturverordnung - SigV).
<http://www.iid.de/iukdg/sigve.html>
- [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 pass phrase).

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.

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 photo-copy of his ID card etc. See also certificate request.

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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 application 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. 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.

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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.

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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 Digital Signature Act (SigG) and the Digital Signature Ordinance (SigV) aim "to establish general conditions under which digital signatures are deemed secure and forgeries of digital signatures or manipulation of signed data can be reliably ascertained." It came into force on August 1st, 1997. 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.

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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 to 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.

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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).

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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 is 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 called a certificate.

PUBLIC KEY ENCRYPTION ALGORITHM

See asymmetric algorithm.

PUBLIC KEY EXCHANGE ALGORITHM

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

PUBLIC KEY SERVER

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

Q-R

RA

See Registration Authority.

REGISTRATION AUTHORITY

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

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

REGTP

“The Regulatory Authority for Telecommunications and Posts (RegTP) was created on 1 January 1998 as a higher federal authority attached to the Federal Ministry of Economics and Technology. Its headquarters are in Bonn. Its detailed functions may be taken from the Telecommunications Act (TKG) of 27 July 1996 (Federal Law Gazette I p 1120) and the Postal Act (Federal Law Gazette I of 22 December 1997 p 3294). The Regulatory Authority has taken over the functions of the former Federal Ministry of Posts and Telecommunications (BMPT) which was dissolved at the end of 1997. Moreover, the former Federal Office for Posts and Telecommunications (BAPT) which, in addition to implementation functions according to the TKG, performs other functions (e. g. according to the Electromagnetic Compatibility Act) has been integrated into the Regulatory Authority. The BAPT had its headquarters in Mainz and, with its 54 regional offices, was represented all over the Federal Republic of Germany. The regional offices' postal addresses have not changed, solely the Office's designation changed to Regulatory Authority for Telecommunications and Posts (RegTP).” (From the RegTP Web site.)

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.

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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

TC TrustCenter Certification Practice Statement

Version 1.1 of April 1st, 2001

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.