



TC TrustCenter Certificate Policy Definitions

Version of June 12, 2002

1	INTRODUCTION	2
2	IMPORTANT NOTES	4
3	CHANGES TO THE VERSION OF OCTOBER 1ST, 1999	5
4	CERTIFICATE CLASSES	5
4.1	CLASS 0 CERTIFICATES	5
4.2	CLASS 1 CERTIFICATES	6
4.3	CLASS 2 CERTIFICATES	6
4.3.1	<i>Verification of statements of natural persons</i>	<i>6</i>
4.3.2	<i>Verification of statements regarding organizations</i>	<i>6</i>
4.3.3	<i>Verification of statements regarding the relationship of natural person with organizations</i>	<i>6</i>
4.4	CLASS 3 CERTIFICATES	7
4.4.1	<i>Verification of statements regarding natural persons</i>	<i>7</i>
4.4.2	<i>Verification of statements regarding organizations</i>	<i>7</i>
4.4.3	<i>Verification of statements regarding the relationship of natural person to organizations</i>	<i>7</i>
5	NAMING CONVENTIONS.....	8
5.1	X.509 CERTIFICATES	8
5.2	WTLS CERTIFICATES	10
5.3	PGP CERTIFICATES	10
6	VERIFICATION OF CERTIFICATE INFORMATION.....	11
7	CERTIFICATE REVOCATION	12



1 Introduction

This document describes the TC TrustCenter Certificate Policy Definitions. The purpose of this document is to allow an estimation of the trustworthiness of the certificates issued by TC TrustCenter.

Each certificate is only as trustworthy as the procedure followed for its issuance. The higher the certificate class, the more extensive identification verifications are being used as the basis for the issuance of the certificate. The certificates themselves contain information regarding the class of the certificate for anyone who wishes to rely on the certificate. The verification procedures being followed for each certificate class are explained in this Certificate Policy Definitions.

The Certificate Policy Definitions describe the process used by TC TrustCenter as a certification service provider (Certification Authority) when identifying a certificate holder. This document explains the classification of certificates in the certificate classes for applicants respectively certificate holders as well as for third parties. This enables a decision as to whether the presented certificate is sufficient for the used application. Both parties, often referred to as "Subscribing Customer" (certificate holder) and "Relying Customer" (the party relying on the trustworthiness of a certificate), are also referred to as "participants".

Within the context of classification into certificate classes a distinction is made between natural persons and organizations. Certificates of persons who do not make a statement regarding an organization do not contain statements about an organization which the certificate holder belongs to. Contrary to the foregoing, organizational certificates always contain a statement regarding an organization. These certificates may either be attributed to an organization (such as server certificates which cannot be attributed to natural persons) or they may be attributed to a member of an organization, such as an employee of a company for example. Information about an organization must be entered into all organizational certificates.

Along with describing the classification of the certificate classes (Clause 4), the personal identification is explained in detail. The personal identification is necessary for some certificate classes to increase the amount of trust that may be placed in the reliability and strength of the bond created by TC TrustCenter's issuance of a certificate belonging to that particular certificate class to the subscriber.

Naming conventions for certificates are explained next (Clause 5). A certificate often contains nothing but the subscriber's full name and his e-mail address, but sometimes an organization and the location of its headquarters (or the subscriber's place of residence) is specified as well. The description of these guidelines in section 5 is followed by a couple of examples that demonstrate proper (certificate) names.

The issue of how TC TrustCenter verifies the subscriber information represented in a certificate is addressed in Clause 6. Not all data appearing in a certificate must have necessarily been confirmed. A spreadsheet is provided from which a relying party can deduce, for any given certificate policy supported by TC TrustCenter, exactly what type of information is checked, and how.

Finally, information about when and how a certificate is to be revoked is given in Clause 7.

Information on products and services is available on our Web site.

It is essential to read the following section, "2. Important notes".

TC TrustCenter Certificate Policy Definitions

Version of June 12, 2002



Contact information:

TC TrustCenter AG
Sonninstrasse 24-28
20097 Hamburg, Germany

Internet: <http://www.trustcenter.de>
E-Mail: info@trustcenter.de
Phone: +49 (0)40 80 80 26-0
Fax: +49 (0)40 80 80 26-126

Adjustment due to market necessities: Due to constantly changing market needs it is inevitable to adjust the services of a certification authority to the concrete needs of customers. The Certificate Policy Definitions are therefore adjusted regularly.

German edition prevails: Some documents and the website are available both in the German and the English edition. In cases of doubt, the German edition shall prevail.

Errors and omissions excepted: Errors on statements made in this document are expressly excepted, especially with regard to technical descriptions or procedures explained herein.

Copyright notice: This document is protected by intellectual property rights. No information or images, fully or partially, in any form or by any means, may be reproduced, copied, duplicated, published or used in electronic systems or translations without the prior written consent of TC TrustCenter. This represents a crime, excluding printing and duplicating for one's own use.

All information in this document is compiled with great care. Neither TC TrustCenter nor the author are liable for any damages or disservice, that are in connection with the use of this document.

„TC TrustCenter“, the TC TrustCenter logo, „Ident Point“, „TC PKI“ and „TC Info Line“ are registered trademarks of the TC TrustCenter AG.

All brands, product names and trademarks used in this document, but not listed above, are trademarks or service marks of the respective owners.

Copyright © 2002 TC TrustCenter AG, Sonninstrasse 24 - 28, 20097 Hamburg, Germany. All rights reserved.



2 Important notes

Issuance of certificates according to the current Certificate Policy Definitions: All certificates issued by TC TrustCenter are issued based on the current Certificate Policy Definitions at the time of the issuance of the certificate. A later modification of the Certificate Policy Definitions has no influence on already issued certificates..

The higher the certificate class, the higher the level of trust: All certificates issued by TC TrustCenter belong to one of several “level of trust” certificate classes, each one indicating which information contained in a certificate has been verified, and how personal identification is done. This enables a relying party to assess the trustworthiness of the contents of a certificate: The higher the certificate class, the higher the trustworthiness. It does not affect, however, the security of the encryption and the confidentiality of secure communication.

No verification of creditworthiness: TC TrustCenter confirms the identity of a certificate applicant as described in this document. This does not include verification of liquidity, creditworthiness or anything of that nature. A certificate provides a certain level of assurance that the certificate belongs to the entity named therein. It gives no indication whatsoever about the trustworthiness of the entity himself.

No verification of harmlessness of software: TC TrustCenter issues among others special certificates for organizations and natural persons that can be used to sign programming code. It has to be obeyed that TC TrustCenter does not certify the programming code itself, its harmlessness, its algorithmical correctness or any other applicability. Certificates issued in this scope are intended to enable the user to recognize manipulations of the software distributed by the manufacturer. Next to this, the origin of the software can be deducted by such certificates.

No assurance of up-to-date certificate data: TC TrustCenter verifies the information contained in a certificate request only within the scope and during registration at the time of issuance of a certificate. TC TrustCenter accordingly does not provide any assurance that this data is up-to-date after registration. When extending a certificate, the data contained therein will not be verified again. Every certificate holder is obliged to revoke its certificate if data contained therein is not accurate any more.

The end user must determine whether a given certificate is adequate: TC TrustCenter issues certificates under different certificate policies, which describe the level of trust that may be placed in their authenticity. Any participant of the certification service must decide for himself whether a given certificate policy, which is represented by a certificate class as described in this document, meets the security needs for the application in question.

Participants obligation to inform himself: It is essential for any end user participating in TC TrustCenter’s certification services to acquire sufficient knowledge about the use of digital signatures, certificates and public key algorithms.

Subscriber’s duties to take good care and to cooperate: The subscriber has to contribute to the security of certificates and digital signatures. Therefore, it is essential to follow the guidelines as set out in this document.

TC TrustCenter reserves its right to revoke certificates: In the event that cryptographic algorithms or associated parameter are unsafe due to technological progress or new developments in cryptology, TC TrustCenter reserves its right to revoke certificates that are based on such algorithms and parameter. Certificates may also be revoked if the certificate holder has made false statements, respectively TC TrustCenter has obtained knowledge that the statements in the certificate do no longer comply with the facts.



3 Changes to the version of October 1st, 1999

- TC TrustCenter also issues certificates for WAP-Gateways (WTLS).
- The requirements of Class 3 for organizations are more customer friendly in comparison to the previous version: The personal identification of an authorized representative as stated in the certificate of commercial registration (or an equivalent document) is no longer necessary. Instead, an authorized representative of the organization may appoint a person (PKI-administrator), who is responsible for the administration of the certificates related to the organization. This person then must be personally identified.
- The identification based on the personal (physical) presence of the certificate holder for a Class 3 certificate is always necessary. The identification may be carried out either by a TC TrustCenter IdentPoint®, by using the Post Ident® procedure or in an authorized IdentPoint®, utilizing the guidelines for identification of TC TrustCenter.
- In addition to the verification of data based on a (notarized) extract of a competent official register, it is now possible to verify data using on trustworthy address- or company data bases of third parties. Only such data bases are used that comply with the requirements of TC TrustCenter.
- Within the process of reorganization of the certificate class structure, the issuance of Class 4 certificates has been ceased. Class 4 certificates issued before the date of publication of these Certificate Policy Definitions comply with the Certificate Policy Definitions valid on the day of their issuance.

4 Certificate classes

The trustworthiness of certificates depends on the procedures used for their issuance. Every certificate issued by TC TrustCenter belongs to a defined class of "Level of Trust". The class of a certificate describes the general measures taken by TC TrustCenter in order to confirm a certificate's contents and the identity of the certificate holder. The higher the certificate class, the more comprehensive the validation of the applicants identity is.

The certificate itself contains information about the certificate class for all those who intend to rely on the certificate. This enables a relying party to assess the trustworthiness of the data contained in a certificate. What verification measures are being taken for which certificate class can be read in these Certificate Policy Definitions.

The security of the encryption, and consequently, the level of protection against unauthorized access to the transmitted data, is not affected by the chosen certificate class. It depends only on the key length used. The level of protection when using a Class 1 certificate is exactly the same as when using a Class 2 or a Class 3 certificate, as long as the same key length is being used.

4.1 Class 0 certificates

TC TrustCenter issues, on request, certificates for testing and demonstration purposes. These are valid for a short period of time only.

Data contained in a Class 0 certificate is not verified by TC TrustCenter in any way!



4.2 Class 1 certificates

Class 1 certificates always contain an e-mail address. Class 1 certificates confirm that the stated e-mail address existed at the time of application and that the owner of the public key had access to this e-mail address.

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

4.3 Class 2 certificates

4.3.1 Verification of statements of natural persons

Statements made in a Class 2 certificate regarding natural persons, if such are included, are verified in the following way:

- if an e-mail address is stated in the certificate, its correctness is tested by an access test. Alternatively, the organization may validate the correctness of the e-mail address.
- Statements of names belonging to a natural person are verified by
 - a) confirmation of a third party regarding the correctness and the completeness
 - or by
 - b) confirmation of the statements by presentation of a copy of an official photo ID document with a signature and by a handwritten signature respectively a digital signature.

4.3.2 Verification of statements regarding organizations

Statements made in Class 2 certificates regarding organizations are verified in the following way:

- Name and registered office of an organization are verified. This verification may be carried out by a presentation of a copy of a document, which verifies the existence of the organization (current extract of a competent official register in which the organization is listed or a comparable document). The verification may also be carried out utilizing data provided by trustworthy third parties.
- The correctness of an e-mail address of organizations or members of organizations (if such is stated in the certificate) may be confirmed by a responsible person of the organization so that an access test is optional.

4.3.3 Verification of statements regarding the relationship of natural person with organizations

The affiliation of a person named in a certificate to a stated organization, where applicable also the affiliation to a department of the organization, must be confirmed by an authorized member of that organization. This confirmation must have a handwritten signature and a stamp of the organization (for governmental agencies an official seal is needed) or it must be digitally signed. The certificate used for the digital signature must be a TC TrustCenter Class 2 certificate (with a verification of the statements in accordance with 4.3.1 b) above), a TC TrustCenter Class 3 certificate or a certificate in compliance with the German Signature Act.



4.4 Class 3 certificates

4.4.1 Verification of statements regarding natural persons

The verification of statements about a natural person covers the following points:

- If an e-mail address is stated, its correctness is verified by an access test. If statements about an organization are made in the certificate, the organization itself may confirm the correctness of the e-mail address.
- If a natural person is named in a Class 3 certificate, the personal appearance and the presentation of an official photo ID is necessary.
- The verification of the identity of the certificate holder may either take place in a branch office of the German Post utilizing the Post Ident® procedure, in a TC TrustCenter Ident-Point® (a authorized IdentPoint® of the organization) or with another representative of TC TrustCenter, authorized to perform the identity verification.
- Only official ID documents that contain a photo and a handwritten signature of the ID holder are accepted for verification purposes. In the Federal Republic of Germany such documents are among others the personal identity card (Personalausweis) and the passport (Reisepass). In any case such documents must fulfil the requirements set out by §1 section 2 of the Identity Card Act (Gesetz über Personalausweise) respectively § 4 section 1 of the Passport Act (Passgesetz).

4.4.2 Verification of statements regarding organizations

For organizational certificates the following verification are performed:

- Name and registered office of the organization. For Class 3 certificates it is, depending on the organization, necessary to present an extract of the competent official register respectively a comparable document. It is important that the document states that the organization exists in fact. The document presented must be up to date (not older than three months) and, if possible, notarized. As for Class 2 certificates, this verification may be performed based on data bases of trustworthy third parties.
- Further certificate data will be verified to the extend possible. For server certificates for instance, the registration of the stated domain will be checked against the organization named in the certificate application.

4.4.3 Verification of statements regarding the relationship of natural person to organizations

- The affiliation of a person to a stated organization, where applicable also the affiliation to a department of the organization, must be confirmed by an authorized member of that organization. This confirmation must have a handwritten signature and a stamp of the organization (for governmental agencies an official seal is needed) or it must be digitally signed. The certificate used for the digital signature must be a TC TrustCenter Class 3 certificate or a certificate in compliance with the German Signature Act.



5 Naming conventions

TC TrustCenter issues certificates in accordance with the X.509, the WTLS and the PGP standard. X.509 certificates are, among other things, used by Web servers and Web browsers to ensure secure Internet communication or to enable an authentication of the user by the web server as well as to establish a virtual private network (VPN) on public data interfaces. X.509 certificates can also be utilized to use the encryption and signing standard S/MIME, supported by many browsers or popular e-mail applications. WTLS certificates are used for the secure data transfer between WAP servers and WAP clients (e.g. cellular phones). PGP certificates are, among other things, used for the encrypted communication via e-mail or for encrypting and signing data files.

This section provides guidelines on entering the appropriate information in the data fields that make up X.509 certificates, generate a certificate name for WTLS certificates and for choosing proper PGP user IDs.

In certain projects and after consultation with TC TrustCenter, it can be deviated from the contents of the certificate fields stated in the following.

5.1 X.509 certificates

X.509 certificates usually consist of the data fields mentioned in the following table, and these are explained in detail and illustrated by examples below.

Field	Meaning
C	Country
SP	State / Province
L	Locality
O	Organization
OU	Organizational Unit
CN	Common Name
Email	E-mail

C (Country): This field contains the two-letter county code as set out in ISO 3166-1. Persons without relationship to an organization state the country of their residence, organizations state the country where their registered office is located. For server certificates that have to be generated with a server software, the subscriber must enter the correct ISO code, e. g. "US" for the USA and "FR" for France.

SP (State/Province): This field is intended for providing the state. In Germany, the state could be entered here. However, we recommend to just leave this field blank.

L (Locality): This field is used for the location of a company's registered office or the location, where the certificate holder lives as stated in the official ID document (or official statement of residence) if an organization is not stated in the "O" field. The postal code is not to be stated.

O (Organization): This field is used for the name of the organization as is it stated in the documents presented for verification or as stated in the data bases of third parties. Usually,

TC TrustCenter Certificate Policy Definitions

Version of June 12, 2002



this is the name under which the organization is acting officially or as stated on its official letter heading. It is recommended to state the organization with its full name and its legal form, e.g. "TC TrustCenter AG" instead of "TC TrustCenter" or "TCTC AG".

OU (Organizational Unit): This field may be used for specifying the department within the organization that the certificate is attributed to. For code signing certificate requests, TC TrustCenter will automatically enter the name of the software used for generating the signature.

CN (Common Name): The CN field is usually used to specify the name of the natural person the certificate is attributed to. If the certificate request is generated using an Internet browser, the common name is constructed by concatenating the user input from the first and last name input fields. The names and parts of the name shall be stated as stated in the official ID card. Parts of names as well as titles or doctoral degrees can only be stated if such are also stated in the official ID card or proven by equivalent documents separately. Doctoral degrees or comparable parts of names shall precede the name.

Server certificate requests are an exception to this rule: Here, the common name field must contain the full domain name of the Web server in order to work with popular browsers, for example `www.stonehillbaker.com`.

For TC Code Signing certificates, the input from the O field ("organization") is automatically copied to the common name field, because the content will usually be displayed when a user verifies signed programming code.

E-mail: This field is must contain a valid e-mail address, if filled out. Many Web server applications, however, will not allow an e-mail address to be specified, because a Web server generally does not have an e-mail address. If the server software provides for an e-mail address, it is recommended to specify the webmaster's e-mail address, like `webmaster@company.com` or `info@company.com`. It is not recommended to enter a personal e-mail address in a server certificate.

The collection of the seven data fields listed above is commonly referred to as the Distinguished Name (DN). Please view the following example for the construction of a DN:

```
/C=DE/L=Hamburg/O=Stonehillbaker Deutschland GmbH/CN=www.stonehillbaker.com/Email=webmaster@stonehillbaker.com
```

The same DN must not be assigned to different entities, while the same entity may have several certificates all bearing the same DN.

Examples for X.509 Distinguished Names

	C	SP	L	O	OU	CN	EMAIL
Natural person	DE		Hamburg			Dr. John Freeman	john.freeman@stonehillbaker.com
Organization	DE		Hamburg	Stonehillbaker Deutschland GmbH	Purchase	Dr. John Freeman	john.freeman@stonehillbaker.com
Server	DE		Hamburg	Stonehillbaker Deutschland GmbH	Internet Services	www.stonehillbaker.com	webmaster@stonehillbaker.com
Code-Signing	DE		Hamburg	Stonehillbaker Deutschland GmbH	Microsoft Authenticode	Stonehillbaker Deutschland GmbH	info@stonehillbaker.com



5.2 WTLS certificates

WTLS certificates do not know data fields as compared to X.509 certificates, that compose the certificate name (X.509 terminology: Distinguished Name, see section "X.509 certificates"). Instead, the certificate name can be chosen freely, in principle.

Nevertheless it is recommended to compose the character string like a X.509 DN, whereas to only include necessary information due to the limited memory and display space of WAP end products.

Examples for WTLS certificates

```
/C=DE/O=Stonehillbaker Deutschland GmbH/CN=wap.stonehillbaker.com
```

```
/C=DE/O=Stonehillbaker Deutschland  
GmbH/CN=wap.stonehillbaker.com/Email=info@stonehillbaker.com
```

5.3 PGP certificates

PGP's certificate format does not provide data fields in certificates like X.509 does. PGP version 5.0 and above asks the user to specify name and e-mail address separately, and the latter is appended to the user's name, enclosed by pointed brackets (from PGP 5.0 onwards, these brackets are added automatically). As an example, a PGP user ID may have the following form, which is recommended for non-commercial PGP certificates:

```
Dr. John Freeman <john.freeman@stonehillbaker.com>
```

Commercial users should choose a user ID that contains the same information a corresponding X.509 certificate would have. Using the data field identifiers the X.509 standard specifies, a PGP user ID then has the following structure:

```
CN, O, OU, L, C <Email>
```

In principle, all of the identifiers above are optional and one should omit OU, L and C, and provide CN and O, e. g.

```
Dr. John Freeman, Stonehillbaker Deutschland GmbH  
<john.freeman@stonehillbaker.com>
```

or alternatively (more detailed but less clear)

```
Dr. John Freeman, Stonehillbaker Deutschland GmbH, Purchase, Ham-  
burg, DE <john.freeman@stonehillbaker.com>
```

The direct application of certificates from PGP software is currently not supported by TC TrustCenter.

Examples for PGP User IDs

Person	Dr. John Freeman, Hamburg Dr. John Freeman <john.freeman@stonehillbaker.com>
Organization	Dr. John Freeman, Stonehillbaker Deutschland GmbH, Hamburg <john.freemmann@stonehillbaker.com>



6 Verification of certificate information

TC TrustCenter verifies the contents of the X.509 certificate data fields as specified in the following table (PGP accordingly). The entries used in the table are described below.

Class	C	SP	L	O	OU	CN	Email
Class 0	No check	No check	No check	No check	No check	No check	No check
Class 1	No check	No check	No check	Empty	Empty	No check	Access test
Class 2 organization	RegA or ADB	No check	RegA or ADB	RegA or ADB	Written confirmation	Written confirmation	Access test or written confirmation
Class 2 natural person with organization	RegA or ADB	No check	RegA or ADB	RegA or ADB	Written confirmation	Written confirmation	Access test or written confirmation
Class 3 organization	Notarized RegA or CDB	No check	Notarized RegA or CDB	Notarized RegA or CDB	Written confirmation	Ident, domain if applicable	Access test or written confirmation
Class 3 natural person with organization	Notarized RegA or CDB	No check	Notarized RegA or CDB	Notarized RegA or CDB	Written confirmation	Ident	Access test or written confirmation

No check: TC TrustCenter does not verify the content of this data field.

Empty: This field must be empty.

Access test: If the certificate contains an e-mail address, this e-mail address will be checked. Class 1 certificates always contain an e-mail address. In order to verify the validity of an e-mail address and the subscriber's access to this address, TC TrustCenter sends an e-mail to the address contained in the certificate request (exception: For Class 2 and Class 3 certificates for organizations it can be waived to send this e-mail, as far as the correctness of this e-mail address has been confirmed by a responsible person. This e-mail includes information that must be sent back to TC TrustCenter for the identification of the applicant to be completed.

RegA: Information in this field is verified by checking an extract of the competent register or comparable documents. It is important that the document states that the organization exists in fact. Depending on the legal form of the organization and on the country, there are different competent authorities. For privately organized companies this is usually the commercial register. For governmental organizations (such as governmental agencies, ministries or state owned organizations) there are usually no registers. In such cases the existence of the organization is to be confirmed by the agency holding the official seal or the competent supervisory authority.

ADB: The statements in this field are verified based on data bases of third parties (e.g. credit card companies, Post). Statements that are based on inquiries of the person that is to be certified will not be accepted.



CDB: The statements in this field are verified based on company data bases of third parties. The notarization of the statements is not necessary. The commercial data bases will be contacted by TC TrustCenter directly or on behalf of TC TrustCenter. Statements that are based on inquiries of the organization that is to be certified will not be accepted.

Written confirmation: Data entered in this field must be confirmed in writing by a responsible person. This should be done in conjunction with an application confirmation, naming the employees who shall obtain a certificate, and the department they work for and, if applicable also the e-mail address or the domain name. This confirmation does not have to be submitted for every single certificate, but could also be submitted for large amount of certificates. Example: Certificates for employees of a company or a department of a company.

Ident: The verification of such data is being executed by comparison of the presented official ID card and the application form, which is being sent to TC TrustCenter in the process of the identification.

Domain: For server certificates, it is verified that the full domain name given in the CN field is registered to the organization named in the certificate by using Internet domain registration services. If O contained "Stonehillbaker" and CN was "www.stonehillbaker.com", it would be verified that "www.stonehillbaker.com" is registered to the organization named in O. If this is not the case, the applicant must provide an authorization of the owner of the domain for the use of the domain name by the certificate holder.

7 Certificate Revocation

A certificate must be revoked (in writing, via telephone or via the website of TC TrustCenter) in case:

1. The corresponding private key has been lost,
2. It is suspected that unauthorized persons have access to the private key or are able to manipulate the private key,
3. Certificate data has become incorrect (e. g. because of a change of one's e-mail address).

* * *