



GeoTrust

Certificate Policy
for
CodeSigning Certificates
(Authenticode and Java)

Policy OID = 1.3.6.1.4.1.14370.1.4

Version of February 14th, 2006

1	INTRODUCTION	3
2	IMPORTANT NOTES	5
3	CERTIFICATE CLASSES	6
3.1	CLASS 0 CERTIFICATES.....	6
3.2	CLASS 1 CERTIFICATES.....	6
3.3	CLASS 2 CERTIFICATES.....	7
	<i>Verification of statements about natural persons</i>	7
	<i>Verification of statements about organizations</i>	7
	<i>Verification of statements about the relationship of a natural person to an organization</i>	7
3.4	CLASS 3 CERTIFICATES.....	7
	<i>Verification of statements about natural persons</i>	7
	<i>Verification of statements regarding the relationship of natural person to organizations</i>	7
4	CLASS 2 CODESIGNING CERTIFICATES	8
4.1	IDENTIFICATION OF NATURAL PERSONS.....	8
4.2	VERIFICATION OF STATEMENTS ABOUT ORGANIZATIONS	8
4.3	VERIFICATION OF STATEMENTS ABOUT THE RELATIONSHIP OF A NATURAL PERSON TO AN ORGANIZATION	9
4.4	VERIFICATION OF E-MAIL ADDRESSES	9
5	NAMING CONVENTIONS	10
5.1	CHARACTER SET AND RULES FOR CONVERSION	10
	<i>5.1.1 Conversion of Characters</i>	10
5.2	X.509 CERTIFICATES	11
6	VERIFICATION OF CERTIFICATE INFORMATION	13
7	CERTIFICATE REVOCATION	15

1 Introduction

This document is GeoTrust's and TC TrustCenter's Certificate Policy for CodeSigning Certificates. The purpose of this document is to allow an estimation of the trustworthiness of the certificates issued by GeoTrust and TC TrustCenter.

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

CodeSigning Certificates are usually issued to organizations. The organization uses the CodeSigning certificate to sign programming code, thus proving the authenticity and integrity of this code to third parties.

It has to be taken into account that GeoTrust and TC TrustCenter do 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 identify the origin of the software and to detect manipulations of the software distributed by the manufacturer.

Each certificate is only as trustworthy as the procedures followed for its issuance. For this reason, many certification service providers (Certification Authorities, CAs) group 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.

This Certificate Policy describes the processes used by GeoTrust and TC TrustCenter as a Certification Authority when identifying a certificate holder. This document explains the classification of certificates in the certificate classes for applicants, certificate holders as well as for third parties. This enables a decision as to whether the presented certificate is sufficient for the application in question. 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".

Parallel with the description of the classification of certificates into classes (Section 3), 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) are 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 113) 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.

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

Contact information:

TC TrustCenter AG
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 is 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 GeoTrust or 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 GeoTrust, 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: All CodeSigning certificates issued by GeoTrust and TC TrustCenter are issued based on the Certificate Policy being valid at the time of the issuance of the certificate. Later modification of the Certificate Policy has no influence on already issued certificates.

No verification of creditworthiness: GeoTrust and TC TrustCenter confirm 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 and reliability of the entity itself.

No verification of harmlessness of software: GeoTrust and TC TrustCenter issue CodeSigning certificates for organizations. These certificates can then be used to sign software. GeoTrust and TC TrustCenter do not certify the programming code itself, its harmlessness, its algorithmical correctness, or its applicability. CodeSigning certificates are intended to enable the user to detect manipulations of the software distributed by the manufacturer. Furthermore, the origin of the software can be deduced by such certificates.

No assurance of up-to-date certificate data: GeoTrust and TC TrustCenter verify the information contained in a certificate request only within the scope and during registration at the time of issuance of a certificate. GeoTrust and TC TrustCenter accordingly do not provide any assurance that this data is up-to-date after registration. When renewing a certificate, the data contained therein will not necessarily 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: GeoTrust and TC TrustCenter issue CodeSigning certificates under this policy. Any participant of the certification service must decide for itself whether a given CodeSigning certificate meets the security needs for the application in question.

Participant's obligation to inform itself: It is essential for any end user participating in the 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.

GeoTrust and TC TrustCenter reserve its right to revoke certificates: If cryptographic algorithms or associated parameters become unsafe due to technical progress or new developments in cryptology, GeoTrust and TC TrustCenter reserve the right to revoke certificates based on such algorithms and parameters. Certificates may also be revoked if the certificate owner provided false information, or if GeoTrust or TC TrustCenter has obtained knowledge that data in the certificate no longer complies with the facts.

3 Certificate classes

The trustworthiness of certificates depends on the procedures used for their issuance. Every certificate issued by GeoTrust and TC TrustCenter belongs to a defined “Level of Trust” class. The class of a certificate describes the general measures taken by GeoTrust and 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 applicant’s identity.

All CodeSigning certificates issued under this Certificate Policy are Class 2 certificates.

The security of the encryption, and consequently, the level of protection against unauthorized access to the transmitted data and/or falsification of signed 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. The verification measures being taken for each certificate class are described below.

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

In addition to the verifications confirming the certificate’s content, GeoTrust and TC TrustCenter perform additional checks for certificates issued to 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 GeoTrust or TC TrustCenter by mail, e-mail, or by fax. Alternatively GeoTrust and TC TrustCenter may verify the authorization to apply for a certificate by phone.

3.1 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!

3.2 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 for the existence and the accessibility of the e-mail address, no data contained in the certificate is being checked.

3.3 Class 2 certificates

Verification of statements about natural persons

Statements made in a Class 2 certificate regarding natural persons require the presentation of a copy of an official photo ID document with signature or the confirmation of an accredited third party regarding the correctness and the completeness of the data

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.

Verification of statements about organizations

Statements made in Class 2 certificates about organizations are verified by 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).

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

3.4 Class 3 certificates

Verification of statements about natural persons

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. Only official ID documents that contain a photo and a handwritten signature of the ID holder are accepted for verification purposes.

Verification of statements regarding organizations

In the case of an organization that could reasonably be expected to be registered with a local, state or national authority, it is necessary to present copies of the registration documents. The documents presented should be up to date and notarized or be original.

Alternatively the validity of the registration may be verified through a reputable third party database.

Additional data in the certificate are verified as far as possible. For example it may be checked if a domain name in the certificate is registered to the organization applying for the certificate.

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.

4 Class 2 CodeSigning Certificates

In general, a CodeSigning certificate is issued to an organization or a part of an organization; it is not issued to a single person.

It is formally assigned to a single person (the certificate holder, e.g. a developer), who is then responsible for the proper use of the CodeSigning certificate. This person must be identified in compliance with the rules for Class 2 certificates (or higher) of these Certificate Policy.

The CodeSigning certificate may be installed by the certificate holder on a limited number of systems.

4.1 Identification of natural persons

Persons responsible for a certificate must prove their identity either by

- a) confirmation of an accredited third party regarding the correctness and the completeness of the data

or by

- b) confirmation of the information by presentation of a copy of an official photo ID document with signature.

4.2 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. In the case of an organization that could reasonably be expected to be registered with a local, state or national authority, it is necessary to present copies of the registration documents.

Alternatively the validity of the registration may be verified through a reputable third party database.

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

Documents, 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 GeoTrust or TC TrustCenter are already in possession of such documents they 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 fulfills at least the requirements of a TC Class 2 certificate.

Documents older than 36 months are not accepted.

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. Alternatively the validity of the registration may be verified through a reputable third party database.

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

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. Furthermore it has to be confirmed that the applicant is authorized to apply for a CodeSigning certificate.

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 e-mail. The certificate used for the digital signature must fulfill at least the requirements of a TC TrustCenter Class 2 certificate.

Alternatively the affiliation of a person named in a certificate to an organization may be verified by phone. In this case GeoTrust or TC TrustCenter initiates a procedure to get in contact with the organization.

4.4 Verification of e-mail addresses

If the certificate contains an e-mail address, its correctness is verified by an access test. A random number is sent to the e-mail address. This number has to be sent back to GeoTrust's or TC TrustCenter's Registration Authority. Alternatively, as CodeSigning certificates are issued for organizations only, a responsible person in that organization may confirm the correctness of the e-mail address; an access test is then optional.

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, GeoTrust and 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.

5 Naming conventions

GeoTrust and TC TrustCenter CodeSigning certificates are issued in accordance with the X.509 standard. X.509 certificates are, among others, 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 for encryption and signing standard S/MIME, supported by many browsers and popular e-mail applications.

This section provides guidelines on entering the appropriate information in the data fields that make up X.509 certificates.

In certain projects and after consultation with GeoTrust or 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, this Certificate Policy requires 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.

GeoTrust and TC TrustCenter recommend adherence to the following conversion rules. Otherwise the proper functionality/functioning of the certificates in connection with other components can not be assured. For example it can not be excluded that some components, 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

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

Examples:

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	Converted
Smith & Meier Ltd.	Smith and Meier Ltd.
Smith & Meier Ltd.	Smith a. Meier Ltd.
Smith & Meier Ltd.	Smith + Meier Ltd.

5.2 X.509 certificates

X.509 certificates usually consist of the data fields mentioned in the following table. 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.

SP (State/Province): This field is intended to provide the state.

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 letterhead. It is recommended to state the organization with its full name and its legal form, e.g. "GeoTrust Inc." instead of "GeoTrust" or "GT Inc."

OU (Organizational Unit): This field may be used to specify the department within the organization that the certificate is attributed to.

In a second OU-field GeoTrust and TC TrustCenter will automatically enter the value "CodeSigning".

CN (Common Name): The CN field is usually used to specify the name of the natural person the certificate is attributed to. As CodeSigning certificates are issued to organizations (as described above) 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.

E-mail: This field must contain a valid e-mail address, if filled.

The collection of the data fields listed above is commonly referred to as the Distinguished Name (DN). See the following example for construction of a DN (in this example the SP-field is left empty):

```
/C=DE/L=Hamburg/OU=Microsoft Authenticode/O=Stonehillbaker Deutschland GmbH/CN=Stonehillbaker Deutschland GmbH/Email=info@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	OU	CN	EMAIL
DE	Hamburg	Hamburg	Stonehillbaker Deutschland GmbH	CodeSigning	Development	Stonehillbaker Deutschland GmbH	john.freeman@stonehillbaker.com
DE		Hamburg	Stonehillbaker Deutschland GmbH		Development	Stonehillbaker Deutschland GmbH	webmaster@stonehillbaker.com
DE		Hamburg	Stonehillbaker Deutschland GmbH	CodeSigning		Stonehillbaker Deutschland GmbH	info@stonehillbaker.com

6 Verification of certificate information

GeoTrust and TC TrustCenter verify the contents of the X.509 CodeSigning certificate data fields as specified in the following table. The entries used in the table are described below.

C	SP	L	O	OU	CN	Email
RegA or ADB or CDB	RegA or ADB or CDB	RegA or ADB or CDB	RegA or ADB or CDB	Automatically filled, written confirmation	Ident , written confirmation, or confirmation by phone	Access test or written confirmation
RegA or ADB or CDB	RegA or ADB or CDB	RegA or ADB or CDB	RegA or ADB or CDB	Automatically filled, written confirmation	Written confirmation	Access test or written confirmation

Table 1

Access test: If the certificate contains an e-mail address, this e-mail address will be checked. In order to verify the validity of an e-mail address and the subscriber's access to this address, an e-mail is sent to the address contained in the certificate request. This e-mail includes information that must be sent back to GeoTrust or TC TrustCenter for the identification of the applicant to be completed. 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.

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 in fact exists . 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 GeoTrust or TC TrustCenter directly or on behalf of GeoTrust or 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 employee who shall obtain a certificate and the department they work for and, if applicable also the e-mail address. 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 accuracy of this data must be confirmed by an authorized person of the organization. GeoTrust or TC TrustCenter (or one of their authorized representatives) 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 GeoTrust or TC TrustCenter in the process of the identification.

7 Certificate Revocation

1. A certificate has to be revoked by the certificate holder (in writing, via telephone or via the website of GeoTrust or 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 an organization's legal status).
2. If cryptographic algorithms or parameters become insecure because of technological progress or new developments in cryptography GeoTrust and TC TrustCenter reserve the right to revoke certificates that are issued using these algorithms or parameters.
3. Certificates may be revoked by GeoTrust and TC TrustCenter if the applicant provided false data, or if GeoTrust or TC TrustCenter gain knowledge that data contained in a certificate has become invalid.
4. If the private key of a certificate is compromised GeoTrust and TC TrustCenter may revoke the certificate in order to prevent misuse of the compromised key.
5. In the event that GeoTrust and TC TrustCenter cease operations, all CodeSigning certificates issued shall be revoked prior to the date that GeoTrust and TC TrustCenter cease operations.
6. GeoTrust and TC TrustCenter confirm the revocation of a certificate by a signed e-mail.

* * *