



TRUSTCENTER
a company of  GeoTrust

TC TrustCenter Certificate Policy Definitions

Version of April 24th , 2006

TC TrustCenter Certificate Policy Definitions

Version of April 24th , 2006



1	INTRODUCTION	3
2	IMPORTANT NOTES	5
3	CHANGES TO OLDER VERSIONS	6
3.1	CHANGES TO THE VERSION OF OCTOBER 1 ST , 1999	6
3.2	CHANGES TO THE VERSION OF JUNE 12 TH , 2002	6
3.3	CHANGES TO THE VERSION OF JULY 15 TH , 2004	7
4	CERTIFICATE CLASSES	8
4.1	CLASS 0 CERTIFICATES	8
4.2	CLASS 1 CERTIFICATES	8
4.3	CLASS 2 CERTIFICATES	8
4.3.1	<i>Verification of statements about natural persons</i>	8
4.3.2	<i>Verification of statements about organizations</i>	9
4.3.3	<i>Verification of statements about the relationship of a natural person to an organization</i>	10
4.4	CLASS 3 CERTIFICATES	10
4.4.1	<i>Verification of statements about natural persons</i>	10
4.4.2	<i>Verification of statements regarding organizations</i>	10
4.4.3	<i>Verification of statements regarding the relationship of natural person to organizations</i>	11
5	NAMING CONVENTIONS	12
5.1	CHARACTER SET AND RULES FOR CONVERSION	12
5.1.1	<i>Conversion of Characters</i>	12
5.2	X.509 CERTIFICATES	13
5.3	WTLS CERTIFICATES	15
6	VERIFICATION OF CERTIFICATE INFORMATION	16
7	CERTIFICATE REVOCATION	18

1 Introduction

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

A certificate is an electronic document which assigns a public cryptographic key to a person or to an organisation and which confirms the identity of that person or organisation. Thus a certificate binds a person or organisation to a cryptographic key

Each certificate is only as trustworthy as the procedures followed for its issuance. For that purpose TC TrustCenter groups the certificates into "certificate classes". 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.

These Certificate Policy Definitions describe the processes 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 for persons who do not provide information about their affiliation to 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.

Parallel with the description of the classification of certificates into classes (Section 4), the personal identification is explained in detail. The personal identification is necessary for some certificate classes to increase the reliance in the strength of the bond between the certificate and the certificate holder.

Naming conventions for certificates are explained next (Section 5). A certificate often contains only the subscriber's full name and his e-mail address. 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.

Section 6 describes how TC TrustCenter verifies the correctness of the data contained in a certificate. Depending on the certificate class not necessarily all the data in a certificate must have been confirmed. A table (page 16) 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 Section 7.

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

TC TrustCenter Certificate Policy Definitions

Version of April 24th , 2006



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

Contact information:

TC TrustCenter GmbH
Sonninstrasse 24-28
20097 Hamburg
Germany

WWW: <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 GmbH.

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

Copyright © 2006 TC TrustCenter GmbH, 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 Certificate Policy Definitions being valid 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. The certificate classes do not affect 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 itself.

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 taken into account that TC TrustCenter does not certify the programming code itself, its harmlessness, its algorithmical correctness, or its applicability. Certificates issued in this context are intended to enable the user to detect manipulations of the software distributed by the manufacturer. Next to this, the origin of the software can be deduced 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 renewing 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: If cryptographic algorithms or associated parameters become unsafe due to technical progress or new developments in cryptology, TC TrustCenter reserves its right to revoke certificates that are based on such algorithms and parameters. Certificates may also be revoked if the certificate holder provided false information, if certificates are misused or are used for criminal purposes, or if TC TrustCenter has obtained knowledge that data in the certificate do no longer comply with the facts.

3 Changes to Older Versions

3.1 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 trustworthy third party identity proofing services or databases. Only such data bases are used that comply with TC TrustCenter 's requirements.
- 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.

3.2 Changes to the version of June 12th, 2002

- For Class 2 certificates, fax copies will be accepted.

Sending documents by mail, in particular international, often causes undesirable delay.

In order to enable customers to acquire class 2 certificates more rapidly TC TrustCenter accepts documents sent by fax.

This means that whenever the Certificate Policy Definitions require the presentation of a copy of a document it is admissible to send a fax.

- Extracts from registers are grouped into three classes depending on their age.

Extracts being not older than 9 month are accepted as up to date. For extracts, which have been issued between 9 and 36 months ago an additional confirmation, signed by an authorized member of the organisation, must be presented. This confirmation must state that the name, and the legal form of the organisation are still valid. TC TrustCenter does not accept register extracts, which are older than 36 months.

- TC TrustCenter now issues Team Certificates and Function Certificates.

A Team Certificate can be used by a group of persons (e.g. a department of an organisation). For formal reasons it is assigned to the person who is responsible for that group (e.g. head of department).

Function Certificates are dedicated to computers or applications in order to serve special purposes, for instance signing of bills. The computer or application can use the certificate to generate a multitude of signatures automatically.

- The production of PGP certificates has been ceased.

3.3 Changes to the version of July 15th, 2004

- TC TrustCenter now issues wildcard certificates. Instead of the of a webserver's host-name a wildcard certificate contains the symbol "*", which serves as a placeholder for several hostnames. Thus, a wildcard certificate is able to protect more than one website. Organizations owning a single domain but running several webserver in that domain can use a wildcard certificate as an efficient solution because protecting more than one website requires the administration of one certificate only.
- TC TrustCenter reserves the right to revoke certificates which have been misused and/or are used for criminal purposes.

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 is the validation of the applicants identity.

The security of the encryption, and consequently, the level of protection against unauthorized access to the transmitted data, depends on the cryptographic algorithms and parameters. It is not affected by the chosen certificate class. 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 used.

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 is presented in these Certificate Policy Definitions.

The following sections contain explanations about the verification procedures. All explanations only refer to data contained in certificates.

In addition to the verifications confirming the certificate’s content TC TrustCenter performs additional checks if certificates are issued for organizations. These checks are to prove that the organization has authorized the certificate application, and that the person submitting the certificate application on behalf of the organization is authorized to do so.

This proof (application confirmation) must be signed by an authorized entity in the organization and can be sent to TC TrustCenter by mail, e-mail, or by fax. Alternatively TC TrustCenter may verify the authorization to apply for a certificate by phone.

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 e-mail address stated in the certificate existed at the time of application and that the owner of the public key had access to this e-mail address.

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

4.3 Class 2 certificates

4.3.1 Verification of statements about natural persons

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

TC TrustCenter Certificate Policy Definitions

Version of April 24th , 2006



- if the certificate contains an e-mail address, its correctness is verified by an access test. Alternatively, for members of organizations a responsible person in that organization may confirm the correctness of the e-mail address.
- Statements about a natural person's name are verified by
 - a) confirmation of an accredited third party regarding the correctness and the completenessor by
 - b) confirmation of the information by presentation of a copy of an official photo ID document with signature.

4.3.2 Verification of statements about organizations

Statements made in Class 2 certificates about 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 proves the existence of the organization (current extract of a competent official register in which the organization is listed or a comparable document).

Extracts being not older than 9 months are accepted as up to date.

For extracts, which have been issued between 9 and 36 months ago, an additional confirmation must be presented. This confirmation must state that the name and the legal form of the organization are still valid. If TC TrustCenter is already in possession of a copy of an extract of an official register it need not be sent again.

The confirmation must be presented on a paper with the official letterhead of the organization. It must be signed by an authorized person.

The confirmation may be sent by fax or e-mail. An e-mail must be signed with a certificate which fulfils at least the requirements of a TC class 2 certificate.

TC TrustCenter does not accept register extracts which are older than 36 months

The existence and correct denomination of governmental or administrative authorities must be confirmed by a competent authority (e.g. a superior authority) with official letterhead, stamped with an official stamp or seal, and signed by an authorized officer.

All vetting may also be carried out utilizing data provided by trustworthy third parties.

If an applicant requires more than one certificate but does not want them to be issued at the same time, TC TrustCenter may perform a pre-vetting at the time of registration or later. The actual application for the certificate is then sent later, but the results of the vetting are already present. When a certificate is issued the pre-vetting must not be more than twelve months ago.

- The correctness of an e-mail address of an organization or a member of an organization (if such is stated in the certificate) may be confirmed by a responsible person of the organization, an access test is then optional.
- Additional data in the certificate are verified as much as possible. For server certificates it is checked if the domain name in the certificate is registered to the organization applying for the certificate. In contrast to that, an automatic verification of the existence on an organizational unit (which can be stated in the OU field of the certificate) is usually not possible.

A domain registration may be checked in advance. When the certificate is issued the domain check must not be more than twelve months old.

A Team Certificate may be used by a group of persons (e.g. a department of an organization); nevertheless it is formally assigned to a single person, who is responsible for the group (e.g. head of department). This person is responsible for the proper use of the Team Certificate, and this person must be identified in compliance with the rules for class 2 certificates (or higher) of these CPD.

Function Certificates are certificates, which are selected for a special purpose (e.g. automatic signature of outgoing mail). Usually they are bound to a fixed computer or application. The computer or application can use the certificate and automatically produce a multitude of signatures. Formally such a certificate is assigned to a person who is responsible for the proper use of the certificate, and this person must be identified in compliance with the rules for class 2 certificates (or higher) of these CPD.

4.3.3 Verification of statements about the relationship of a natural person to an organization

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 confirmation may be sent by fax or email. The certificate used for the digital signature must fulfil at least the requirements of a TC TrustCenter Class 2 certificate (with a verification of the statements in accordance with 4.3.1 b) above).

Alternatively the affiliation of a person named in a certificate to an organization may be verified by phone.

4.4 Class 3 certificates

4.4.1 Verification of statements about natural persons

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

- If an e-mail address is contained in the certificate, 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 a valid 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 IdentPoint® (an 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 verifications 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 or

respectively a comparable document. It is important that the document states that the organization currently exists. The document presented should be up to date and notarized or be original.

Extracts being not older than 9 month are accepted as up to date.

For extracts, which have been issued between 9 and 36 months ago an additional confirmation, signed by an authorized member of the organization, must be presented. This confirmation must state that the name and the legal form of the organization are still valid. If TC TrustCenter is already in possession of a copy of an extract of an official register it must not be sent again.

The confirmation must be presented on a paper with the official letterhead of the organization. It must be signed by an authorized person.

The confirmation may be sent by fax or e-mail. An e-mail must be signed with a certificate which fulfils at least the requirements of a TC class 2 certificate.

TC TrustCenter does not accept register extracts, which are older than 36 months

The existence and correct denomination of authorities is verified in the same manner as with Class 2 certificates.

All vetting may also be carried out utilizing data provided by trustworthy third parties.

- Additional data in the certificate are verified as far as possible. For server certificates it is checked if the domain name in the certificate is registered to the organization applying for the certificate. In contrast to that, an automatic verification of the existence on an organizational unit (which can be stated in the OU field of the certificate) is usually not possible.

A Team Certificate may be used by a group of persons (e.g. a department of an organization); nevertheless it is formally assigned to a single person, who is responsible for the group (e.g. head of department). This person is responsible for the proper use of the Team Certificate, and this person must be identified in compliance with the rules for class 3 certificates of this CPD.

- Function Certificates are certificates, which are selected for a special purpose (e.g. automatic signature of outgoing mail). Usually they are bound to a fixed computer or application. The computer or application can use the certificate and automatically produce a multitude of signatures. Formally such a certificate is assigned to a person who is responsible for the proper use of the certificate, and this person must be identified in compliance with the rules for class 3 certificates of this CPD.

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 and the WTLS 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).

This section provides guidelines on entering the appropriate information in the data fields that make up X.509 certificates, and on generating certificate names for WTLS certificates.

In certain projects and after consultation with TC TrustCenter, deviation from the contents of the certificate fields stated in the following is possible.

5.1 Character Set and Rules for Conversion

The X.509 compliant certificates contain in the designated fields the Distinguished Names of the issuer and of the certificate holder. The following character set is supported:

Upper-case characters	A .. Z
Lower-case characters	a .. z
Digits	0 .. 9
Apostrophe	'
Left parenthesis	(
Right parenthesis)
Plus	+
Comma	,

Hyphen	-
Dot	.
Slash	/
Colon	:
Equal	=
Question mark	?
Space	

This character set contains a limited number of characters. However, TC TrustCenter's certification policies require data in certificates to be spelled exactly as they are spelled in the ID document or register extract. Consequently, there must exist rules for the conversion of "non-presentable" characters.

TC TrustCenter recommends adherence to the following conversion rules. Otherwise the proper functioning of the certificates in connection with other components can not be assured. For example it can not be excluded that some components in a PKI, e.g. older browsers, are not capable of interpreting umlauts correctly.

5.1.1 Conversion of Characters

- Umlauts (Ä, Ö, Ü, ä, ö, ü) are replaced by the respective non-diacritical strings (Ae, Oe, Ue, ae, oe, ue), thereby respecting capitalization and use of lower-case characters.

Examples:

Original	Converted
Müller	Mueller
Überstorf	Ueberstorf

TC TrustCenter Certificate Policy Definitions

Version of April 24th , 2006

- Characters and symbols not being part of the supported character set must be assigned to corresponding characters.

Beispiele:

Original	Converted
René	Rene
François	Francois

- Special characters not contained in the supported character set should either be spelled out or be replaced by corresponding equivalent characters.

Examples:

Original	Konvertiert
Meier & Meier Ltd.	Meier and Meier Ltd.
Meier & Meier Ltd.	Meier a. Meier Ltd.
Meier & Meier Ltd.	Meier + Meier Ltd.

5.2 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 country 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 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. 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 must not 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, this is the name under which the organization is acting officially or as stated on its official

TC TrustCenter Certificate Policy Definitions

Version of April 24th , 2006



letter heading. It is recommended to state the organization with its full name and its legal form, e.g. "TC TrustCenter GmbH" 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 put into the certificate if this data are also present in the official ID card or proven by equivalent documents separately. Doctoral degrees or comparable parts of names shall precede the name.

Furthermore the CN data field may contain other data:

Server Certificates

If the common name field contains the full domain name or the IP address of a web server, e.g. `www.stonehillbaker.com`, the certificate is used as a server certificate.

Wildcard Certificates

Wildcard certificates are a special kind of Server Certificates. They contain the symbol "*" instead of a server name (e.g. `*.stonehillbaker.com`). Several servers in the same domain can be equipped with the same certificate. A certificate issued for `*.stonehillbaker.com` can thus be used for example for `www.stonehillbaker.com`, `mail.stonehillbaker.com`, or `server.stonehillbaker.com`. Apart from that wildcard certificates are treated in the same way as server certificates.

Code Signing Certificates

If the CN-field contains "CodeSigning for <content of the O-field>" the certificate is a CodeSigning certificate. In this case the data from the O-field (Organization) is automatically copied into the CN-field, because usually the CN-field is displayed when a user verifies program code.

Function Certificates

If the CN-field contains the description of a function (e.g. "Automatic Mail Signature") the certificate is used for this designated purpose. If the purpose or function of the certificate is not already clearly specified in the CN-field TC TrustCenter provides — on request— information on the designated purpose of the certificate.

In order to be able to provide information about the usage of a function certificate, and as the denomination needs to be meaningful, the denomination of the function, i.e. the content of the CN-field, must be approved by TC TrustCenter before the certificate is issued.

Formally a function certificate is assigned to a person. This person is responsible for the proper use of the certificate, and this person is identified according to the particular certificate class of the Function Certificate.

Team Certificates

If the CN-field contains "Team-Certificate" the certificate is used by a group of persons or a department of an organization. Which group or department is meant is noted in the OU-field.

TC TrustCenter Certificate Policy Definitions

Version of April 24th , 2006



Formally a function certificate is assigned to a person. This person is responsible for the proper use of the certificate, and this person is identified according to the particular certificate class of the Team Certificate.

Pseudonym Certificates

If the CN-field contains only a number (where appropriate followed by the suffix “:PN”) it is a pseudonym certificate where the clear name of the certificate holder is not contained in the certificate.

E-mail: This field 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@stonehillbaker.com` or `info@stonehillbaker.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). See the following example for 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
Wildcard Certificate	DE		Hamburg	Stonehillbaker Deutschland GmbH	Internet Services	*.stonehillbaker.com	webmaster@stonehillbaker.com
Code-Signing	DE		Hamburg	Stonehillbaker Deutschland GmbH	Microsoft Authenticode	Stonehillbaker Deutschland GmbH	info@stonehillbaker.com

5.3 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
```

6 Verification of certificate information

TC TrustCenter verifies the contents of the X.509 certificate data fields as specified in the following table. 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 or CDB	No check	RegA or ADB or CDB	RegA or ADB or CDB	Written confirmation	Written confirmation, Domain if applicable	Access test or written confirmation
Class 2 natural person with organization	RegA or ADB or CDB	No check	RegA or ADB or CDB	RegA or ADB or CDB	Written confirmation	Written confirmation or confirmation by phone	Access test or written confirmation
Class 2 Function or Team	RegA or ADB or CDB	No check	RegA or ADB or CDB	RegA or ADB or CDB	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
Class 3 Function or Team	Notarized RegA or CDB	No check	Notarized RegA or CDB	Notarized RegA or CDB	Written confirmation	Written confirmation with Ident of the responsible person	Access test or written confirmation

Table 1

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 long 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.

TC TrustCenter Certificate Policy Definitions

Version of April 24th , 2006



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, the function name, or the domain name. This confirmation does not have to be submitted for every single certificate, but could also be submitted for large amounts of certificates. Example: Certificates for employees of a company or a department of a company.

Confirmation by Phone:

The correctness of these data must be confirmed by an authorized person of the organization. TC TrustCenter (or an authorized representative) telephonically contacts the organization and inquires a) if the person named in the certificate is known in the organization and b) if this person is authorized to apply for a certificate.

Ident: The verification of such data is being conducted 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 domain name or IP address given in the CN field is registered to the organization named in the certificate by using Internet domain registration services. If O contains "Stonehillbaker" and CN is www.stonehillbaker.com (or *.stonehillbaker.com in case of a Wildcard certificate), it will be verified that "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

1. A certificate has to be revoked by the certificate holder (in writing, via telephone or via the website of TC TrustCenter) if:
 - a. The corresponding private key has been lost,
 - b. It is suspected that unauthorized persons have access to the private key or are able to manipulate the private key,
 - c. Certificate data has become incorrect (e. g. because of a change of one's e-mail address).
2. If cryptographic algorithms or parameters become insecure because of technological progress or new developments in cryptography TC TrustCenter reserves the right to revoke certificates that are issued using these algorithms or parameters.
3. Certificates may be revoked by TC TrustCenter if the applicant provided false data, or if TC TrustCenter gains knowledge that data contained in a certificate has become invalid.
4. If TC TrustCenter gets aware of a certificate being used abusively and/or for criminal purposes TC TrustCenter reserves the right to revoke such a certificate.
5. If the private key of a certificate is compromised TC TrustCenter may revoke the certificate in order to prevent misuse of the compromised key.
6. TC TrustCenter confirms the revocation of a certificate by a signed e-mail.

* * *