



TC TrustCenter Certificate Policy Definitions

Version of September 1st, 1999

1	INTRODUCTION.....	2
2	IMPORTANT NOTES.....	3
3	CERTIFICATE CLASSES.....	4
3.1	CLASS 0 CERTIFICATES (FOR TESTING ONLY)	4
3.2	CLASS 1 CERTIFICATES.....	4
3.3	CLASS 2 CERTIFICATES.....	4
3.4	CLASS 3 CERTIFICATES.....	5
3.5	CLASS 4 CERTIFICATES.....	6
4	PERSONAL IDENTIFICATION.....	7
4.1	POST IDENT	7
4.2	TC TRUSTCENTER IDENT POINTS®	7
5	NAMING CONVENTIONS	9
5.1	X.509 CERTIFICATES	9
5.2	PGP CERTIFICATES.....	10
5.3	EXAMPLES FOR X.509 DISTINGUISHED NAMES	11
5.4	EXAMPLES FOR PGP USER IDS	11
6	VERIFICATION OF CERTIFICATE INFORMATION	12
7	CERTIFICATE REVOCATION.....	14



1 Introduction

This document describes the TC TrustCenter Policy Definitions (CPD). It explains the classification of the various policies and the meaning of the associated certificate classes to all end users, i. e., subscribers and relying parties. It aims to help the relying party in making a decision whether the level of trust that can be attributed to a given certificate is sufficient for the application at hand.

After describing the certificate classes, the personal identification that is required for some of them is explained in detail. The personal identification increases 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 are discussed next. A certificate often contains nothing but the subscriber's full name and his e-mail address, but sometimes a company and the location of its headquarters (or the subscriber's place of residence) is specified as well. The description of these guidelines is followed by a couple of examples that demonstrate proper choice of (certificate) names.

The issue of how TC TrustCenter verifies the subscriber information represented in a certificate is addressed next. Not all data appearing in a certificate must necessarily have been confirmed, and a table is provided in the concluding section 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 to revoke a certificate is given in the last section.

Detailed product information is available from the products pages on our Web site.

General information on encryption and public key algorithms is available from the support pages on our Web site.

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

Contact information:

TC TrustCenter for Security in Data Networks GmbH
Am Werder 1
21073 Hamburg
Germany

WWW: <http://www.trustcenter.de>
E-Mail: info@trustcenter.de
Phone: +49 40 76629-3301
Fax: +49 40 76629-577



2 Important notes

TC TrustCenter is not a licensed Certification Authority in accordance with § 4 of the German Digital Signature Act (SigG). TC TrustCenter has filed an application at the [RegTP](#) in order to obtain a license.

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 a certificate (or, more precisely, its contents). 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.

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 subscriber or relying party 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.

End user’s obligation to inform himself. It is essential for any end user participating in TC TrustCenter’s certification services to receive proper training in the use of digital signatures, certificates and public key algorithms. Documentation and training regarding these topics is provided by TC TrustCenter on its Web site.

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 forth in the subscriber’s duties to take good care and to cooperate, which are part of the [General Terms and Conditions](#) (GTC).

Adaptation to market demands. Because market structures and demand change continuously, this CPD will inevitably evolve to meet current business needs in electronic commerce. Whenever new services are offered or existing structures are amended, this CPD and / or the GTC will be updated and posted to the repository. For a short period of time, there may be minor differences between these documents.

German version is decisive. Some of the documents and Web pages are available both in German and English. In any case of doubt, the German version is decisive.

Errors excepted.



3 Certificate classes

Every certificate issued by TC TrustCenter belongs to a defined certificate class, reflecting the measures taken by TC TrustCenter in order to confirm a certificate's contents and the subscriber's identity. This enables a relying party to assess the trustworthiness of a certificate presented, and consequently, the digital signature made by the subscriber.

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 on the key size used. Confidentiality is ensured by encrypting data, using any certificate, no matter what certificate class it belongs to. What varies is the level of assurance that the certificate holder is indeed the named entity.

3.1 Class 0 certificates (for testing only)

In order to test how secure communication works in their business environment, TC TrustCenter issues demo certificates to business customers upon request. These are valid for a short period only and may not be used for any other purpose than testing how the certificate integrates with the systems and applications at hand.

Any data contained in a demo certificate is not verified by TC TrustCenter in any way!

3.2 Class 1 certificates

Class 1 certificates are issued to private subscribers only. Class 1 certificates always contain an e-mail address, and TC TrustCenter confirms that the owner of the public key has access to this e-mail address.

Class 1 certificates provide very little authentication of the subscriber's identity. Therefore, the level of assurance is low. TC TrustCenter simply checks that the given e-mail address is valid. Any subscriber information other than the e-mail address must be considered non-verified.

Class 1 certificates are primarily intended for client authentication (to Web servers) and personal e-mail, in order to provide a minimum level of security. Class 1 certificates should not be used or relied upon for private or commercial applications that require personal identification.

3.3 Class 2 certificates

Class 2 certificates are issued for both business and private (individual) use. Regarding the latter, certificates will only be issued to individuals not living in Germany, because otherwise personal identification would be possible without any trouble (see the section "Personal identification"), so Class 3 should be preferred.

Business customers might want to contact TC TrustCenter in advance in order to obtain, if necessary, detailed information on how to proceed, what documents to provide, how to generate a conforming certificate request etc.

Class 2 certificates for business use state that

1. the named organization exists. A corporate entity must provide TC TrustCenter with a copy of the memorandum that establishes the company and that is required for registration with the national register of corporations and / or local chamber of commerce, or with 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. The supplied document must not be older than six months.

2. employees authorized to sign have confirmed the certificate's contents either themselves or given a third person permission to do so on their behalf. This confirmation must either be submitted in writing or as an electronic document that was digitally signed using a TC TrustCenter certificate of Class 2 or above.
3. the certificate data, except for personal information, has been validated by TC TrustCenter as far as possible (see the section "Verification of certificate information" for details). For server certificates, this includes a check that the server domain is registered to the organization named in the certificate. If an e-mail address is included in the certificate, it is checked as well, i. e., the Class 2 policy is a superset of the Class 1 policy.

Private customers receive a written confirmation of their certificate request that contains the information supplied in the request. They must sign the confirmation and send it back to TC TrustCenter, along with a copy of their identity card. This copy replaces the copy of the company memorandum that business customers must provide, in order to provide a comparable level of trust.

Class 2 certificates establish a level of trust that is necessary for acceptance of certificates and digital signatures in certain areas of business communication. They do not, however, require any personal identification. It is strongly recommended that Class 3 certificates are used instead for any application in the area of electronic commerce, electronic banking and other financial transactions exceeding micro payments, in order to establish a higher level of trust!

Class 2 certificates are primarily intended as a simple way to set up secure communication among closed user groups or business partners that know one another outside the Internet, for example to transmit confidential business information between different branches of the same company, or for secure business e-mail communication.

Private customers not living in Germany are provided with a comfortable way of requesting a certificate reflecting a higher level of trust than simple Class 1 certificates, which only require checking the e-mail address.

3.4 Class 3 certificates

Class 3 certificates are issued for both business and private (individual) use. For individuals, a Class 3 certificate includes a check of the subscriber's e-mail address (if present in the certificate), just like a Class 1 certificate. For organizations, a Class 3 certificate is based on Class 2, except that an authenticated company memorandum is required instead of a copy, witnessed by the appropriate chamber of commerce, register of companies or an authorized notary. The memorandum must not be older than 15 days.

In addition, Class 3 requires that the person named in the certificate completes a personal identification procedure as described in the section "Personal identification". For business certificates not bearing the name of any natural person – for example, SSL certificates for a Web server –, this applies to a person that is authorized to sign and named in the company memorandum, i. e. a managing director or a company secretary.

Class 3 certificates state, in addition to the checks required by Class 1 (private use) or Class 2 (business use), respectively, that

1. a natural person responsible for the certificate has been identified on the basis of his official identity card or passport.



2. personal data contained in the certificate matches with that in the identity card or passport.

Class 3 certificates establish a level of trust that meets high standards for both private and commercial needs. Any organizational data contained in a certificate is confirmed on the basis of the company memorandum (or similar documents) or documents signed by authorized employees. The certificate holder's identity, i. e. the natural person named in or responsible for the certificate, is identified on the basis of his official identity card or passport.

Class 3 certificates are primarily intended for e-commerce applications, such as electronic banking and online shopping, where a personal identification is required or preferred.

TC TrustCenter also issues certificates specifically designed for commercial software publishers (MS Authenticode, Netscape Object Signing), both individual and organizational. Please note that TC TrustCenter does not certify the program itself and does not grant its harmlessness, faultlessness, or fitness for a particular purpose. TC TrustCenter simply provides the manufacturer with a means of preventing malicious program modifications, or at least enabling their customers to recognize such alterations.

3.5 Class 4 certificates

Class 4 certificates are issued to private subscribers only. Class 4 certificates comprise the same verification procedures as Class 3 certificates, the only difference being that the personal identification of the subscriber is done at a government authority, the registration office, and personal data contained in his certificate is compared with his register entry.

Class 4 certificates establish the highest level of trust for private communication. Assuming a false identity by means of a faked passport is prevented.



4 Personal identification

If a certificate class requires personal identification of the subscriber (as is the case with Class 3 and 4), then this can either be accomplished at a German post office – the so-called Post Ident procedure – or at a TC TrustCenter Ident Point[®]. TC TrustCenter himself acts as an Ident Point[®], and personal identification may take place at TC TrustCenter's office as well. Personal identification for Class 4 certificates must be done at a registration office, but the other steps from certificate application to certificate issuance remain the same.

Prior to personal identification, a subscriber must submit his certificate application by means of the online application form on TC TrustCenter's Web site. Once the application form is completed, an e-mail is sent to the e-mail address given in the certificate request (if applicable). It contains a number ("e-mail number") that is required for the personal identification.

Please refer to the section „Naming conventions“ for information on how to choose a proper certificate name prior to generating a certificate request using PGP, your server software, internet browser or similar security software.

4.1 Post Ident

Personal identification by Post Ident may be done at any German post office.

Usually one or two workdays after submitting the application form to TC TrustCenter, the subscriber will receive the documents required for personal identification. These include, apart from the covering letter, detailed explanations on the identification procedure, a sheet stating the subscriber's obligations to take good care and to cooperate, a confirmation of application, a coupon for the Post Ident procedure, and two envelopes, one of them white, the other blue.

The number that was sent by e-mail must be written down on the confirmation of application sheet, which must then be signed by the subscriber. The signed confirmation and a photocopy of the subscriber's identity card or passport (both sides) must be put in the blue envelope, which should then be sealed. The subscriber must take the sealed blue envelope, the white envelope, the coupon and his identity card or passport with him when going to the post office. The post office employee will carry out the identification procedure, put all required documents (including the blue envelope) in the white stamped envelope and forward the latter to TC TrustCenter.

Once the documents arrive at TC TrustCenter, their content is checked. If they are verified successfully, the certificate is issued, usually within a workday. The subscriber will be informed of the issuance of his certificate by e-mail, which contains instructions on its installation and use.

4.2 TC TrustCenter Ident Points[®]

Personal identification at a TC TrustCenter Ident Point[®] is quicker and less complicated than the Post Ident procedure.

The advantage of TC TrustCenter Ident Points[®] over post offices is that it does not require sending the Post Ident documents first to the subscriber, and then back to TC TrustCenter. Once the subscriber has received his e-mail number, he can write it down, along with the application number, take both numbers and his identity card or passport, go to the Ident Point[®], and have himself identified by the Ident Point[®] employee. This is done online, and as

TC TrustCenter Certificate Policy Definitions

Version of September 1st, 1999



soon as the personal identification is completed, the subscriber's certificate will be issued the next time TC TrustCenter issues certificates, which usually takes a workday at most.

The subscriber must state e-mail number and application number at the TC TrustCenter Ident Point[®] in order to initiate the personal identification procedure. The Ident Point[®] employee will enter the subscriber's personal data as represented on his identity card or passport. This data is sent to TC TrustCenter, checked for consistency and, upon successful verification, the certificate is issued. The subscriber has to sign a confirmation of application, and a photocopy of his identity card or passport will be made, which is used by TC TrustCenter to verify the information represented in the subscriber's certificate. In case of inconsistencies or false representations with regard to the certificate application, TC TrustCenter reserves the right to revoke the certificate. If a certificate is revoked, the subscriber will be notified of this fact, and has the opportunity to correct the errors indicated by TC TrustCenter and submit a new certificate application.



5 Naming conventions

TC TrustCenter issues certificates in accordance with both the PGP and the X.509 standard. PGP certificates are used for secure e-mail communication and encryption of files. X.509 certificates are used by Web servers to ensure secure internet communication (e. g., submission of sensitive customer data), and by many popular Web browsers to implement client authentication (for example, access control to a Web server) and secure e-mail based on the S/MIME standard. The S/MIME standard is supported by other e-mail applications as well, such as MS Outlook 98.

This section provides guidelines on choosing a proper PGP user ID and on entering the appropriate information in the data fields that make up X.509 certificates

5.1 X.509 certificates

X.509 certificate requests 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	Email

C (Country): This field contains the two-letter ISO code for the respective country. If the certificate request is generated using an internet browser, the country can be selected during the application procedure, and the corresponding ISO code is inserted automatically. When generating server certificate requests, however, which is done offline using the server software (MS Internet Information Server, Netscape Enterprise Server, Apache, ...), 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 US state, if applicable. For other countries where similar structures exist (federal states, provinces etc.), the corresponding information 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 headquarters according to the company memorandum (commercial certificates) or the subscriber's place of residence according to the identity card or passport (private certificates).

O (Organization): If the certificate is used for commercial purposes, the company's or organization's name should be entered in this field. We recommend specifying the name as registered, for example with the local chamber of commerce, so that "Computer Service, Inc." is to be preferred instead of "Computer Service" "CS Inc."

For code signing certificate requests by individuals (freelance software developers etc.), TC TrustCenter will assign "Individual Software Publisher" to this entry automatically.

TC TrustCenter Certificate Policy Definitions

Version of September 1st, 1999



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 assign "MS Authenticode" or "Netscape Object Signing" to this entry automatically, depending on the internet browser being used by the subscriber.

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. Any academic title should be precede the first name, and it may only be specified if present on the identity card or passport.

Server certificate requests are an exception to this rule: Here, the common name field must contain the full domain name of the Web server, for example `www.trustcenter.de`.

Similar provisions apply for organization certificates, where no natural person should appear in the certificate. In this case, it is recommended to repeat the organization's name in the common name field.

For code signing certificate requests by organizations, the input from the organization field is automatically copied to the common name field, because the latter will usually be displayed when a user verifies signed software.

Email: This field is must contain a valid e-mail address (if provided). 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`.

The collection of the seven data fields listed above is commonly referred to as the Distinguished Name (DN). The same DN must not be assigned to different entities, while the same entity may have several certificates all bearing the same DN.

5.2 PGP certificates

Starting with version 6.5, PGP supports X.509 certificates for PGP keys as well. TC TrustCenter does not provide a certification service for this type of PGP key at the time of releasing these Certificate Policy Definitions. Therefore, we subsequently refer to PGP's own proprietary key format only. Please send e-mail to info@trustcenter.de in case you'd like to use X.509 certificates in conjunction with PGP 6.5 and above.

PGP's key format does not provide for data fields in certificates like X.509 does. PGP version 5.0 and above merely ask 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:

```
John Doe <jd@provider.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>
```

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

TC TrustCenter Certificate Policy Definitions

Version of September 1st, 1999



John Doe, Computer Company Ltd. <jd@cc.com>

or alternatively (more detailed but less clear)

John Doe, Computer Company Ltd., Marketing, Hamburg, DE <jd@cc.com>

In addition, a user ID like the following is also possible:

Computer Company Ltd. Marketing <marketing@cc.com>

This attributes a certificate to a group of people. There must be one person (known to TC TrustCenter) responsible for usage of the corresponding private key nonetheless.

5.3 Examples for X.509 Distinguished Names

	C	SP	L	O	OU	CN	EMAIL
Non-commercial	DE		Hamburg			John Doe	jd@provider.com
Commercial	DE		Berlin	Computer Company, Inc.	Marketing	John Doe	jd@cc.com
Organization	US	WA	Seattle	Computer Company, Inc.	Marketing		info@cc.com
Server	DE		Hamburg	Computer Company, Inc.	Internet Services	www.cc.com	webmaster@cc.com
Code Signing	DE		Hamburg	Computer Company, Inc.	MS Authenticode	Computer Company, Inc.	info@cc.com
Code Signing Individual	DE		Hamburg	Individual Software Publisher	Netscape Object Signing	John Doe	jd@provider.com

5.4 Examples for PGP User IDs

Non-commercial	John Doe, London <jd@provider.com> John M. Doe <jd@provider.com>
Commercial	John Doe, Computer Company Ltd., London <jd@cc.com>
Organization	Computer Company Ltd., Organization Key <info@cc.com> The Online Shopper, Hamburg, DE <sales@onlineshop.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 non-commercial	No check	No check	No check	Empty	Empty	No check	Access test
Class 2 non-commercial	Passport	No check	Passport	Empty	Empty	Passport	Access test
Class 2 commercial	Company Memo (copy)	LOC	Company Memo (copy)	Company Memo (copy)	LOC	LOC, Company Memo (copy), InterNIC	Access test
Class 3 non-commercial	Ident Point	No check	Ident Point	Empty	Empty	Ident Point	Access test
Class 3 commercial	Company Memo (authenticated)	LOC	Company Memo (authenticated)	Company Memo (authenticated)	LOC	Ident Point + LOC, Company Memo (authenticated), InterNIC	Access test
Class 4 non-commercial	Ident Point + Registration Office	No check	Ident Point + Registration Office	Empty	Empty	Ident Point + Registration Office	Access test

No check: TC TrustCenter does not verify the contents of this data field at all. This is mostly true for the SP field (State or Province), which is optional. TC TrustCenter recommends to leave this field blank, unless the subscriber is located in the USA. Any information listed in a data field labeled “No check” must be considered non-verified!

Empty: This field must be empty. This concerns specifying business data in the O and OU fields for non-commercial certificates, which is not allowed.

Access test: In order to verify the validity of an e-mail address and the subscriber’s access to this address, TC TrustCenter’s sends an e-mail to the address contained in the certificate request. This e-mail includes information that must be sent back to TC TrustCenter for the access test to complete successfully.

Company Memo: Information in this field is compared to the company’s memorandum (provided either as photocopy or authenticated) that is required for registration with the local chamber of commerce, or similar documents.

LOC (letter of confirmation): Data entered in this field must be confirmed in writing by a member of the organization named in the certificate who is authorized to sign. This should be done in conjunction with placing an order at TC TrustCenter, naming the employees who shall obtain a certificate, and, if applicable, the department they work for.

Passport: Data contained in the appropriate fields is compared to the photocopy of the subscriber’s identity card or passport that is sent to TC TrustCenter. Personal identification, however, is not required.

Ident Point: Data contained in the appropriate fields is compared to the photocopy of the subscriber’s identity card or passport that is sent to TC TrustCenter as part of the personal

TC TrustCenter Certificate Policy Definitions

Version of September 1st, 1999



identification procedure. Please see the section “Personal identification” for details concerning this procedure.

Registration office: Data is compared to the copy of the subscriber’s register entry at the registration office that is sent to TrustCenter as part of the personal identification procedure.

InterNIC: For server certificates, it is verified that the domain name given in the CN field is registered to the organization named in the certificate by using services like the InterNIC database. If O contained “TC TrustCenter” and CN was “`www.trustcenter.de`”, it would be checked that “`trustcenter.de`” was registered to TC TrustCenter.



7 Certificate Revocation

A certificate must be revoked in case:

1. The corresponding private key has been lost or compromised.
2. Certificate data has become incorrect (e. g. because of a change of one's e-mail address).

Revocation can be done in several ways:

1. If the subscriber still has access to his private key, he may use the [revocation request form](#) that is available on TC TrustCenter's Web site. He must use his certificate to authenticate himself.
2. If the subscriber has lost or is unable to access his private key for any reason, he can call TC TrustCenter and authenticate himself by naming the revocation password chosen during the certificate application.
3. The subscriber can request revocation by writing a letter to TC TrustCenter. Authentication is achieved by the subscriber's signature.
4. Any third party that confirmed data contained in certificate must inform TC TrustCenter in writing as soon as the confirmed information has become invalid. Once TC TrustCenter has been informed of this fact, it will revoke the certificate promptly.

TC TrustCenter notifies the subscriber via digitally signed e-mail upon carrying out the certificate revocation.