

Certification Practice Statement Version 1.0

Replaced by Version 2.0

Warranty

thawte hereby warrants that it takes reasonable steps to verify that the information contained in any *thawte* certificate is accurate at the time of issue. Thawte also warrants that certificates are revoked if thawte believes that the contents of a certificate are no longer accurate, or that the key associated with a certificate has been compromised in any way. The nature of the steps Thawte takes to verify the information contained in a certificate vary according to the certification fees charged, the nature and identity of the certificate subscriber, and the applications for which the certificate will be marked as trusted. Sample verification practices are given in a separate document, "Sample Verification Practices". Thawte makes no other warranties.

Liability

Thawte hereby accepts direct and consequential liability for any negligence in the performance of its verification practices. Thawte hereby disclaims liability for the acts of third parties, certificate subscribers and other non-Thawte entities.

Privacy

The contents of certificates issued by Thawte are public information. Thawte hereby guarantees that it will not divulge any additional subscriber information to any third party for any reason, unless requested by a court of law having jurisdiction over that specific information.

Force Majeure

Thawte accepts no liability for any breach of warranty, delay, or failure in performance under this CPS that results from events beyond its control such as acts of God, acts of war, acts of terrorism, epidemics, power outages, fire, earthquakes, year 2000 related failures of third parties, and other natural or manmade disasters.

Certificate revocation

Thawte shall revoke or suspend certificates at its sole discretion, and shall publish the list of revoked certificates in a publicly accessible Certificate Revocation List.

Record Keeping

Thawte shall keep records material to the issue of certificates for a minimum of 5 years.

Certificate Content

A Thawte certificate purports to certify only the information contained therein. A relying party shall make no assumptions about information that does not appear in a certificate.

Subscriber Information

A subscriber is solely responsible for the protection of its private keys. Subscribers shall notify Thawte immediately if they believe a private key has or may have been compromised in any way. Subscribers shall be liable to Thawte and third parties for any misrepresentations they make to Thawte, as well as for direct and indirect consequences of those misrepresentations. Applicants for and subscribers to Thawte's certification services acknowledge that they have been advised to obtain proper training in the use of a public key infrastructure prior to requesting or relying upon a certificate.

Relying Parties

It is unreasonable for any party to rely on a digital certificate issued by Thawte if that party has actual or constructive notice of the compromise of the certificate or its associated private key. Such notice includes, but is not limited to the contents of the certificate and information incorporated in the certificate by reference, as well as the contents of this CPS and the current set of revoked certificates published by Thawte.

Governing Law

In order to ensure uniform procedures and interpretation for all users, irrespective of their country of residence or nationality, the laws of the Republic of South Africa shall govern the enforceability, construction, interpretation and validity of this CPS.

Dispute Resolution Process

In the event of any dispute or claim arising from the issue of a Thawte certificate, the complainant undertakes to notify Thawte in writing by registered mail of the exact nature of the dispute. The complainant undertakes to allow Thawte a reasonable time to attempt to resolve the dispute before invoking any dispute resolution mechanism.

Should Thawte be unable to resolve the dispute, the parties to the dispute shall attempt to agree on a mutually acceptable forum and process for arbitration of the dispute, which arbitration shall be final and binding.

Should the parties to a dispute be unable to agree on a mutually acceptable forum and process for arbitration, the dispute shall be referred to the High Court of the Republic of South Africa, Western Cape Provincial Division. No other court shall have jurisdiction over disputes arising from certificates issued by Thawte.

Chained CA Certificate Practices and Liability

Thawte may delegate trust to other certificate authorities (CA's) through certificate chaining or cross-certification. Thawte requires that a cross-certified CA verify the content of a certificate with processes that are at least as conservative as those employed by Thawte. Thawte hereby agrees to be liable to third parties for certificates issued by Chained CA's in compliance with their CPS, as if Thawte in fact issued those certificates.