thawte
Certification Practice Statement

Version 3.3

Effective Date: November, 2006

thawte Certification Practice Statement

Revision date: 28/07/2006

Trademark Notices

Acknowledgement

thawte acknowledges the assistance of many reviewers of the document specializing in diverse areas of business, law, policy, and technology.

History of changes: Version 3.3 (Effective date November, 2006)

Section 1.1	Deleted: "***thawte's*** Certification Authorities (CAs) offer three distinct classes of end user subscriber certificates – High Assurance and Low As Certificates is the level of Subscriber identification and authentication performed (*See* CPS §§ 3.1.8, 3.1.9). In addition, specific types of certifica (*See* CPS §1.3.4) and certificate profiles (*See* CPS §7.1)." Added: "***thawte's*** Certification Authorities (CAs) offer four distinct classes of end user subscriber certificates – High Assurance with extended v Low Assurance. The distinction between these classes of Certificates is the level of Subscriber identification and authentication performed (*See* certificates within these classes have specific intended uses (*See* CPS §1.3.4) and certificate profiles (*See* CPS §7.1). ***thawte*** High Assurance with extended validation Certificates are certificates issued by ***thawte*** in conformance with the Guidelines for Extended consisting of major certification authorities and browser vendors."
Section 1.1. Table 1	Added: new Product, "High Assurance with extended validation secure SSL certificates issued by thawte in conformance with the Guidelines for Ex encryption used to support SSL sessions between web browsers and servers."
Section 1.1. Table 1	Added New product: "High Assurance with extended validation Premium Server Gated Cryptography SSL certificates issued by thawte in conforma
Section 1.3.1 Table 3	Added: thawte Primary Root CA Added: thawte Extended Validation SSL CA
Section 1.3.3 table 5	Added "High assurance with extended validation…Incorporated Organizations (including Government agencies, Educational Institutions, Governme qualify for EV Certificates are more fully described in Appendix A1 of this CPS."
Section 1.3.4	Added: "High Assurance with extended validation"
Section 2.2.1.3	Added: "thawte's limitation of liability for EV certificates is further described in Section 37 of Appendix A1 to this CPS"
Section 3.1.1.1	Added:" EV SSL certificate content and profile requirements are discussed in Section 6 of Appendix A3 to this CPS"
Section 3.1.1.7	1.1.1.1 Added: "SSL Web Server Certificates with EV "SSL Web Server Certificates with EV distinguished name attributes are discussed in Section 6 of Appendix A3 to this CPS."
Section 3.1.8.1 - Table 14	"SSL Web Server Certificates with EV… ***thawte***'s procedures for issuing Extended Validation SSL Certificates are described in Appendix A1 to thi
Section 4.1.1 – Table 19	Added: "High Assurance with extended validation – SSL Web Server Certificates with EV"
Section 4.4.9 – Table 20	Added "thawte Primary Root CA"; "thawte Extended Validation SSL CA"
Section 6.2.2 –	Deleted "Table 21 below shows the threshold number of shared required for the different types of ***thawte*** CAs. It should be noted that the number o less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Deleted Table 21 Added: "The threshold number of shares needed to sign a CA certificate is 3. It should be noted that the number of shares distributed for disaster rec distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with th
Section 6.2.7.1.2	*Added "and High Assurance with extended validation Certificates"*
Section 7.1.1	Added***: "SSL Web Server Certificates with EV standard certificate profiles are discussed in Section 6 of Appendix A3 to this CPS.""***
Section 7.1.2.7	Added new Section
Section 9	Added Definitions for Extended Validation
APPENDIX A	Added Appendix A1-A3 for Extended Validation Certificate procedures

History of changes: Version 2.3 (Effective date July 28, 2006)

Section 1.1	Deleted: ***thawte*** Medium Assurance SSL123 Certificates are issued to Domains to provide confidentiality encryption. ***thawte*** validates that the person enrolling for the certificate has control of the domain by requiring the person to respond to an e-mail hosted at that domain. No organization authentication is performed on the owner of the domain. ***thawte*** Medium Assurance. SSL123 provide confidentiality encryption for internal Intranets. ***thawte*** validates that the Server, Intranet name or IP are not publicly accessible via the World Wide Web. Added: ***thawte*** Medium Assurance SSL123 Certificates are issued to Domains to provide confidentiality encryption. ***thawte*** validates that the person enrolling for the certificate has control of the domain by requiring the person to respond to an e-mail hosted at that domain. No organization authentication is performed on the owner of the domain.
Section 1.1	Deleted: By utilizing **thawte's** SSL Web Server Certificate you are sending a clear signal to your customers. They know that the information they submit will not be intercepted while in transit, and that you are a verified, real-world organization. Added: High Assurance secure SSL certificates with stringent 3 step authentication capable of 256-bit encryption used to support

	SSL sessions between web browsers and servers.
Section 1.1	Deleted: Secure SSL certificates with full authentication capable of 256-bit encryption that secure multiple hosts on a single domain on the same server. Added: Secure SSL certificates with stringent 3 step authentication capable of 256-bit encryption that secure multiple hosts on a single domain on the same server.
Section 1.1	Deleted: Premium Server Gated Cryptography SSL certificates with stringent 3 step authentication, automatic 128-bit step-up encryption and capable of 256-bit encryption.* By unleashing the full protection of your SSL-enabled server, a SGC SuperCert from **thawte** will allow you to extend 128-bit encryption to clients that use older browsers with 40-bit or 56-bit encryption capabilities. Added: High Assurance Premium Server Gated Cryptography SSL certificates with stringent 3 step authentication, automatic 128-bit step-up encryption and capable of 256-bit encryption * used to support SSL sessions between web browsers and web servers. • Compatible with browsers IE 4.X or Netscape 4.06 and later
Section 1.1	Deleted: Domain validated SSL certificates capable of 256-bit encryption and issued within minutes ** ** Please note that delays in issuance can be caused if the domain is not registered with an accredited online registrar. A **thawte** SSL123 Certificate provides validation of a registered domain and **thawte** validates that the person enrolling for the certificate has control of the domain by requiring the person to answer an e-mail sent to the e-mail address listed or predetermined for that domain. SSL123 for Intranets provide validation that the Server, Intranet name or IP are not publicly accessible via the World Wide Web. Added: Medium Assurance domain validated SSL certificates capable of 256-bit encryption used to support SSL sessions between web browsers and servers.
Section 1.1	Deleted: **thawte's** Reseller Partner Program permits entities acting as a host ("Web Host") to the web sites of their clients to manage lifecycle processes for server and code signing Certificates on behalf of their clients. The ISP Program offers Resellers (e.g. Web Hosting companies, ISPs, Registrars) the ability to enroll for SSL Web Server,SSL Wildcard, SSL123, SGC SuperCerts and Code Signing Certificates on behalf of their customers . Although the Reseller assists with the enrollment process (See CPS § 4.1.1), the Reseller does not perform validation functions, but instead **thawte** performs these validation functions. Also, it is the Resellers' customers that obtain SSL Web Server, SSL Wildcard, SSL123, SGC SuperCerts and Code Signing Certificates as the actual Subscribers and are ultimately responsible for Subscriber obligations under the appropriate Subscriber Agreement. Resellers have an obligation to provide the applicable Subscriber Agreements to their clients to inform them of their obligations. Added: **thawte's** Reseller Partner Program offers Resellers (e.g. Web Hosting companies, ISPs, Registrars) the ability to enroll for SSL Web Server,SSL Wildcard, SSL123, SGC SuperCerts and Code Signing Certificates on behalf of their customers . Although the Reseller assists with the enrollment process (See CPS § 4.1.1), the Reseller does not perform validation functions, but instead **thawte** performs these validation functions. Also, it is the Resellers' customers that obtain SSL Web Server, SSL Wildcard, SSL123, SGC SuperCerts and Code Signing Certificates as the actual Subscribers and are ultimately responsible for Subscriber obligations under the appropriate Subscriber Agreement. Resellers have an obligation to provide the applicable Subscriber Agreements to their clients to inform them of their obligations.
Section 1.1	Deleted: **thawte** performs the RA function for all high assurance certificates, and for low assurance "Freemail" certificates, which do not include the subscriber's name. Added: **thawte** performs the RA function for all high assurance certificates, medium assurance certificates and for low assurance "Freemail" certificates, which do not include the subscriber's name.
Section 1.3.4.	Deleted: This CPS applies to all **thawte** PKI Participants, including **thawte**, Customers, Resellers, Subscribers, and Relying Parties. This CPS describes the practices governing the use of High Assurance, and Low Assurance Certificates within the **thawte** PKI. Each type of Certificate is generally appropriate for use with the applications set forth in CPS §§ 1.3.4.1 and § 1.1 (Table 1). Added: This CPS applies to all **thawte** PKI Participants, including **thawte**, Customers, Referrers, Resellers, Subscribers, and Relying Parties. This CPS describes the practices governing the use of High Assurance, Medium Assurance and Low Assurance Certificates within the **thawte** PKI. Each type of Certificate is generally appropriate for use with the applications set forth in CPS §§ 1.3.4.1 and § 1.1 (Table 1).
Section 2.3.3	Deleted: **thawte**, Inc. is a wholly owned subsidiary of VeriSign, Inc. VeriSign's financial resources are set forth in disclosures appearing at:**http://corporate.verisign.com/investor/sec-filings.html**. VeriSign shall also maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. Added: **thawte**, Inc. is a wholly owned subsidiary of VeriSign, Inc. VeriSign's financial resources are set forth in disclosures appearing at: http://www.verisign.com/verisign-inc/vrsn-investors/sec-filings/index.html. VeriSign shall also maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.
Section	

2.5.6	Deleted: A Subscriber may make changes to the name included in a certificate within 30 days of issue. **thawte** authenticates the new domain in terms of Section 3.1.8.1. Added: A Subscriber may make changes to the host of the common name (i.e. Host Name) included in a certificate anytime within the lifespan of the certificate. **thawte** authenticates the new domain in terms of Section 3.1.8.1.
Section 3.1.1.2	Deleted: Server Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in Table 8 below. Added: Server Certificates (except SSL123 Certificates) contain an X.501 distinguished name in the Subject name field and consist of the components specified in Table 8 below.
Section 3.1.8.1	Deleted: Organization authentication is not for SSL123. Specified that confirmation with an appropriate Organizational contact is not done for SSL123 Certificates Added: Organization authentication is not performed for SSL123 Certificates. These certificates are authenticated as described in Table 14 below. Where a domain name or e-mail address is included in the certificate thawte authenticates the Organization's right to use that domain name. Confirmation of an organization's right to use a domain name is not performed for SSL123 Certificates. For these certificates, validation of domain control only is performed, as described in Table 14 below.
Section 3.1.9.2.3	Added: US Notary public (limited to Notary Publics in States where the licensing status information is provided online by the appropriate licensing authority)
Section: 3.2.1	Deleted: Subscriber Certificates, which have not been revoked, may be replaced (i.e., rekeyed or renewed) before the expiration date. Currently 1 year certificates may be renewed starting 90 days before expiration and 2 year certificates may be renewed starting 32 days before expiration. Added: Subscriber Certificates, which have not been revoked, may be replaced (i.e., rekeyed or renewed) before the expiration date. Currently 1 and 2 year certificates may be renewed starting 90 days before expiration. However, in the Reseller Partner Program, 1 year certificates may be renewed 90 days before expiration and 2 year certificates may be renewed starting 32 days before expiration.
Section 3.4:	Deleted: Prior to the revocation of a Certificate, **thawte** verifies that the revocation has been requested by the Certificate's Subscriber or the entity that approved the Certificate Application. The subscriber must contact **thawte** and request a Revocation Form. Upon receipt of the completed form (signed by either the Authorizing or Technical Contact), the certificate will be revoked. However, only the Authorizing Contact can sign a revocation form for SSL123 Certificates. Added: Prior to the revocation of a Certificate, **thawte** verifies that the revocation has been requested by the Certificate's Subscriber, the entity that approved the Certificate Application. Acceptable procedures for authenticating the revocation requests of a Subscriber include: • Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or the equivalent thereof), and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record • Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked, • Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service • However, only the Authorizing Contact can sign a revocation form for SSL123 Certificates.
Section 6.1.1. .	Deleted: Generation of end-user Subscriber key pairs is performed by the Subscriber, except in the case of customers of Web Hosts who participate in the ISP program. In such cases, the Reseller Partner may generate server key pairs on behalf of Subscribers as described in CPS §1.1. Added: Generation of end-user Subscriber key pairs is performed by the Subscriber, or authorized representative of the subscriber such as a Web hosting company
Section 7.1.1.	Deleted: md5RSA Added: md5RSA or sha1RSA: Certificate signatures produced using these algorithms shall comply with RFC 3279. Use of sha-1WithRSAEncryption shall be given strong preference over md5WithRSAEncryption.

<table>
<tr><td>Section:
7.1.2.3</td><td>Deleted: http://crl.thawte.com/ThawteServerCA.crl

Added: http://crl.thawte.com/ThawtePremiumServerCA.crl</td></tr>
<tr><td>Section
7.1.2.5.</td><td>Deleted: http://crl.thawte.com/ThawteServerCA.crl

Added: http://crl.thawte.com/ThawteSGCCA.crl

<table><tr><td>Authority information Access</td><td>http://ocsp.thawte.com</td><td>Non-Critical</td></tr></table></td></tr>
<tr><td>Section
7.1.2.6</td><td>Added: SSL Wildcard Certificates

thawte SSL Wildcard Certificates include the extensions specified in Table 26 below:

<table><tr><th>Extension</th><th>Value or Value Constraint</th><th>Criticality</th></tr><tr><td>Basic Constraints</td><td>Subject Type=End Entity
Path Length Constraint=None</td><td>Critical</td></tr><tr><td>Enhanced Key Usage</td><td>Server Authentication (1.3.6.1.5.5.7.3.1)
Client Authentication (1.3.6.1.5.5.7.3.2)</td><td>Non-Critical</td></tr><tr><td>CRL Distribution Points</td><td>http://crl.thawte.com/ThawtePremiumServerCA.crl</td><td>Non-Critical</td></tr><tr><td>Authority information Access</td><td>http://ocsp.thawte.com</td><td>Non-Critical</td></tr></table>
Table 26 –thawte SSL Web Server Certificate Extensions</td></tr>
<tr><td>Section:
7.1.3</td><td>Deleted: thawte Certificates are signed with md5RSA.

Added: thawte Certificates are signed with md5RSA or sha1RSA Certificate signatures produced using these algorithms shall comply with RFC 3279. Use of sha-1WithRSAEncryption shall be given strong preference over md5WithRSAEncryption.</td></tr>
<tr><td>Section:
7.2</td><td>Deleted: Algorithm used to sign the CRL. Thawte CRLs are signed using md5RSA (OID: 1.2.840.113549.1.1.4) in accordance with RFC 2459.

Added: Algorithm used to sign the CRL. Thawte CRLs are signed using md5RSA or sha1RSA (OID: 1.2.840.113549.1.1.4) in accordance with RFC 2459.</td></tr>
<tr><td>Section
9.2.</td><td>Deleted:

<table><tr><td>SGC SuperCerts</td><td>High Assurance Certificate used to support SSL sessions between web browsers and web servers that are encrypted using strong cryptographic protection consistent with applicable export laws.</td></tr></table>
Added:

<table><tr><td>SGC SuperCerts</td><td>High Assurance Premium Server Gated Cryptography SSL certificates with stringent 3 step authentication, automatic 128-bit step-up encryption and capable of 256-bit encryption * used to support SSL sessions between web browsers and web servers.
* With browsers IE 4.X or Netscape 4.06 and later</td></tr></table></td></tr>
<tr><td>Section
9.2.</td><td>Deleted:

<table><tr><td>SSL Web Server Certificates</td><td>An organizational Certificate used to support SSL sessions between web browsers and servers.</td></tr></table>
Added:
<table><tr><td>SSL Web Server Certificates</td><td>High Assurance secure SSL certificates with stringent 3 step authentication capable of 256-bit encryption used to support SSL sessions between web browsers and servers.</td></tr></table></td></tr>
<tr><td>Section
9.2.</td><td>Deleted:

<table><tr><td>High Assurance</td><td>Certificates issued to organizations and sole proprietors to provide authentication; message, software, and content integrity; and confidentiality encryption.</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td>Added:
<table><tr><td>High Assurance</td><td>Certificates issued to organizations and sole proprietors to provide stringent 3 step authentication; message, software, and content integrity; and confidentiality encryption.</td></tr></table></td></tr>
<tr><td>Section 9.2.</td><td>Deleted:
<table><tr><td>Reseller Partner Program</td><td>A program that allows to enroll for SSL Web Server Certificates, and SGC SuperCerts on behalf of end-user Subscribers who are customers of the Web Host.</td></tr></table>
Added:
<table><tr><td>ISP Partner Program</td><td>A program that allows Web Hosts to enroll for SSL Web Server Certificates, SSL Wildcard Certificates, SSL123 Certificates and SGC SuperCerts on behalf of end-user Subscribers who are customers of the Reseller.</td></tr></table></td></tr>
<tr><td>Section 9.2.</td><td>Added:
<table><tr><td>Code Signing Certificates</td><td>Certificates which secure delivery of code and content to browsers over the Internet.</td></tr></table></td></tr>
<tr><td>Section 9.2.</td><td>Added:
<table><tr><td>Medium Assurance</td><td>Certificates that are issued to Domains to provide
confidentiality encryption. thawte validates that the person enrolling for the certificate has control of the domain by requiring the person to respond to an e-mail hosted at that domain. No organization authentication is performed on the owner of the domain.</td></tr></table></td></tr>
<tr><td>Section 9.2.</td><td>Added:
<table><tr><td>SSL123 Certificates</td><td>Medium Assurance domain validated SSL certificates capable of 256-bit encryption and issued within minutes used to support SSL sessions between web browsers and servers.
Delays in issuance can be caused if the domain is not registered with an accredited online registrar.</td></tr></table></td></tr>
<tr><td>Section 9.2.</td><td>Added:
<table><tr><td>Wildcard Certificates</td><td>Secure SSL certificates with stringent 3 step authentication capable of 256-bit encryption that secure multiple hosts on a single domain on the same server.</td></tr></table></td></tr>
</table>

TABLE OF CONTENTS

1. Introduction

A Certification Practice Statement ("CPS") is defined by the Electronic Commerce and Information Technology Division of the American Bar Association as "a statement of the practices which a certification authority employs in issuing certificates." The ***thawte*** CPS explains the policies, practices, and procedures that govern the ***thawte*** public key infrastructure ("***thawte*** PKI").

Please Note: The capitalized terms in this CPS are defined terms with specific meanings. Please see Section 9 for a list of definitions.

1.1 Overview

thawte's Certification Authorities (CAs) offer four distinct classes of end user subscriber certificates – High Assurance with extended validation, High Assurance, Medium Assurance and Low Assurance. The distinction between these classes of Certificates is the level of Subscriber identification and authentication performed (*See* CPS §§ 3.1.8, 3.1.9). In addition, specific types of certificates within these classes have specific intended uses (*See* CPS §1.3.4) and certificate profiles (*See* CPS §7.1).

thawte High Assurance with extended validation Certificates are certificates issued by ***thawte*** in conformance with the Guidelines for Extended Validation Certificates published by the a forum consisting of major certification authorities and browser vendors.

thawte High Assurance Certificates are issued to organizations (including sole proprietors) to provide authentication; message, software, and content integrity; and confidentiality encryption. ***thawte*** High Assurance Certificates provide assurances of the identity of the Subscriber based on a confirmation that the Subscriber organization does in fact exist, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorized to do so. ***thawte*** High Assurance Certificates for servers (SSL Web Server Certificates, SSL Wildcard Certificates and SGC SuperCerts) also provide assurances that the Subscriber is entitled to use the domain name listed in the Certificate Application.

thawte Medium Assurance SSL123 Certificates are issued to Domains to provide confidentiality encryption. ***thawte*** validates that the person enrolling for the certificate has control of the domain by requiring the person to respond to an e-mail hosted at that domain. No organization authentication is performed on the owner of the domain.

thawte Low Assurance Certificates are individual Certificates, whose validation procedures are based on assurances that the Subscriber's e-mail address is associated with a public key. They are appropriate for digital signatures, encryption, and access control for non-commercial or low-value transactions where proof of identity is unnecessary. In addition, ***thawte*** also offers Freemail Web of Trust individual certificates, which include confirmation of the Subscriber's identity. *See* CPS §3.1.9 for more information.

Within these classes of Certificates, ***thawte*** issues the following specific types of certificates to end user subscribers in accordance with this CPS:

Certificate Type	*Assurance Level*	*Issued to*	*Description and Benefit*
SSL Web Server Certificates with EV	High with extended validation	Organizations	High Assurance with extended validation secure SSL certificates issued by thawte in conformance with the Guidelines for Extended Validation Certificates. Capable of 256-bit encryption used to support SSL sessions between web browsers and servers.
SSL Web Server Certificates	High	Organizations (including sole proprietors) and individuals in the USA and Germany	High Assurance secure SSL certificates with stringent 3 step authentication capable of 256-bit encryption used to support SSL sessions between web browsers and servers.
Wildcard Certificates	High	Organizations (including sole proprietors) and individuals in the USA and Germany	Secure SSL certificates with stringent 3 step authentication capable of 256-bit encryption that secure multiple hosts on a single domain on the same server.
SGC SuperCerts	High	Organizations (including sole proprietors) and individuals in the USA and Germany	High Assurance Premium Server Gated Cryptography SSL certificates with stringent 3 step authentication, automatic 128-bit step-up encryption and capable of 256-bit encryption * used to support SSL sessions between web browsers and web servers. * Compatible with browsers IE 4.X or Netscape 4.06 and later
Code Signing Certificates	High	Organizations (including so and individuals in the USA and Germany le proprietors)	Certificates which secure delivery of code and content to browsers over the Internet.

Certificate Type	*Assurance Level*	*Issued to*	*Description and Benefit*
SSL123 Certificates	Medium	Registered Domain	Medium Assurance domain validated SSL certificates capable of 256-bit encryption used to support SSL sessions between web browsers and servers.
Personal E-mail Certificates	Low	Individuals	Secure e-mail communication ***thawte*** Personal E-mail Certificates contain "Thawte Freemail Member" as the common name. ***thawte's*** Freemail Web of Trust Certificates includes the Subscriber's authenticated name as the common name.

Table 1 – Certificate Types within the *thawte* PKI

thawte also offers the following programs for organizations which require multiple Server and Code Signing Certificates:

Program	*Purpose and Benefit*	*Program Description*
Starter PKI Program (SPKI)	The SPKI Program allows an organization to issue multiple SSL Web Server, SGC SuperCerts and Code Signing Certificates by means of self-service.	SPKI Customers approve or deny certificate requests using the SPKI system functionality. Customers manage the life cycle of certificates themselves and thus have full control of revocation and renewal of certificates. As with other certificates, ***thawte*** performs the back-end certificate issuance. Customers only issue certificates for SSL Web Server, SGC SuperCerts and Code Signing Certificates within their own organizations.

Program	*Purpose and Benefit*	*Program Description*
Reseller Partner Program	This program provides a one-stop base that allows Resellers to purchase, manage and resell SSL Web Server, SSL Wildcard, SSL123, SGC SuperCerts and Code Signing Certificates.	***thawte's*** Reseller Partner Program offers Resellers (e.g. Web Hosting companies, ISPs, Registrars) the ability to enroll for SSL Web Server,SSL Wildcard, SSL123, SGC SuperCerts and Code Signing Certificates on behalf of their customers . Although the Reseller assists with the enrollment process (*See* CPS § 4.1.1), the Reseller does not perform validation functions, but instead ***thawte*** performs these validation functions. Also, it is the Resellers' customers that obtain SSL Web Server, SSL Wildcard, SSL123, SGC SuperCerts and Code Signing Certificates as the actual Subscribers and are ultimately responsible for Subscriber obligations under the appropriate Subscriber Agreement. Resellers have an obligation to provide the applicable Subscriber Agreements to their clients to inform them of their obligations.
t-refer Program	This program allows companies to refer customers to ***thawte***. Once a certificate is issued to the customer, the referrer is paid a referral fee. SSL Web Server, SSL123, SGC SuperCerts and Code Signing Certificates are sold through this channel.	**t-refer** allows entities to install a link on their website: via this link their customers can buy ***thawte*** certificates. The referrer is not necessarily affiliated to the customer and will not need to be involved in the enrollment process with the customer. The channel is used to allow referrals to ***thawte*** for compensation without having to pre-pay. The discounts offered in the referral channel are lower than those in the Reseller Partner Program. The customer is responsible for both the enrollment and payment of their certificate.

Table 2 – *thawte* PKI Programs

1.1.1 Role of the thawte CPS and Ancillary Agreements

The CPS describes at a general level the overall business, legal, and technical infrastructure of the ***thawte*** PKI. The CPS describes, among other things:

- Obligations of Certification Authorities, Registration Authorities, Subscribers, and Relying Parties within the ***thawte*** PKI,
- Legal matters that are covered in Subscriber Agreements and Relying Party Agreements within the ***thawte*** PKI,

- Audit and related security and practices reviews that ***thawte*** and ***thawte*** PKI Participants undertake,
- Methods used within the ***thawte*** PKI to confirm the identity of Certificate Applicants for each type of Certificate,
- Operational procedures for Certificate life cycle services undertaken in the ***thawte*** PKI, including Certificate application, issuance, acceptance, revocation, and renewal,
- Operational security procedures for audit logging, records retention, and disaster recovery used within the ***thawte*** PKI,
- Physical, personnel, key management, and logical security practices of PKI Participants,
- Certificate and Certificate Revocation List content within the ***thawte*** PKI, and
- Administration of the CPS, including methods of amending it.

In addition, there are ancillary agreements imposed by ***thawte*** which apply to ***thawte*** PKI Participants. These agreements bind Customers, Subscribers, and Relying Parties of ***thawte***. Among other things, the agreements flow down ***thawte*** requirements to these ***thawte*** PKI Participants and, in some cases, state specific practices for how they must meet ***thawte*** requirements.

1.1.2 Background Concerning Digital Certificates and the thawte PKI

This CPS assumes that the reader is generally familiar with Public Key Infrastructures (PKIs), Digital Certificates, Digital Signatures, Encryption, and the ***thawte*** PKI. If not, ***thawte*** advises that the reader obtain some training in the use of public key cryptography and public key infrastructure as implemented in the ***thawte*** PKI. General educational and training information is accessible from ***thawte*** at **http://www.thawte.com**. Also, a brief summary of the roles of the different ***thawte*** PKI Participants is set forth in CPS § 1.3.

1.1.3 Compliance with Applicable Standards

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including AICPA/CICA *WebTrust Program for Certification Authorities*, ANS X9.79:2001 *PKI Practices and Policy Framework*, and other industry standards related to the operation of CAs.

The structure of this CPS generally corresponds to the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, known as RFC 2527 of the Internet Engineering Task Force, an Internet standards body. The RFC 2527 framework has become a standard in the PKI industry. This CPS conforms to the RFC 2527 framework in order to make policy mapping and comparisons, assessment, and interoperation easier for persons using or considering using ***thawte*** services. ***thawte*** reserves the right to vary from the RFC 2527 structure as needed, for example to enhance the quality of the CPS or its suitability to ***thawte***

PKI participants. Moreover, the CPS structure may not correspond to future versions of RFC 2527.

1.2 Identification

This document is the ***thawte*** Certification Practice Statement.

1.3 Community and Applicability

The community governed by this CPS is the ***thawte*** PKI, which is a PKI that accommodates a worldwide, large, public, and widely distributed community of users with diverse needs for communications and information security. This CPS is the document that governs the ***thawte*** PKI. Participants in the ***thawte*** PKI are located across the globe.

1.3.1 Certification Authorities

The term Certification Authority ("CA") is an umbrella term that refers to all entities issuing Certificates within the ***thawte*** PKI. ***thawte*** currently operates the following Certification Authorities within the ***thawte*** PKI:

Type	*CA Name*	*CA Description*	*Registration Authorities*
thawte Root CAs	Thawte Server CA	High Assurance Root CA that issues: - Server Certificates - Sub-CA Certificates for ***thawte*** Issuing CAs	- ***thawte*** - ***thawte*** SPKI Customers
	thawte Primary Root CA	High Assurance offline Root CA that issues:	***thawte***
	VeriSign Class 3 Public Primary CA	High Assurance Root CA that tissues: Sub-CA Certificates for ***thawte*** Issuing CAs	• VeriSign
	Thawte Personal Freemail CA	Low Assurance Root CA that issues: - Sub-CA Certificates for ***thawte*** Issuing CAs	- ***thawte***
	Thawte Premium Server CA	High Assurance Root CA that issues: - Server Certificates - Sub-CA Certificates for ***thawte*** Issuing CAs	- ***thawte***

Type	*CA Name*	*CA Description*	*Registration Authorities*
	Thawte Personal Premium CA	Currently inactive	***thawte***
	Thawte Personal Basic CA	Currently inactive	***thawte***
	Thawte Time Stamping CA	Currently inactive	***thawte***
Subordinate Issuing CAs	Thawte Personal Freemail Issuing CA	Sub-CA that issues: Low assurance individual "Freemail" certificates for S/MIME and client authentication Low assurance "Freemail Web of Trust" certificates for S/MIME and client authentication	***thawte*** ***thawte*** Web of Trust Notaries
	Thawte Code Signing CA	Sub-CA that issues: High Assurance Code Signing Certificates	***thawte*** ***thawte*** SPKI Customers
	thawte SSL Domain CA	Sub-CA that issues: • Medium assurance Domain validated SSL certificates	• ***thawte***
	thawte SGC CA	Sub-CA that issues: • High assurance SGC SuperCerts	• ***thawte***
	thawte Extended Validation SSL CA	Sub-CA that issues: Extended validation SSL Certificates	***thawte***
	thawte Extended Validation SSL SGC CA	Sub-CA that issues: Extended validation SGC SuperCerts	***thawte***

Table 3 – CAs Within the Thawte PKI

Note: Refer to the ***thawte*** Repository at **http://www.thawte.com/repository** for updates to the current listing of ***thawte*** CAs.

1.3.2 Registration Authorities

Registration Authorities ("RAs") within the ***thawte*** PKI include the following:

Registration Authority	***Role***
thawte	***thawte*** performs the RA function for all high assurance certificates, medium assurance certificates and for low assurance "Freemail" certificates, which do not include the subscriber's name.
SPKI Customers	SPKI Customers perform identification and authentication of high assurance Certificate subscribers within the SPKI Customer's organization as described in CPS §1.1.
thawte Web of Trust Notaries	***thawte's*** Web of Trust Notaries perform the RA function for low assurance "Freemail Web of Trust certificates which contain the subscriber's authenticated name.

Table 4 – RAs within the *thawte* PKI

1.3.3 End Entities

Subscribers within the ***thawte*** PKI include the following:

Class	*Issued to*	*Types of Subscribers*
Low Assurance	Individuals	Any individual, including members of the general public.
Medium Assurance	Registered Domains	Any person who has control of a domain referring to a device including, but not limited to: • Web servers, mail servers and web traffic management devices • Intranet device utilizing IP addresses
High Assurance	Organizations	Organizations (including agencies, Educational Institutions, Government Departments, etc.) that control a device including, but not limited to: • Web servers, mail servers and web traffic management devices • Devices digitally signing code or other content.
	Sole Proprietors	Small Office Home Office ("SOHO") clients that are typically individuals who run a sole proprietor online or development business.
High Assurance with extended validation	Organizations	Incorporated Organizations (including government agencies, Educational Institutions, Government Departments, etc.) The types of Organizations that qualify for EV Certificates are more fully described in Appendix A1 of this CPS.

Table 5 – Subscribers within the *thawte* PKI

CAs are themselves, as a technical matter, Subscribers of Certificates, either as a Root CA issuing a self-signed Certificate to itself, or as a Subordinate CA issued a Certificate by a superior CA. References to "Subscribers" in this CPS, however, apply only to end-user Subscribers.

1.3.4 Applicability

This CPS applies to all ***thawte*** PKI Participants, including ***thawte***, Customers, Referrers, Resellers, Subscribers, and Relying Parties. This CPS describes the practices governing the use of High Assurance with extended validation, High Assurance, Medium Assurance and Low Assurance Certificates within the ***thawte*** PKI. Each type of Certificate is generally appropriate for use with the applications set forth in CPS §§ 1.3.4.1 and § 1.1 (Table 1). Nonetheless, by contract or within specific environments (such as an intra-company environment), ***thawte*** PKI Participants are permitted to use Certificates for higher security applications than the ones described in CPS §§ 1.1, 1.3.4.1. Any such usage, however, shall be limited to such entities and subject to CPS §§ 2.2.1.2, 2.2.2, and these entities shall be solely responsible for any harm or liability caused by such usage.

1.3.4.1 Suitable Applications

Individual Certificates and some organizational Certificates permit Relying Parties to verify digital signatures. ***thawte*** PKI Participants acknowledge and agree, to the extent permitted by applicable law, that where a transaction is required to be in writing, a message or other record bearing a digital signature verifiable with reference to a ***thawte*** Certificate may be valid, effective, and enforceable to an extent no less than if the same message or record been written and signed on paper. Subject to applicable law, a digital signature or transaction entered into with reference to a ***thawte*** Certificate shall be effective regardless of the geographic location where the ***thawte*** Certificate is issued or the digital signature created or used, and regardless of the geographic location of the place of business of the CA or Subscriber.

1.3.4.2 Restricted Applications

In general, ***thawte*** Certificates are general-purpose Certificates. ***thawte*** Certificates may be used to interoperate with diverse Relying Parties worldwide. Usage of ***thawte*** Certificates is not generally restricted to a specific business environment, such as a pilot, financial services system, vertical market environment, or virtual marketplace. Nonetheless, such use is permitted and Customers using Certificates within their own environment may place further restrictions on Certificate use within these environments. ***thawte*** and other ***thawte*** PKI Participants, however, are not responsible for monitoring or enforcing any such restrictions in these environments.

Nonetheless, certain ***thawte*** Certificates are limited in function. For example, CA Certificates may not be used for any functions except CA functions. Moreover, individual Certificates are intended for client applications and shall not be used as server or organizational Certificates. In addition, High Assurance organizational Certificates issued to devices are limited in function to web servers, mail servers or web traffic management devices (in the case of SSL Web Server Certificates and SGC SuperCerts) and Code Signing (in the case of Code Signing Certificates).

Also, with respect to ***thawte*** Certificates, the key usage extension is intended to limit the technical purposes for which a private key corresponding to the public key in a Certificate may be used within the ***thawte*** PKI. *See* CPS § 6.1.9. In addition, end-user Subscriber Certificates shall not be used as CA Certificates. This restriction is confirmed by the absence of a Basic Constraints extension. *See* CPS § 7.1.2. The effectiveness of extension-based limitations, however, is subject to the operation of software manufactured or controlled by entities other than ***thawte***.

More generally, Certificates shall be used only to the extent use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

1.3.4.3 Prohibited Applications

thawte Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Also, subject to CPS § 1.3.4, Low Assurance Personal E-mail and Freemail Web of Trust Certificates shall not be used as proof of identity or as support of nonrepudiation of identity or authority.

1.4 Contact Details

1.4.1 Specification Administration Organization

The organization administering this CPS is VeriSign, Inc. Inquiries should be addressed as follows:

VeriSign, Inc.
487 East Middlefield Road
Mountain View, CA 94043, USA
Attn: Practices Development – ***thawte*** CPS
+1 (650) 961-7500 (voice)
+1 (650) 426-5113 (fax)
practices@verisign.com

1.4.2 Contact Person

Address inquiries about the CPS to practices@verisign.com. or to the following address:

VeriSign, Inc.
487 East Middlefield Road
Mountain View, CA 94043 USA
Attn: Practices Development – ***thawte*** CPS
+1 (650) 961-7500 (voice)
+1 (650) 426-5113 (fax)
practices@verisign.com

1.4.3 Person Determining CPS Suitability for the Policy

The VeriSign/***thawte*** Practices Development group is responsible for determining whether this CPS and other documents in the nature of certification practice statements and certificate policies that supplement or are subordinate to this CPS are suitable under the ***thawte*** CPS.

2. General Provisions

2.1 Obligations

2.1.1 CA Obligations

CAs perform the specific obligations appearing throughout this CPS. In addition, ***thawte*** uses commercially reasonable efforts to ensure that Subscriber Agreements and Relying Party Agreements bind Subscribers and Relying Parties within the ***thawte*** PKI. Examples of such efforts include, but are not limited to, requiring assent to a Subscriber Agreement as a condition of enrollment or requiring assent to a Relying Party Agreement as a condition of receiving Certificate status information. Similarly, Resellers (where required by contract) must use Subscriber Agreements and Relying Party Agreements in accordance with the requirements imposed by ***thawte***. The Subscriber Agreements and Relying Party Agreements used by ***thawte*** and Resellers must include the provisions required by CPS §§ 2.2-2.4.

2.1.2 RA Obligations

Where the RA function is not performed by ***thawte*** itself, external RAs assist ***thawte*** by performing validation functions, approving or rejecting Certificate Applications, requesting revocation of Certificates, and approving renewal requests. The provisions of the CPS specify obligations of each category of RAs: ***thawte*** itself, SPKI Customers and ***thawte*** Web of Trust Notaries.

2.1.3 Subscriber Obligations

Subscriber obligations apply to Subscribers within the ***thawte*** PKI, through this CPS, by way of Subscriber Agreements approved by ***thawte***. Certain Subscriber Agreements in force within the ***thawte*** PKI appear at: **http://www.thawte.com/repository**.

Within the ***thawte*** PKI, Subscriber Agreements require that Certificate Applicants provide complete and accurate information on their Certificate Applications and manifest assent to the applicable Subscriber Agreement as a condition of obtaining a Certificate.

Subscriber Agreements apply the specific obligations appearing in the CPS to Subscribers within the ***thawte*** PKI. Subscriber Agreements require Subscribers to use their Certificates in accordance with CPS § 1.3.4. They also require Subscribers to protect their private keys in accordance with CPS §§ 6.1-6.2, 6.4. Under these Subscriber Agreements, if a Subscriber discovers or has reason to believe there has been a Compromise of the Subscriber's Private Key or the activation data protecting

such Private Key, or the information within the Certificate is incorrect or has changed, that the Subscriber must promptly:

- Notify ***thawte*** in accordance with CPS § 4.4.1.1 and request revocation of the Certificate in accordance with CPS §§ 3.4, 4.4.3.1, and
- Notify any person that may reasonably be expected by the Subscriber to rely on or to provide services in support of the Subscriber's Certificate or a digital signature verifiable with reference to the Subscriber's Certificate.

Subscriber Agreements require Subscribers to cease use of their private keys at the end of their key usage periods under CPS § 6.3.2.

Subscriber Agreements state that Subscribers shall not monitor, interfere with, or reverse engineer the technical implementation of the ***thawte*** PKI, except upon prior written approval from ***thawte***, and shall not otherwise intentionally compromise the security of the ***thawte*** PKI.

2.1.4 Relying Party Obligations

Relying Party obligations apply to Relying Parties within the ***thawte*** PKI, through this CPS, by way of ***thawte's*** Relying Party Agreement(s). Relying Party Agreement(s) in force within the ***thawte*** PKI appear at: **http://www.thawte.com/repository.**

Relying Party Agreements within the ***thawte*** PKI state that before any act of reliance, Relying Parties must independently assess the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose. They state that ***thawte***, CAs, and RAs are not responsible for assessing the appropriateness of the use of a Certificate. Relying Party Agreements specifically state that Relying Parties must not use Certificates beyond the limitations in CPS § 1.3.4.2 and for purposes prohibited in CPS § 1.3.4.3.

Relying Party Agreements further state that Relying Parties must utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain. Under these Agreements, Relying Parties must not rely on a Certificate unless these verification procedures are successful.

Relying Party Agreements also require Relying Parties to check the status of a Certificate on which they wish to rely, as well as all the Certificates in its Certificate Chain in accordance with CPS § 4.4.10. If any of the Certificates in the Certificate Chain have been revoked, according to Relying Party Agreements, the Relying Party must not rely on the end-user Subscriber Certificate or other revoked Certificate in the Certificate Chain.

Finally, Relying Party Agreements state that assent to their terms is a condition of using or otherwise relying on Certificates. Relying Parties that are also Subscribers agree to be bound by Relying Party terms under this section, disclaimers of warranty, and limitations of liability when they agree to a Subscriber Agreement.

Relying Party Agreements state that if all of the checks described above are successful, the Relying Party is entitled to rely on the Certificate, provided that reliance upon the Certificate is reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Relying Party Agreements state that Relying Parties must not monitor, interfere with, or reverse engineer the technical implementation of the ***thawte*** PKI, except upon prior written approval from ***thawte***, and shall not otherwise intentionally compromise the security of the ***thawte*** PKI.

2.1.5 Repository Obligations

thawte is responsible for the repository functions for its CAs. Upon revocation of an end-user Subscriber's Certificate, ***thawte*** publishes notice of such revocation on the ***thawte*** website at **https://www.thawte.com/cgi/lifecycle/roots.exe**. ***thawte*** publishes CRLs for its CAs pursuant to CPS §§ 2.6, 4.4.9.

2.2 Liability

2.2.1 Certification Authority Liability

The warranties, disclaimers of warranty, and limitations of liability among ***thawte***, Resellers, and their respective Customers within the ***thawte*** PKI are set forth and governed by the agreements among them. This CPS § 2.2.1 relates only to the warranties that certain CAs (***thawte*** CAs) must make to end-user Subscribers receiving Certificates from them and to Relying Parties, the disclaimers of warranties they shall make to such Subscribers and Relying Parties, and the limitations of liability they shall place on such Subscribers and Relying Parties.

thawte uses, and (where required) Resellers shall use, Subscriber Agreements and Relying Party Agreements in accordance with CPS § 2.1.1. These Subscriber Agreements shall meet the requirements imposed by ***thawte*** (in the case of Resellers). Requirements that Subscriber Agreements contain warranties, disclaimers, and limitations of liability below apply to those Resellers that use Subscriber Agreements. ***thawte*** adheres to such requirements in its Subscriber Agreements. ***thawte's*** practices concerning warranties, disclaimers, and limitations in Relying Party Agreements apply to ***thawte***. Note that terms applicable to Relying Parties shall also be included in Subscriber Agreements, in addition to Relying Party Agreements, because Subscribers often act as Relying Parties as well.

2.2.1.1 Certification Authority Warranties to Subscribers and Relying Parties

thawte's Subscriber Agreements include, and other Subscriber Agreements shall include, a warranty to Subscribers that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services and use of a repository conform to this CPS in all material aspects.

thawte's Relying Party Agreements contain a warranty to Relying Parties who reasonably rely on a Certificate that:

- All information in or incorporated by reference in such Certificate, except Non-verified Subscriber Information, is accurate, and
- The entities approving the Certificate Application and issuing the Certificate have substantially complied with this CPS when issuing the Certificate.

2.2.1.2 Certification Authority Disclaimers of Warranties

To the extent permitted by applicable law, ***thawte's*** Subscriber Agreements and Relying Party Agreements disclaim, and other Subscriber Agreements shall disclaim, ***thawte's*** possible warranties, including any warranty of merchantability or fitness for a particular purpose.

2.2.1.3 Certification Authority Limitations of Liability

To the extent permitted by applicable law, ***thawte's*** Subscriber Agreements and Relying Party Agreements limit, and other Subscriber Agreements shall limit ***thawte's*** liability. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. They also include the following liability caps limiting ***thawte's*** damages concerning High Assurance Certificates to two (2) times the purchase price of the Certificate.

thawte's limitation of liability for EV certificates is further described in Section 37 of Appendix A1 to this CPS

2.2.1.4 Force Majeure

To the extent permitted by applicable law, ***thawte's*** Subscriber Agreements and Relying Party Agreements include, and other Subscriber Agreements shall include, a force majeure clause protecting ***thawte***.

2.2.2 Registration Authority Liability

The warranties, disclaimers of warranty, and limitations of liability between an RA and the CA it is assisting to issue Certificates, or the applicable Reseller, are set forth and governed by the agreements between them.

2.2.3 Subscriber Liability

2.2.3.1 Subscriber Warranties

thawte's Subscriber Agreements require Subscribers to warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- No unauthorized person has ever had access to the Subscriber's private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Other Subscriber Agreements shall also contain these requirements.

2.2.3.2 Private Key Compromise

This CPS sets forth ***thawte*** requirements for the protection of the private keys of Subscribers, which are included by virtue of CPS § 6.2.7.1 in Subscriber Agreements. Subscriber Agreements state that Subscribers failing to meet these ***thawte*** requirements are solely responsible for any loss or damage resulting from such failure.

2.2.4 Relying Party Liability

Subscriber Agreements and Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to

the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in CPS § 2.1.4.

2.3 Financial Responsibility

2.3.1 Indemnification by Subscribers and Relying Parties

2.3.1.1 Indemnification by Subscribers

To the extent permitted by applicable law, ***thawte's*** Subscriber Agreements require, and other Subscriber Agreements shall require, Subscribers to indemnify ***thawte*** and any non- ***thawte*** RA's for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

2.3.1.2 Indemnification by Relying Parties

To the extent permitted by applicable law, ***thawte's*** Subscriber Agreements and Relying Party Agreements require, and other Subscriber Agreements shall require, Relying Parties to indemnify ***thawte*** and any non- ***thawte*** RA's for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

2.3.2 Fiduciary Relationships

To the extent permitted by applicable law, ***thawte's*** Subscriber Agreements and Relying Party Agreements disclaim, and other Subscriber Agreements shall disclaim, any fiduciary relationship between ***thawte*** or a non- ***thawte*** RA on one hand and a Subscriber or Relying Party on the other hand.

2.3.3 Administrative Processes

thawte, Inc. is a wholly owned subsidiary of VeriSign, Inc. VeriSign's financial resources are set forth in disclosures appearing at: http://www.verisign.com/verisign-inc/vrsn-investors/sec-filings/index.html

. VeriSign shall also maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

Subject to any limits appearing in applicable law, the laws of the state of California, USA, shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in California, USA. This choice of law is made to ensure uniform procedures and interpretation for all ***thawte*** PKI Participants, no matter where they are located.

This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that this CPS § 2.4.1 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

2.4.2 Severability, Survival, Merger, Notice

To the extent permitted by applicable law, ***thawte's*** Subscriber Agreements and Relying Party Agreements contain, and other Subscriber Agreements shall contain, severability, survival, merger, and notice clauses. A severability clause in an agreement prevents any determination of the invalidity or unenforceability of a clause in the agreement from impairing the remainder of the agreement. A survival clause specifies the provisions of an agreement that continue in effect despite the termination or expiration of the agreement. A merger clause states that all understandings concerning the subject matter of an agreement are incorporated in the agreement. A notice clause in an agreement sets forth how the parties are to provide notices to each other.

2.4.3 Dispute Resolution Procedures

2.4.3.1 Disputes Among ***thawte*** and Customers

Disputes between ***thawte*** and one of its Customers shall be resolved pursuant to provisions in the applicable agreement between the parties.

2.4.3.2 Disputes with End-User Subscribers or Relying Parties

To the extent permitted by applicable law, ***thawte's*** Subscriber Agreements and Relying Party Agreements contain, and other Subscriber Agreements shall contain, a dispute resolution clause. The clause states that dispute resolution procedures require an initial negotiation period of sixty (60) days followed by litigation in the federal or state court encompassing Santa Clara County, California, USA in the case of claimants who are U.S. residents, or, in the case of all other claimants, arbitration administered by the International Chamber of Commerce ("ICC") in accordance with the ICC Rules of Conciliation and Arbitration.

2.5 Fees

2.5.1 Certificate Issuance or Renewal Fees

thawte is entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates.

2.5.2 Certificate Access Fees

thawte CA Certificates are made publicly available through their inclusion in leading browser software. ***thawte*** Subscriber Certificates are not published in a publicly accessible repository. ***thawte*** does not charge a fee as a condition of making Certificates available to Relying Parties.

2.5.3 Revocation or Status Information Access Fees

thawte does not charge a fee as a condition of making the CRL's required by CPS § 4.4.9 available in a repository or otherwise available to Relying Parties. ***thawte*** does not permit access to revocation information or Certificate status information in its repository by third parties that provide products or services that utilize such Certificate status information without ***thawte's*** prior express written consent.

2.5.4 Fees for Other Services Such as Policy Information

thawte does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, is subject to a license agreement with ***thawte***.

2.5.5 Refund Policy

2.5.5.1 Before a Certificate is Issued.

If you cancel a Certificate request before the Certificate has been issued, ***thawte*** will refund you any amount paid, less an administration fee of 10% if documents have been received and work has been performed on the Certificate Application. To request a refund, please e-mail billing@thawte.com.

2.5.5.2 After Certificate Has Been Issued.

If you cancel a certificate after it has been issued and you believe that you have grounds to request a refund, you must request such a refund from the ***thawte*** account manager allocated to your Certificate Application. Grounds for such a refund would be:

(i) Technical problems due to an error on our system, where the ***thawte*** Technical Support team has been unable to rectify the situation.

(ii) If the reason for the cancellation or revocation is due to ***thawte*** breaching a warranty or other material obligation under this Agreement, or the ***thawte*** CPS, then you will be entitled to a full refund of the Certificate fees paid to ***thawte***. Alternatively you may choose to receive a new Certificate at no charge. All refunds must be authorized by the ***thawte*** Customer Support Manager, or Technical Support Manager.

2.5.6 Reissue Policy

In order to adhere to our stringent policies and practices, reissues can only be issued under the following conditions. Please note that ***thawte*** cannot reissue a certificate if the application does not adhere to these conditions.

A Subscriber may make changes to the host of the common name (i.e. Host Name) included in a certificate anytime within the lifespan of the certificate. ***thawte*** authenticates the new domain in terms of Section 3.1.8.1.

thawte may reissue a certificate under the following circumstances:

- the host name changes but domain name remains the same e.g. www.domain.com changes to secure.domain.com
- your software changes or the request was for the incorrect server software.
- you have lost or corrupted your private key
- you have forgotten your pass phrase or password for your Private key

The conditions that apply are:

- All company and domain details must remain the same except as indicated above.

- The new certificate will be signed from the date of reissue until the anniversary date of the initial certificate i.e. the original expiry date will remain the same.
- You may only get a reissue for the same product as the initial certificate that you requested.

2.6 Publication and Repository

2.6.1 Publication of CA Information

thawte is responsible for the repository function for the ***thawte*** CAs. ***thawte*** publishes this CPS, Subscriber Agreements, and Relying Party Agreements in the repository section of ***thawte's*** website at **http://www.thawte.com/repository**.

thawte publishes Certificates in accordance with Table 6 below.

Certificate Type	*Publication Requirements*
Thawte Root CA Certificates	Available to Relying Parties through inclusion in current browser software. Provided to Subscribers as part of the Certificate Chain provided with the end-user Subscriber Certificate.
Thawte Issuing CA Certificates	Provided to Subscribers as part of the Certificate Chain provided with the end-user Subscriber Certificate.
End-User Subscriber Certificates	Not publicly published by ***thawte***. Provided to Subscribers upon certificate issuance.

Table 6 – Certificate Publication Requirements

thawte publishes Certificate status information in accordance with CPS § 4.4.9.

2.6.2 Frequency of Publication

Updates to this CPS are published in accordance with CPS § 8. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. Certificates are published upon issuance. Certificate status information is published in accordance with CPS § 4.4.9.

2.6.3 Access Controls

Information published in the repository portion of the ***thawte*** web site is publicly accessible information. Read only access to such information is unrestricted. ***thawte*** requires persons to agree to a Relying Party Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. ***thawte*** has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

2.6.4 Repositories

See CPS § 2.1.5.

2.7 Compliance Audit

A WebTrust for Certification Authorities ("WebTrust for CAs") examination is performed of the ***thawte*** CAs on an annual basis. In addition, ***thawte*** is entitled to perform audits of its SPKI Customers and ***thawte*** Web of Trust Notaries.

2.7.1 Frequency of Entity Compliance Audit

Compliance audits are performed on an annual basis at the sole expense of ***thawte***.

2.7.2 Identity / Qualifications of Auditor

thawte's CA compliance audits are performed by a public accounting firm that:

- Demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function, and
- Is accredited by the American Institute of Certified Public Accountants (AICPA), which requires the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education.

2.7.3 Auditor's Relationship to Audited Party

A public accounting firm that is independent of ***thawte*** performs compliance audits of ***thawte's*** operations.

2.7.4 Topics Covered by Audit

The scope of ***thawte's*** annual WebTrust for Certification Authorities examination includes:

- CA business practices disclosure,
- CA environmental controls,
- CA key life cycle management, and
- Certificate life cycle management.

2.7.5 Actions Taken as a Result of Deficiency

With respect to compliance audits of ***thawte's*** operations, significant exceptions or deficiencies identified during the compliance audit will result in a determination of actions to be taken. This determination is made by ***thawte*** management with input from the auditor. If exceptions or deficiencies are identified, ***thawte*** management is responsible for developing and implementing a corrective action plan. If ***thawte***

determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the ***thawte*** PKI, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, ***thawte*** management will evaluate the significance of such issues and determine the appropriate course of action.

2.7.6 Communications of Results

Results of the compliance audit of ***thawte's*** operations may be released at the discretion of ***thawte*** management.

2.8 Confidentiality and Privacy

2.8.1 Types of Information to be Kept Confidential and Private

The following records of Subscribers are, subject to CPS § 2.8.2, kept confidential and private ("Confidential/Private Information"):

- CA application records, whether approved or disapproved,
- Certificate Application records (subject to CPS § 2.8.2),
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by ***thawte*** or VeriSign
- ***thawte*** audit reports created by ***thawte*** or their respective auditors (whether internal or public), except for WebTrust for Certification Authorities audit reports which may be published at the discretion of ***thawte***,
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of ***thawte*** hardware and software and the administration of Certificate services and designated enrollment services.

2.8.2 Types of Information Not Considered Confidential or Private

thawte PKI Participants acknowledge that Certificates, Certificate revocation and other status information, ***thawte's*** repository, and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under CPS § 2.8.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

See CPS § 2.8.2.

2.8.4 Release to Law Enforcement Officials

thawte PKI Participants acknowledge that ***thawte*** shall be entitled to disclose Confidential/Private Information if, in good faith, ***thawte*** believes disclosure is necessary in response to subpoenas and search warrants. This section is subject to applicable privacy laws.

2.8.5 Release as Part of Civil Discovery

thawte PKI Participants acknowledge that ***thawte*** shall be entitled to disclose Confidential/Private Information if, in good faith, ***thawte*** believes disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents. This section is subject to applicable privacy laws.

2.8.6 Disclosure Upon Owner's Request

thawte's privacy policy contains provisions relating to the disclosure of Confidential/Private Information to the person who provided such information to ***thawte***. This section is subject to applicable privacy laws.

2.8.7 Other Information Release Circumstances

No stipulation.

2.9 Intellectual Property Rights

The allocation of Intellectual Property Rights among ***thawte*** PKI Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such ***thawte*** PKI Participants. The following subsections of CPS § 2.9 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

2.9.1 Property Rights in Certificates and Revocation Information

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. ***thawte*** and Customers grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement. ***thawte*** and Customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable Relying Party Agreement or any other applicable agreements.

2.9.2 Property Rights in the CPS

thawte PKI Participants acknowledge that ***thawte*** retains all Intellectual Property Rights in and to this CPS.

2.9.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

2.9.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CA's and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, regardless of the' physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, ***thawte's*** Root CA public keys and the root Certificates containing them are the property of ***thawte***. Thawte licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software. Finally, without limiting the generality of the foregoing, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares.

---

3. Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

3.1.1.1 CA Certificates

thawte CA Certificates contain X.501 Distinguished Names in the Issuer and Subject fields. ***thawte*** CA Distinguished Names consist of the components specified in Table 7 below.

Attribute	*Value*
Common Name (CN)	CA Name
Organizational Unit (OU)	"Certification Services Division" or "Thawte Certification" (except for Thawte Code Signing CA and Thawte Personal Freemail Issuing CA which omit this attribute)
Organization (O)	"Thawte Consulting cc" or "Thawte Consulting" or "Thawte" or "Thawte Inc."
Locality (L)	"Cape Town" except for the Thawte Time Stamping CA which includes "Durbanville", and Thawte Code Signing CA and Thawte Personal Freemail Issuing CA which omit this attribute
State or Province (P)	"Western Cape"
Country (C)	"ZA" (except for Thawte Code Signing CA and Thawte Personal Freemail Issuing CA which omit this attribute)
E-Mail (E)	Used for Root CAs only (excluding the Thawte Time Stamping CA). Contains a contact e-mail address for the CA.

Table 7 – Distinguished Name Attributes in CA Certificates

3.1.1.2 Server Certificates

Server Certificates (except SSL123 Certificates) contain an X.501 distinguished name in the Subject name field and consist of the components specified in Table 8 below.

Attribute	*Value*
Common Name (CN)	Authenticated domain name
Organizational Unit (OU)	Optionally includes Subscriber-provided department or division name
Organization (O)	Authenticated organization name
Locality (L)	Set based on subscriber locality
State or Province (P)	Set based on subscriber state or province
Country (C)	Set based on subscriber country
E-Mail (E)	Not used

Table 8 – Distinguished Name Attributes in Server Certificates

EV SSL certificate content and profile requirements are discussed in Section 6 of Appendix A3 to this CPS

3.1.1.3 Certificate subject details –SSL123

3.1.1.3.1 Certificate subject details – SSL123Certificates

Attribute	*Value*
Common Name (CN)	Registered domain name
Organizational Unit (OU)	"Domain Validated"
Organizational Unit (OU)	Go to https://www.***thawte***.com/repository/index.html
Organizational Unit (OU)	***thawte*** SSL123 Certificate
Organization (O)	Registered domain name
Locality (L)	Not used
State or Province (P)	Not used
Country (C)	Not used
E-Mail (E)	Not used

Table 9 – Distinguished Name Attributes in SSL123 Certificates

3.1.1.3.2 Certificate subject details- SSL123 Certificates for Intranet

Attribute	*Value*
Common Name (CN)	Server, Intranet name or IP address within the private range for intranets as specified by RFC 1597
Organizational Unit (OU)	"Validated for Intranet Usage"

Attribute	*Value*
Organizational Unit (OU)	Go to https://www.thawte.com/repository/index.html
Organizational Unit (OU)	***thawte*** SSL123 Certificate
Organization (O)	Server, Intranet name or IP address
Locality (L)	Not used
State or Province (P)	Not used
Country (C)	Not used
E-Mail (E)	Not used

Table 10 – Distinguished Name Attributes in SSL123 Certificates for Intranet Use

3.1.1.4 Code Signing Certificates

Code Signing Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in Table 11 below.

Attribute	*Value*
Common Name (CN)	Authenticated organization name
Organizational Unit (OU)	"Secure Application Development" or Subscriber-provided department or division name
Organization (O)	Authenticated organization name
Locality (L)	Set based on subscriber locality
State or Province (P)	Set based on subscriber state or province
Country (C)	Set based on subscriber country
E-Mail (E)	Not used

Table 11 – Distinguished Name Attributes in Code Signing Certificates

3.1.1.5 Personal E-mail Certificates

Personal E-mail Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in Table 12 below.

Attribute	*Value*
Common Name (CN)	"Thawte Freemail Member"
E-Mail (E)	Authenticated e-mail address

Table 12 – Distinguished Name Attributes in Freemail Certificates

3.1.1.6 Freemail Web of Trust Certificates

Freemail Web of Trust Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in Table 13 below.

Attribute	*Value*
Common Name (CN)	Authenticated Subscriber name
E-Mail (E)	Authenticated e-mail address

Table 13 – Distinguished Name Attributes in Freemail Web of Trust Certificates

The Common Name (CN) component of the Subject distinguished name of end-user Subscriber Certificates is authenticated in the case of CA, Server, Code Signing, and Freemail Web of Trust Certificates.

- The authenticated common name value included in the Subject distinguished names of organizational Certificates is a domain name (in the case of Server Certificates) or the legal name of the organization (in the case of Code Signing Certificates).
- The common name value included in the Subject distinguished name of individual Certificates represents the individual's generally accepted personal name (in the case of Freemail Web of Trust Certificates).
- For Freemail Certificates, the generic name "Thawte Freemail Member" is included as the common name value in the Subject distinguished name.

3.1.1.7 SSL Web Server Certificates with EV

"SSL Web Server Certificates with EV distinguished name attributes are discussed in Section 6 of Appendix A3 to this CPS."

3.1.2 Need for Names to be Meaningful

Server and Code Signing Certificates contain names with commonly understood semantics permitting the determination of the identity of the organization or individual (in the case of a sole proprietorship) that is the Subject of the Certificate. For such Certificates, pseudonyms of end-user Subscribers (names other than a Subscriber's true organizational or personal name) are not permitted.

Freemail Web of Trust Certificates contain the Subscriber's generally accepted personal name. Personal E-mail Certificates contain the Common Name "***thawte*** Freemail Member."

Thawte CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

3.1.3 Rules for Interpreting Various Name Forms

No stipulation.

3.1.4 Uniqueness of Names

For High Assurance Certificates, ***thawte*** ensures that Subject Distinguished Names are unique within the domain of a specific CA through automated components of the Subscriber enrollment process. For Low Assurance Certificates, Subscribers are permitted to have multiple certificates with the same Subject Distinguished Name.

3.1.5 Name Claim Dispute Resolution Procedure

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. ***thawte***, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. ***thawte*** is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.1.6 Recognition, Authentication, and Role of Trademarks

See CPS § 3.1.5.

3.1.7 Method to Prove Possession of Private Key

thawte verifies the Certificate Applicant's possession of a private key through the use of a digitally signed certificate request pursuant to PKCS #10, another cryptographically-equivalent demonstration, or another ***thawte***-approved method.

3.1.8 Authentication of Organization Identity

thawte confirms the identity of High Assurance organizational end-user Subscribers (including sole proprietors) and other enrollment information provided Certificate Applicants (except for Nonverified Subscriber Information) in accordance with the procedures set forth in the subsections that follow. In addition to the procedures below, the Certificate Applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate in accordance with CPS § 3.1.7.

3.1.8.1 Authentication of the Identity of Organizational End-User Subscribers

thawte confirms the identity of a Certificate Applicant for a High Assurance Server or Code Signing Certificate by:

- Verifying that the organization exists through the use of at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization and
- Confirming with an appropriate Organizational contact by telephone, postal mail, or a comparable procedure certain information about the organization, 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

Organization authentication is not performed for SSL123 Certificates. These certificates are authenticated as described in Table 14 below.

Where a domain name or e-mail address is included in the certificate thawte authenticates the Organization's right to use that domain name. Confirmation of an organization's right to use a domain name is not performed for SSL123 Certificates. For these certificates, validation of domain control only is performed, as described in Table 14 below.

Certificate Type	*Additional Procedures*
SSL123 Certificate	***thawte*** validates the Certificate Applicant's control of a domain by requiring the person to answer an e-mail sent to the e-mail address listed or predetermined for that domain.
SSL123 for Intranet Certificate	***thawte*** validates that the Server or Intranet name or IP are not publicly accessible via the World Wide Web. When an IP address is used ***thawte*** validates that the IP address is within the private range for intranets as specified by RFC 1597
SGC SuperCert and Code Signing Certificates	***thawte*** performs the additional checks necessary to satisfy United States export regulations and licenses issued by the United States Department of Commerce Bureau of Industry and Science ("BIS") (formerly known as the Bureau of Export Administration ("BXA"))., OFAC and Denied Entities.
SSL Web Server Certificates with EV	***thawte***'s procedures for issuing Extended Validation SSL Certificates are described in Appendix A1 to this CPS."

Table 14 – Specific Authentication Procedures

With respect to Starter PKI (SPKI) Customers, the identity confirmation process begins with ***thawte's*** confirmation of the identity of the Starter PKI Customer itself in accordance with this section. Following such confirmation, the Starter PKI Customer is responsible for approving the issuance of SSL Web Server and Code Signing Certificates within its own organization by ensuring that the server designated as the Subject of a SSL Web Server Certificate actually exists.

3.1.8.2 Authentication of the Identity of CA's

For ***thawte*** CA Certificate Applications, certificate requests are created, processed and approved by authorized ***thawte*** personnel using a controlled process that requires the participation of multiple trusted ***thawte*** employees.

3.1.9 Authentication of Individual Identity

thawte provides two types of Low Assurance individual Personal E-mail certificates:

- Personal E-mail Certificates, also known as Freemail Certificates, which include verification of the Subscriber's e-mail address
- Freemail Web of Trust Certificates, which also include verification of the Subscriber's name.

3.1.9.1 Personal E-mail Certificates

Personal E-mail Certificates are issued using the Thawte Personal Freemail Issuing CA root and therefore they are referred to as Thawte Freemail Certificates. For Personal E-mail Certificates, ***thawte*** confirms that the Certificate Applicant holds the private key corresponding to the public key to be included in the Certificate in accordance with CPS § 3.1.7. In addition, ***thawte*** performs a limited confirmation of the Certificate Applicant's e-mail address through an e-mail ping.

thawte does not authenticate the identity of the Certificate Applicant. As a result, the Certificate Applicant's personal name is not included in a ***thawte*** Personal E-mail Certificate. Instead, "Thawte Freemail Member" is included as the common name value in the Subject distinguished name field of the Certificate.

3.1.9.2 Freemail Web of Trust Certificates

In addition to the verification steps required by CPS §3.1.9.1, for Freemail Web of Trust Certificates, ***thawte*** utilizes its international network of "***thawte*** Web of Trust Notaries" to authenticate the identity of Subscribers. ***thawte*** has established a point system whereby ***thawte*** Web of Trust Notaries are empowered to award a certain number of points to the Certificate Applicant based on the ***thawte*** Web of Trust Notary's experience level (Refer Table 15). The Certificate Applicant, in turn must receive a certain number of points, before his or her name can be included in a Freemail Web of Trust Certificate.

3.1.9.2.1 Points System

The ***thawte*** Web of Trust is based on a points system. When a ***thawte*** Web of Trust Notary makes an assertion about the identity of another, he or she effectively issues the individual with a specified number of points. A ***thawte*** Web of Trust Notary is able to issue between 10 and 35 points at a time, depending on experience. A ***thawte*** Web of Trust Notary can only issue points to a particular person once and cannot issue points to themselves.

When an E-mail member has obtained 50 Trust Points, he or she will be able to request a new certificate. This new certificate will contain the member's name instead of stating "Freemail member" in the distinguished name field,.

Once he or she has obtained 100 points, the member may automatically become a ***thawte*** Web of Trust Notary and will have the ability to issue Trust Points. The number of points that a ***thawte*** Web of Trust Notary is able to issue will increase as he or she issues more points to others. ***thawte*** judges the "experience" of a ***thawte*** Web of Trust Notary by the number of trust assertions he or she has made, as specified in Table 13 below:

Experience Level	*Awardable Points*
New Notary	10 Points
After 5 assertions	15 Points
After 10 assertions	20 Points
After 15 assertions	25 Points
After 25 assertions	30 Points
After 35 assertions	35 Points

Table 15 – Awardable Points by Experience Level

3.1.9.2.2 Web of Trust Rules

thawte Web of Trust Notaries and members of the Web of Trust are required to follow clear guidelines and rules to ensure a higher level of assurance for the information in the subject name field of Freemail Web of Trust certificates. These rules, specified in Table 16 below, are binding on all ***thawte*** Web of Trust Notaries and members.

Requirement	*Description*
Personal Appearance	A ***thawte*** Web of Trust Notary may only assign Trust Points to a member if he or she meets the member in person, and views the originals of the member's identification documents. The member must provide the Notary with copies of these identification documents.
Presentation of Identification Documents with Copies	A ***thawte*** Web of Trust Notary must confirm the identity of the member by comparing the member's information in the ***thawte*** Personal Certificate System with the identification documents presented by the member. The ***thawte*** Web of Trust Notary must also ensure that the copies of the identification documents presented by the member are true copies of the original documents presented by the member. The member's identification documents must include at least one photo identity document. This photo identity document must be issued by a state or governmental body, and must be nationally recognized as an acceptable form of identity. Photographs that are included in this documentation must bear a good likeness to the member.

Requirement	*Description*
Retention of Copies	Each ***thawte*** Web of Trust Notary must retain a copy of the identifying documentation used to confirm the member's identity for every assertion made by that ***thawte*** Web of Trust Notary.
Statement of Notarization	The member and the ***thawte*** Web of Trust Notary must both sign a copy of the "Statement of Notarization" provided by ***thawte*** during the identity assertion process. The ***thawte*** Web of Trust Notary must keep this signed statement on record for 5 years.
Confidentiality	***thawte*** Web of Trust Notaries may not disclose to any party other than ***thawte*** any information received from the member during the notarization process, and must take reasonable steps to keep documentation confidential.
Notary Fees	***thawte*** Web of Trust Notaries may charge a fee for an identity assertion as long as the fee charged is reflected in the Directory of Notaries. The fee may not differ from that quoted in the Directory.
Liability	A ***thawte*** Web of Trust Notary may be held responsible and have his or her Freemail Web of Trust Certificate revoked if he or she is unable to provide ***thawte*** with copies of a member's identifying documentation upon request.
Notary Trust Points	***thawte*** may, at its sole discretion, at any time, change the number of Trust Points that a ***thawte*** Web of Trust Notary can assign. In the absence of such action by ***thawte***, a ***thawte*** Web of Trust Notary will be able to assign between 10 and 35 Trust Points based on the number of assertions that the ***thawte*** Web of Trust Notary has already made.

Table 16 – Web of Trust Rules

3.1.9.2.3 Remote Authentication

thawte has implemented a system that makes remote authentication possible for applicants who are not in the vicinity of ***thawte*** Web of Trust Notaries. For a nominal fee, ***thawte*** allows applicants to have their identities validated by two of the following people ("Referees"):

- Bank manager
- Registered lawyer
- Registered CPA (accountant)

- US Notary public (limited to Notary Publics in States where the licensing status information is provided online by the appropriate licensing authority)

Applicants are required to download a form from the ***thawte*** website. Applicants must take two of these copies of the form to each referee, along with an original and a photocopy of two national forms of photo identity (passport and driver's license, for instance). The referees must complete both copies of the form in the presence of the applicants and sign both photocopies of the identity documentation. The applicants will keep one copy of the form, and the referees are asked to keep the other copy for a maximum period of 31 days, or until such time as ***thawte*** has contacted them to verify that they did really sign the forms.

Each applicant must provide a copy of the form, along with the signed photocopy of his/her photo identity to ***thawte***. ***thawte*** will then verify the authenticity of the forms before issuing 100 Trust Points to the applicant. ***thawte*** will keep these forms on record for at least five years.

3.2 Routine Rekey and Renewal

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. ***thawte*** generally requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey"). However, in certain cases (i.e., for web server certificates) ***thawte*** permits Subscribers to request a new certificate for an existing key pair (technically defined as "renewal"). Table 17 below describes ***thawte's*** requirements for routine rekey (issuance of a new certificate for a new key pair that replaces an existing key pair) and renewal (issuance of a new certificate for an existing key pair).

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal," focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated. For all types of ***thawte*** Certificates, except for Server Certificates, this distinction is not important as a new key pair is always generated as part of ***thawte's*** end-user Subscriber Certificate replacement process.

However, for Server Certificates, because the Subscriber key pair is generated on the web server and most web server key generation tools permit the creation of a new Certificate Request for an existing key pair, there is a distinction between "rekey" and "renewal." In addition, new CA Certificates may be issued for existing ***thawte*** CA key pairs subject to the constraints specified in Table 17 below.

Certificate Type	*Routine Rekey and Renewal Requirements*
Personal E-mail, (named Freemail) Freemail Web of Trust and Code Signing Certificates	For these types of Certificates, Subscriber key pairs are browser generated as part of the online enrollment process. The Subscriber does not have the option to submit an existing key pair for "renewal." Accordingly, for these types of Certificates, rekey is supported and Certificate renewal is not.
Server Certificates	For Server Certificates, Subscriber key pairs are generated outside of the online enrollment process (i.e., generated on a web server). Most server key generation tools, permit the Subscriber to create a new Certificate Signing Request (CSR) for a previously used key pair. However, submission of a CSR for a previously used key pair is not necessary. ***thawte*** will sign the previous CSR for the new validity period, where the server's key management functionality allows the installation of a new certificate for an existing key pair. Accordingly, for Server Certificates, both rekey and renewal are supported.
CA Certificates	Renewal of CA Certificates is permitted as long as the cumulative certified lifetime of the CA key pair does not exceed the applicable maximum CA key pair lifetime specified in CPS § 6.3.2. Thawte CAs may also be rekeyed in accordance with CPS § 4.7. Accordingly, for Thawte CA Certificates both rekey and certificate renewal are supported.

Table 17 – Routine Rekey and Renewal Requirements

3.2.1 Routine Rekey and Renewal for End-User Subscriber Certificates

Subscriber Certificates, which have not been revoked, may be replaced (i.e., rekeyed or renewed) before the expiration date. Currently 1 and 2 year certificates may be renewed starting 90 days before expiration. However, in the Reseller Partner Program, 1 year certificates may be renewed 90 days before expiration and 2 year certificates may be renewed starting 32 days before expiration.

Expired certificates may also be renewed. The validity period for the renewed certificate will be calculated from the date the original certificate expired. As part of the initial registration process, Subscribers choose a password. Upon requesting rekey or renewal of a Certificate within the specified timeframe, if a Subscriber's software supports rekey and the Subscriber successfully submits their password, reenrollment information, and the enrollment information (including contact information) has not changed, thawte may rekey, or renew the certificate. After rekeying or renewal in this fashion, and on at least alternative instances of subsequent rekeying or renewal thereafter, Thawte shall reconfirm the identity of the Subscriber in accordance with the requirements specified in CPS §3.1.8.1 and §3.1.9 for the authentication of an original Certificate Application.

3.2.2 Routine Rekey and Renewal for CA Certificates

thawte CAs may be rekeyed periodically in accordance with CPS § 4.7.

thawte CA Certificates may be renewed within the parameters specified in CPS § 6.3.2. For example, if an initial Root CA certificate was issued with a lifetime of 10 years, renewed certificates may be issued to extend the validity period of the CA's key pair for an additional 15 years, reaching the maximum permitted validity period of 25 years. CA Certificate Renewal is not permitted after Certificate Expiration.

For Thawte Root CAs and Thawte Sub-CA Certificates, renewal requests are created and approved by authorized ***thawte*** personnel through a controlled process that requires the participation of multiple trusted individuals.

3.3 Rekey After Revocation

Rekey after revocation is not be permitted if:

- revocation occurred because the Certificate (other than a Personal E-mail Certificate) was issued to a person other than the one named as the Subject of the Certificate,
- the Certificate (other than a Personal E-mail Certificate) was issued without the authorization of the person named as the Subject of such Certificate, or
- the entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false.

Subject to the foregoing paragraph, Subscriber Certificates, which have been revoked, may be replaced (i.e., rekeyed) in accordance with Table 18 below.

Timing	*Requirement*
Prior to Certificate expiration	For replacement of a Certificate following revocation of the Certificate, ***thawte*** verifies that the person seeking certificate replacement is, in fact, the Subscriber (for individuals) or an authorized organizational representative (for organizations) through the use of a password, as described in CPS § 3.2.1. Other than this procedure, the requirements for the validation of an original Certificate Application in CPS §§ 3.1.8.1, 3.1.9 are used for replacing a Certificate following revocation. Such Certificates contain the same Subject distinguished name as the Subject distinguished name of the Certificate being replaced.
After Certificate expiration	In this scenario, the requirements specified in CPS §§ 3.1.8.1, § 3.1.9 for the authentication of an original Certificate Application shall be used for replacing an end-user Subscriber Certificate.

Table 18 – Requirements for Certificate Replacement After Revocation

3.4 Revocation Request

Prior to the revocation of a Certificate, ***thawte*** verifies that the revocation has been requested by the Certificate's Subscriber, the entity that approved the Certificate Application. Acceptable procedures for authenticating the revocation requests of a Subscriber include:

- Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or the equivalent thereof), and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record
- Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked,
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service
- However, only the Authorizing Contact can sign a revocation form for SSL123 Certificates.

thawte Administrators are entitled to request the revocation of end-user Subscriber Certificates. ***thawte*** authenticates the identity of Administrators before permitting them to perform revocation functions.

4. Operational Requirements

4.1 Certificate Application

4.1.1 End-User Subscriber Certificate Applications

For ***thawte*** Certificates, all end-user Certificate Applicants shall undergo an enrollment process consisting of:

- completing a Certificate Application and providing the required information,
- generating, or arranging to have generated, a key pair in accordance with CPS § 6.1,
- the Certificate Applicant delivering his, her, or its public key to ***thawte*** in accordance with CPS § 6.1.3,
- demonstrating to ***thawte*** pursuant to CPS § 3.1.7 that the Certificate Applicant has possession of the private key corresponding to the public key delivered to ***thawte***, and
- manifesting assent to the relevant Subscriber Agreement.

Reseller Partners may submit Certificate Applications on behalf of their customers pursuant to the Reseller Partner Program (*See* CPS § 1.1).

Certificate Applications are submitted either to ***thawte*** or an SPKI Customer for processing, resulting in approval or denial. The entity processing the Certificate Application and the entity issuing the Certificate pursuant to CPS § 4.2 may be two different entities as shown in the Table 19 below.

Certificate Type	*Entity Processing Certificate Applications*	*Entity Issuing Certificate*
High Assurance with extended validation – SSL Web Server Certificates with EV	• ***thawte***	***thawte***
High Assurance – SSL Web Server Certificates and Code Signing	• ***thawte*** • SPKI Customers	***thawte***
Medium Assurance – SSL123 Certificates	***thawte***	***thawte***
Low Assurance – Personal E-mail (Freemail)	***thawte***	***thawte***
Low Assurance – Freemail Web of Trust	***thawte*** Web of Trust Notary	***thawte***

Table 19 – Entities Receiving Certificate Applications

4.1.2 CA Certificate Applications

The Thawte Root CAs issue certificates only to subordinate CAs, with the exception of the Thawte Server CA which issues end-user Subscriber certificates. Thawte CA certificate requests are created and approved by authorized ***thawte*** personnel through a controlled process that requires the participation of multiple trusted individuals.

4.2 Certificate Issuance

4.2.1 Issuance of End-User Subscriber Certificates

After a Certificate Applicant submits a Certificate Application, ***thawte*** (*See* CPS § 4.1.1) attempts to confirm the information in the Certificate Application (other than Non-Verified Subscriber Information) pursuant to CPS §§ 3.1.8.1, 3.1.9. Upon successful performance of all required authentication procedures pursuant to CPS § 3.1, ***thawte*** approves the Certificate Application and issues a Certificate based on the information in the Certificate Application. If authentication is unsuccessful, ***thawte*** denies the Certificate Application. The procedures of this section are also used for the issuance of Certificates in connection with the submission of a request to replace (i.e., renew or rekey) a Certificate.

4.2.2 Issuance of CA Certificates

See CPS §4.1.2.

4.3 Certificate Acceptance

Upon Certificate generation, ***thawte*** notifies Subscribers that their Certificates are available and notifies them of the means for obtaining such Certificates.

Upon issuance, Certificates are made available to end-user Subscribers, either by allowing them to download them from a web site (such as their Certificate Status Page) or via a message sent to the Subscriber containing the Certificate. For example, ***thawte*** may send the Subscriber a PIN, which the Subscriber enters into an enrollment web page to obtain the Certificate. The Certificate may also be sent to the Subscriber in an e-mail message. Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

4.4.1.1 Circumstances for Revoking End-User Subscriber Certificates

An end-user Subscriber Certificate is revoked if:

- ***thawte***, a Customer, or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key,
- ***thawte*** or a Customer has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
- The Subscriber Agreement with the Subscriber has been terminated,
- ***thawte*** or a Customer has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the CPS,
- The Certificate (other than a Personal E-mail Certificate) was issued to a person other than the one named as the Subject of the Certificate,
- the Certificate (other than a Personal E-mail Certificate) was issued without the authorization of the person named as the Subject of such Certificate,
- ***thawte*** or a Customer has reason to believe that a material fact in the Certificate Application is false,
- ***thawte*** or a Customer determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,
- In the case of High Assurance organizational Certificates, the Subscriber's organization name changes,

- The information within the Certificate, other than Nonverified Subscriber Information, is incorrect or has changed, or
- The Subscriber requests revocation of the Certificate in accordance with CPS § 3.4.
- The continued use of that certificate is harmful to the ***thawte*** trust infrastructure.

thawte Subscriber Agreements require end-user Subscribers to immediately notify ***thawte*** of a known or suspected compromise of its private key in accordance with the procedures in CPS § 4.4.3.1.

4.4.1.2 Circumstances for Revoking CA Certificates

thawte will revoke CA Certificates if:

- ***thawte*** discovers or has reason to believe that there has been a compromise of the CA private key,
- ***thawte*** discovers or has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the CPS, the Certificate was issued to an entity other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the entity named as the Subject of such Certificate,
- ***thawte*** determines that a material prerequisite to Certificate issuance was neither satisfied nor waived, or
- Authorized ***thawte*** personnel request revocation of the Certificate.

4.4.2 Who Can Request Revocation

4.4.2.1 Who Can Request Revocation of an End-User Subscriber Certificate

The following entities may request revocation of an end-user Subscriber Certificate:

- ***thawte*** or the SPKI Customer that approved the Subscriber's Certificate Application may request the revocation of any end-user Subscriber Certificate in accordance with CPS § 4.4.1.1.
- Individual Subscribers may request revocation of their own individual Certificates.
- In the case of organizational Certificates, only a duly authorized representative of the organization is entitled to request the revocation of Certificates issued to the organization.

4.4.2.2 Who Can Request Revocation of a CA Certificate

Only ***thawte*** is entitled to request or initiate the revocation of the Certificates issued to its own CAs. ***thawte*** may initiate the revocation of any CA Certificate in accordance with CPS § 4.4.1.2.

4.4.3 Procedure for Revocation Request

4.4.3.1 Procedure for Requesting Revocation of an End-User Subscriber Certificate

An end-user Subscriber requesting revocation is required to communicate the request to ***thawte***, who in turn will promptly initiate revocation of the Certificate. Communication of such revocation requests shall be in accordance with CPS § 3.4.

4.4.3.2 Procedure for Requesting Revocation of a CA Certificate

Thawte CA certificate revocation requests may be made and approved by authorized ***thawte*** personnel through a controlled process that requires the participation of multiple trusted individuals.

4.4.4 Revocation Request Grace Period

Revocation requests must be submitted as promptly as possible within a commercially reasonable period of time.

4.4.5 Circumstances for Suspension

thawte does not offer suspension services for CA or end-user Subscriber Certificates.

4.4.6 Who Can Request Suspension

Not applicable.

4.4.7 Procedure for Suspension Request

Not applicable.

4.4.8 Limits on Suspension Period

Not applicable.

4.4.9 CRL Issuance Frequency

thawte publishes CRLs showing the revocation of ***thawte*** Certificates in accordance with the schedule in Table 20 below:

CA Type	*CA Name*	*CRL Issuance Frequency*
Root CAs (Non-Issuing)	Thawte Personal Freemail CA thawte Primary Root CA	At least quarterly and upon Sub-CA certificate revocation
Root CAs (Issuing CAs)	Thawte Server CA Thawte Premium Server CA	At least daily

CA Type	*CA Name*	*CRL Issuance Frequency*
Inactive Root CAs	Thawte Personal Premium CA Thawte Personal Basic CA Thawte Time Stamping CA	Requirements to be determined upon CA activation
Subordinate Issuing CAs	Thawte Personal Freemail Issuing CA Thawte Code Signing CAthawte Extended Validation SSL CA thawte Extended Validation SSL SGC CA	At least daily

Table 20 – CRL Issuance Frequency

Expired Certificates are removed from the CRL after the Certificates' expiration.

4.4.10 Certificate Revocation List Checking Requirements

Not applicable

4.4.11 On-Line Revocation/Status Checking Availability

Not applicable

4.4.12 On-Line Revocation Checking Requirements

In order for on-line revocation checking to be possible, the certificate needs to be issued with the CDP extension.

4.4.13 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.15 Special Requirements Regarding Key Compromise

In addition to the procedures described in CPS § 4.4.9 – 4.4.10, ***thawte*** uses commercially reasonable efforts to notify potential Relying Parties if ***thawte*** discovers, or has reason to believe, that there has been a Compromise of the private key of a Thawte CA.

4.5 Security Audit Procedures

4.5.1 Types of Events Recorded

thawte manually or automatically logs the following significant events:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device life cycle management events.
- CA and Subscriber certificate life cycle management events, including:
  - Certificate Applications, renewal, rekey, and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of Certificates and CRLs.
- Security-related events including:
- Successful and unsuccessful PKI system access attempts
- PKI and security system actions performed by ***thawte*** personnel
- Security profile changes
- System crashes, hardware failures and other anomalies
- Firewall and router activity
- CA facility visitor entry/exit.

Log entries include the following elements:

- Date and time of the entry
- Serial or sequence number of entry, for automatic journal entries
- Identity of the entity making the journal entry
- Kind of entry.

thawte RAs log Certificate Application information including:

- Kind of identification document(s) presented by the Certificate Applicant
- Record of unique identification data, numbers, or a combination thereof (e.g., Certificate Applicant's drivers license number) of identification documents, if applicable
- Storage location of copies of applications and identification documents
- Identity of entity accepting the application
- Method used to validate identification documents, if any
- Name of submitting RA, if applicable.

4.5.2 Frequency of Processing Log

Audit logs are examined periodically for significant security and operational events. In addition, ***thawte*** reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within Thawte CA and RA systems.

4.5.3 Retention Period for Audit Log

Audit logs are retained onsite at least two (2) months after processing and thereafter archived in accordance with CPS § 4.6.2.

4.5.4 Protection of Audit Log

Electronic and manual audit log files are protected from unauthorized viewing, modification, deletion, or other tampering through the use of physical and logical access controls.

4.5.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed weekly.

4.5.6 Audit Collection System

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by ***thawte*** personnel.

4.5.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

4.5.8 Vulnerability Assessments

thawte performs vulnerability assessments of its CA and RA systems on a periodic basis. Policies, practices and system configurations are updated, as appropriate, based on the results of such assessments.

4.6 Records Archival

4.6.1 Types of Events Recorded

In addition to the audit logs specified in CPS § 4.5, ***thawte*** maintains records that include documentation of:

- ***thawte's*** compliance with the CPS and other obligations under its agreements with their Subscribers, and
- actions and information that are material to each Certificate Application and to the creation, issuance, use, revocation, expiration, and rekey or renewal of all Certificates issued by ***thawte***.

thawte's records of Certificate life cycle events include:

- the identity of the Subscriber named in each Certificate (except for Freemail Certificates, for which only a record of the Subscriber's unambiguous name is maintained),

- the identity of persons requesting Certificate revocation (except for Freemail Certificates, for which only a record of the Subscriber's unambiguous name is maintained),
- other facts represented in the Certificate,
- time stamps, and
- certain foreseeable material facts related to issuing Certificates including, but not limited to, information relevant to successful completion of a Compliance Audit under CPS § 2.7.

Records may be maintained electronically or in hard copy, provided that such records are accurately and completely indexed, stored, preserved, and reproduced.

4.6.2 Retention Period for Archive

Records associated with Certificates are retained for at least 5 years following the date the Certificate expires or is revoked. If necessary, ***thawte*** may implement longer retention periods in order to comply with applicable laws.

4.6.3 Protection of Archive

thawte protects its archived records compiled under CPS § 4.6.1 so that only authorized Trusted Persons are permitted to access archived data. Electronically archived data is protected against unauthorized viewing, modification, deletion, or other tampering through the implementation of appropriate physical and logical access controls. The media holding the archive data and the applications required to process the archive data are maintained to ensure that the archived data can be accessed for the time period set forth in CPS § 4.6.2.

4.6.4 Archive Backup Procedures

thawte incrementally backs up electronic archives of its issued Certificate information on a daily basis and performs full backups on a weekly basis. Copies of paper-based records compiled under CPS § 4.6.1 are maintained in an off-site facility in accordance with CPS § 4.8.

4.6.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries contain time and date information. It should be noted that such time information is not cryptographic-based.

4.6.6 Procedures to Obtain and Verify Archive Information

See CPS § 4.6.3.

4.7 Key Changeover

thawte CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in CPS § 6.3.2. ***thawte*** CA Certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services in accordance with CPS § 6.1.

Prior to the expiration of the CA Certificate for a Superior CA, key changeover procedures are enacted to facilitate a smooth transition for entities within the Superior CA's hierarchy from the old Superior CA key pair to new CA key pair(s). ***thawte's*** CA key changeover process requires that:

- A Superior CA ceases to issue new Subordinate CA Certificates no later than 60 days before the point in time ("Stop Issuance Date") where the remaining lifetime of the Superior CA key pair equals the approved Certificate Validity Period for the specific type(s) of Certificates issued by Subordinate CAs in the Superior CA's hierarchy.
- Upon successful validation of Subordinate CA (or end-user Subscriber) Certificate requests received after the "Stop Issuance Date," Certificates will be signed with a new CA key pair.
- The Superior CA continues to issue CRLs signed with the original Superior CA private key until the expiration date of the last Certificate issued using the original key pair has been reached.

4.8 Disaster Recovery and Key Compromise

thawte has implemented a robust combination of physical, logical, and procedural controls to minimize the risk and potential impact of a key compromise or disaster. In addition, ***thawte*** has implemented disaster recovery procedures described in CPS § 4.8.2 and Key Compromise response procedures described in CPS § 4.8.3. ***thawte's*** compromise and disaster recovery procedures have been developed to minimize the potential impact of such an occurrence and restore ***thawte's*** operations within a commercially reasonable period of time.

4.8.1 Corruption of Computing Resources, Software, and/or Data

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to ***thawte*** Security and ***thawte's*** incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, ***thawte's*** key compromise or disaster recovery procedures will be enacted.

4.8.2 Disaster Recovery

thawte has implemented a disaster recovery site separate from ***thawte's*** principal secure facilities. ***thawte*** has developed and implemented a disaster recovery plan to

mitigate the effects of any kind of natural or man-made disaster. This plan is regularly tested, verified, and updated to be operational in the event of a disaster.

Disaster recovery plans address the restoration of information systems, services and key business functions. ***thawte's*** disaster recovery site has implemented the physical security protections and operational controls required by ***thawte's*** security policies to provide for a secure and sound backup operational setup. In the event of a natural or man-made disaster requiring temporary or permanent cessation of operations from ***thawte's*** primary facilities, ***thawte's*** disaster recovery process is initiated by the ***thawte*** Emergency Response Team.

thawte has the capability to restore or recover operations within twenty four (24) hours following a disaster with, at a minimum, support for the following functions: Certificate revocation, publication of certificate status information, and Certificate issuance. ***thawte 's*** disaster recovery plan has been designed to provide full recovery within one week following disaster occurring at ***thawte's*** primary sites. Where possible, operations are resumed at ***thawte's*** primary sites as soon as possible following a major disaster.

thawte maintains redundant hardware and backups of its CA and RA system software at its disaster recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with CPS § 6.2.4. ***thawte's*** disaster recovery database is synchronized regularly with the production database. ***thawte's*** disaster recovery equipment is protected by physical security protections comparable to the physical security tiers specified in CPS § 5.1.1.

thawte maintains offsite backups of important CA information for ***thawte*** CAs. Such information includes, but is not limited to Certificate Application data, database records for all Certificates issued, and system configuration information.

4.8.3 Key Compromise

Upon the suspected or known Compromise of a ***thawte*** CA private key, ***thawte*** and VeriSign's Key Compromise Response procedures are enacted by the VeriSign/ ***thawte*** Compromise Incident Response Team. This team, which includes VeriSign and ***thawte*** Security, Cryptographic Business Operations, Production Services personnel, and other VeriSign and ***thawte*** management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from VeriSign and ***thawte*** executive management.

If CA Certificate revocation is required, the following procedures are performed:

- The Certificate's revoked status is communicated to Relying Parties through the ***thawte*** repository in accordance with CPS § 4.4.9,
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected ***thawte*** PKI Participants, and

- ***thawte*** will generate a new key pair in accordance with CPS § 4.7, except where the CA is being terminated in accordance with CPS § 4.9.

4.9 CA Termination

In the event that it is necessary for a ***thawte*** CA to cease operation, ***thawte*** makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, ***thawte*** will develop a termination plan to minimize disruption to Customers, Subscribers, and Relying Parties.

Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA,
- Handling the cost of such notice,
- The preservation of the CA's archives and records for the time periods required in CPS § 4.6,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs,
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,
- The payment of compensation (if necessary) to Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's private key and the hardware tokens containing such private key, and
- Provisions needed for the transition of the CA's services to a successor CA.

5. Physical, Procedural, and Personnel Security Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

thawte's Certificate and CRL signing systems are housed in secure facilities in Mountain View, California, USA that are protected by multiple tiers of physical security, video monitoring, and two factor authentication including biometrics. Online Cryptographic Signing Units ("CSUs") are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with VeriSign and ***thawte's*** segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes. Progressively restrictive physical access privileges control access to each tier.

thawte's certificate management systems are housed in secure facilities in the United States that are protected by multiple tiers of physical security, video monitoring, and dual access.

thawte's RA operations are conducted within ***thawte*** facilities on in the United States and in South Africa that are protected by multiple tiers of physical security including proximity badge access.

thawte also maintains disaster recovery facilities in the United States for its CA operations. ***thawte's*** disaster recovery facilities are protected by multiple tiers of physical security comparable to those of ***thawte's*** primary facilities.

5.1.2 Physical Access

See CPS § 5.1.1.

5.1.3 Power and Air Conditioning

thawte's secure facilities are equipped with primary and backup:

- power systems to ensure continuous, uninterrupted access to electric power and
- heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

thawte has taken reasonable precautions to minimize the impact of water exposure to ***thawte*** systems.

5.1.5 Fire Prevention and Protection

thawte has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. ***thawte's*** fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within ***thawte*** facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal.

Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with ***thawte's*** normal waste disposal requirements.

5.1.8 Off-Site Backup

thawte performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using a bonded third party storage facility and ***thawte's*** disaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all ***thawte*** employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- or the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- customer service personnel,
- cryptographic business operations personnel,
- security personnel,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

thawte considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements of CPS § 5.3.

5.2.2 Number of Persons Required Per Task

thawte maintains a policy and rigorous control procedures to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (e.g., CSUs) and associated keying material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold "Secret Shares" and vice versa. Requirements for CA private key activation data and Secret Shares are specified in CPS § 6.2.7.

Other operations such as the validation and issuance of High Assurance Certificates require the participation of at least two Trusted Persons.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing ***thawte*** HR or security functions and a check of well-recognized forms of identification (e.g., passports and driver's licenses). Identity is further confirmed through the background checking procedures in CPS §§ 5.3.1, 5.3.2.

thawte ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities;
- issued electronic credentials to access and perform specific functions on Thawte CA, RA, or other IT systems.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Background checks are repeated at least every 5 years for personnel holding Trusted Positions.

5.3.2 Background Check Procedures

Prior to commencement of employment in a Trusted Role, ***thawte*** conducts background checks which include the following:

- confirmation of previous employment,
- check of professional reference,
- confirmation of the highest or most relevant educational degree obtained,
- search of criminal records (local, state or provincial, and national),

- check of credit/financial records,
- search of driver's license records, and
- search of Social Security Administration/National Identification/Passport (or similar) records.

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, ***thawte*** will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include the following:

- Misrepresentations made by the candidate or Trusted Person,
- Highly unfavorable or unreliable personal references,
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

Reports containing such information are evaluated by HR and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

5.3.3 Training Requirements

thawte provides its personnel with training upon hire and the requisite on-the-job training needed for personnel to perform their job responsibilities competently and satisfactorily. ***thawte*** periodically reviews and enhances its training programs as necessary.

thawte's training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts,
- Job responsibilities,
- Thawte security and operational policies and procedures,
- Use and operation of deployed hardware and software,
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

thawte provides refresher training and updates to its personnel to the extent required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily. Periodic security awareness training is provided on an ongoing basis.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of ***thawte*** policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Contracting Personnel Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a ***thawte*** employees in a comparable position.

Independent contractors and consultants who have not completed the background check procedures specified in CPS § 5.3.2 are permitted access to ***thawte's*** secure facilities only to the extent they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation Supplied to Personnel

thawte personnel involved in the operation of ***thawte's*** PKI services are required to read this CPS and the ***thawte*** Security Policy. ***thawte*** provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. For Thawte Root CAs and Issuing CAs, the cryptographic modules used for key generation meet the requirements of at least FIPS 140-1 level 2.

All CA key pairs are generated in pre-planned Key Generation Ceremonies. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by ***thawte*** Management.

Generation of end-user Subscriber key pairs is performed by the Subscriber, or authorized representative of the subscriber such as a Web hosting company.

For Code Signing, Freemail, and Freemail Web of Trust Certificates, the Subscriber uses a cryptographic module provided with their browser software for key generation. For server Certificates, the end-user Subscriber uses a separate key generation utility (e.g., the web server software's key generation utility or a code signing key generation utility).

6.1.2 Private Key Delivery to Entity

End-user Subscriber key pairs are generated by the end-user Subscriber. As a result, private key delivery to a Subscriber is not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

End-user Subscribers submit their public keys to ***thawte*** for certification electronically through the use of a PKCS#10 or PKCS#7 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL).

6.1.4 CA Public Key Delivery to Users

thawte makes the CA Certificates for Root CAs available to Subscribers and Relying Parties through their inclusion in Microsoft, Netscape and other web browser software. As new Root CA Certificates are generated, ***thawte*** provides such new Certificates to the browser manufacturers for inclusion in new browser releases and updates. In addition, ***thawte*** generally provides the full certificate chain (including the issuing CA and any superior CAs in the chain) to the end-user Subscriber upon Certificate issuance.

6.1.5 Key Sizes

Thawte CA key pairs are at least 1024 bit RSA. ***thawte*** recommends that end-user Subscribers generate 1024 bit RSA key pairs, but currently permits the use of 512 bit RSA key pairs to support certain legacy applications and web servers.

6.1.6 Public Key Parameters Generation

Not applicable.

6.1.7 Parameter Quality Checking

Not applicable.

6.1.8 Hardware/Software Key Generation

thawte generates its CA pairs keys in appropriate hardware cryptographic modules in accordance with CPS § 6.2.1. End-user Subscriber key pairs may be generated in hardware or software.

6.1.9 Key Usage Purposes

thawte utilizes the Key Usage extension as specified in CPS § 7.1.2.

6.2 Private Key Protection

thawte has implemented a combination of physical, logical, and procedural controls to ensure the security of Thawte CA private keys. Logical and procedural controls are described in CPS §§ 6.5, 6.6. Physical access controls are described in CPS § 5.1. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Standards for Cryptographic Modules

For Thawte CA key pair generation and CA private key storage, ***thawte*** uses hardware cryptographic modules that meet the requirements of at least FIPS 140-1 level 2.

6.2.2 Private Key (m out of n) Multi-Person Control

thawte has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. ***thawte*** uses "Secret Sharing" to split the activation data needed to make use of a CA private key into separate parts called "Secret Shares" which are held by trained and trusted individuals called "Shareholders." A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module.

The threshold number of shares needed to sign a CA certificate is 3. It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with this CPS. Secret Shares are protected in accordance with CPS § 6.4.2.

6.2.3 Private Key Escrow

thawte does not escrow CA or end-user Subscriber private keys with any third party for purposes of access by law enforcement.

6.2.4 Private Key Backup

thawte creates backup copies of CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for CA private key storage meet the requirements of CPS § 6.2.1. CA private keys are copied to backup hardware cryptographic modules in accordance with CPS § 6.2.6. Modules containing onsite backup copies of CA private keys are subject to the requirements of CPS §§ 5.1, 6.2.1. Modules containing disaster recovery copies of CA private keys are subject to the requirements of CPS § 4.8.2.

thawte does not generate, store, backup or archive end-user Subscriber private keys.

6.2.5 Private Key Archival

When Thawte CA key pairs reach the end of their validity period, such CA key pairs will be archived for a period of at least 5 years. Archived CA key pairs will be securely stored using hardware cryptographic modules that meet the requirements of CPS § 6.2.1. Procedural controls prevent archived CA key pairs from being returned to production use. Upon the end of the archive period, archived CA private keys will be securely destroyed in accordance with CPS § 6.2.9.

thawte does not archive copies of Subscriber private keys.

6.2.6 Private Key Entry into Cryptographic Module

thawte generates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, ***thawte*** makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

6.2.7 Method of Activating Private Key

thawte PKI Participants are required to protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.7.1 End-User Subscriber Private Keys

This section describes the ***thawte*** requirements for protecting activation data for end-user Subscribers' private keys. In addition, Subscribers have the option of using enhanced private key protection mechanisms available today including the use of smart cards, biometric access devices, and other hardware tokens to store private keys. The use of two factor authentication mechanisms (e.g., token and pass phrase, biometric and token, or biometric and pass phrase) is encouraged.

6.2.7.1.1 Low Assurance Certificates

The ***thawte*** requirements for Low Assurance private key protection is for Subscribers to take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization. In addition, ***thawte*** recommends that Subscribers use a password in accordance with CPS § 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password.

6.2.7.1.2 High Assurance Certificates and High Assurance with extended validation Certificates

The ***thawte*** requirements for High Assurance and High Assurance with extended validation private key protection is for Subscribers to:

- Use a smart card, other cryptographic hardware device, biometric access device, password, or security of equivalent strength to authenticate the Subscriber before the activation of the private key; and
- Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation or server and its associated private key without the Subscriber's authorization.

Use of a password along with a smart card, other cryptographic hardware device, or biometric access device in accordance with CPS § 6.4.1 is recommended. When deactivated, private keys shall be kept in encrypted form only.

6.2.7.2 CA Private Keys

Thawte CA private keys are activated by a threshold number of Shareholders supplying their activation data (tokens or pass phrases) in accordance with CPS § 6.2. For ***thawte's*** offline CAs, the CA private key is activated for one session (e.g., for the certification of a Subordinate CA or an instance where a Root CA signs a CRL) after which it is deactivated and the module is returned to secure storage. For ***thawte's*** online CAs, the CA private key is activated for an indefinite period and the module remains online in the production data center until the CA is taken offline (e.g., for system maintenance). ***thawte*** Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

6.2.8 Method of Deactivating Private Key

Thawte CA private keys are deactivated upon removal from the token reader.

End-user Subscriber private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader

depending upon the authentication mechanism employed by the user. In all cases, end-user Subscribers have an obligation to adequately protect their private key(s) in accordance with CPS §§ 2.1.3, 6.4.1.

6.2.9 Method of Destroying Private Key

At the conclusion of a Thawte CA's operational lifetime, one or more copies of the CA private key are archived in accordance with CPS § 6.2.5. Remaining copies of the CA private key are securely destroyed. In addition, archived CA private keys are securely destroyed at the conclusion of their archive periods. CA key destruction activities require the participation of multiple trusted individuals.

Where required, ***thawte*** destroys CA private keys in a manner that reasonably ensures that there are no residual remains of the key that could lead to the reconstruction of the key. ***thawte*** utilizes the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Thawte CA and end-user Subscriber Certificates are backed up and archived as part of ***thawte's*** routine backup procedures.

6.3.2 Usage Periods for the Public and Private Keys

The Operational Period of a Certificate ends upon its expiration or revocation. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that private keys may continue to be used for decryption and public keys may continue to be used for signature verification. The maximum Operational Periods for ***thawte*** Certificates for Certificates issued on or after the effective date of this CPS are set forth in Table 22 below.

In addition, Thawte CAs stop issuing new Certificates at an appropriate date prior to the expiration of the CAs Certificate such that no Certificate issued by a Subordinate CA expires after the expiration of any Superior CA Certificates.

Certificate Issued By:	*Operational Period*
Root CAs	Up to 25 years
Root CA to Sub-CA	Up to 10 years
CA to end-user Subscriber	Up to 2 years

Table 22 – Certificate Operational Periods

thawte PKI Participants shall cease all use of their key pairs after their usage periods have expired.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data (Secret Shares) used to protect tokens containing Thawte CA private keys is generated in accordance with the requirements of CPS § 6.2.2. The creation and distribution of Secret Shares is logged.

thawte strongly recommends that end-user Subscribers select strong passwords to protect their private keys. ***thawte*** also recommends the use of two factor authentication mechanisms (e.g., token and pass phrase, biometric and token, or biometric and pass phrase) for private key activation.

6.4.2 Activation Data Protection

thawte Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

thawte recommends that end-user Subscribers store their private keys in encrypted form and protect their private keys through the use of a hardware token and/or strong pass phrase. The use of two factor authentication mechanisms (e.g., token and pass phrase, biometric and token, or biometric and pass phrase) is encouraged.

6.4.3 Other Aspects of Activation Data

See CPS §§ 6.4.1, 6.4.2.

6.5 Computer Security Controls

thawte performs all CA and RA functions using Trustworthy Systems that meet the requirements of ***thawte's*** security policy.

6.5.1 Specific Computer Security Technical Requirements

thawte ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access. In addition, ***thawte*** limits access to production servers to those individuals with a valid business reason for such access. ***thawte's*** production networks are logically separated from other components. This separation prevents network access except through defined application processes.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by ***thawte*** and VeriSign in accordance with ***thawte*** and VeriSign systems development and change management standards.

6.6.2 Security Management Controls

thawte has mechanisms and/or policies in place to control and monitor the configuration of its CA systems.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

thawte performs all its CA and RA functions using networks secured in accordance with ***thawte's*** security policy to prevent unauthorized access and other malicious activity. ***thawte*** protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 Cryptographic Module Engineering Controls

Cryptographic modules used by ***thawte*** meet the requirements specified in CPS § 6.2.1.

7. Certificate and CRL Profile

7.1 Certificate Profile

7.1.1 Version

thawte issues X.509 version 3 certificates which contain the standard fields specified in Table 23 below:

Field	***Value or Value constraint***	
Version	Version 3	
Serial Number	Unique value per Issuer DN	
Signature Algorithm	md5RSA or sha1RSA: Certificate signatures produced using these algorithms shall comply with RFC 3279. Use of sha-1WithRSAEncryption shall be given strong preference over md5WithRSAEncryption.	
Issuer	Common Name (CN) =	CA Name

Field	*Value or Value constraint*	
Distinguished Name	Organizational Unit (OU) =	"Certification Services Division" or "Thawte Certification"
	Organization (O) =	"Thawte Consulting cc" or "Thawte Consulting" or "Thawte"
	Locality (L) =	"Cape Town" except for the Thawte Timestamping CA which includes "Durbanville"
	State or Province (P) =	"Western Cape"
	Country (C) =	"ZA"
	E-Mail (E) =	Used for Root CAs only (excluding the Thawte Timestamping CA). Contains a contact e-mail address for the CA.
Valid From	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 2459.	
Valid To	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 2459. The validity period will be set in accordance with the constraints specified in CPS § 6.3.2.	
Subject Distinguished Name	Populated in accordance with CPS §3.1.1.	
Subject Public Key	Encoded in accordance with RFC 2459 using the RSA algorithm and key lengths of at least 512 bits in accordance with CPS § 6.1.5 (except for SGC SuperCerts which require a key length of at least 1024 bits).	
Signature	Generated and encoded in accordance with RFC 2459.	

Table 23 – Certificate Profile Basic Fields

SSL Web Server Certificates with EV standard certificate profiles are discussed in Section 6 of Appendix A3 to this CPS."

7.1.2 Certificate Extensions

thawte populates Certificates with the extensions specified in CPS §§ 7.1.2.1-7.1.2.8. Other extensions may be supported in the future.

7.1.2.1 Root CA Certificates

Thawte Root CA certificates include the extensions specified in Table 24 below:

Extension	*Value or Value Constraint*	*Criticality*
Basic Constraints	Subject Type=CA Path Length Constraint=None	Critical

Table 24 – Root CA Certificate Extensions

7.1.2.2 Subordinate CA Certificates

thawte Subordinate CA certificates include the extensions specified in Table 25 below:

Extension	*Value or Value Constraint*	*Criticality*
Key Usage	Certificate Signing Off-line CRL Signing CRL Signing(06)	Non-Critical
Basic Constraints	Subject Type=CA Path Length Constraint=0	Critical
Subject Alternative Name	Contains a reference to the CA key	Non-Critical

Table 25 – Subordinate CA Certificate Extensions

7.1.2.3 SSL Web Server Certificates

thawte SSL Web Server certificates include the extensions specified in Table 26 below:

Extension	*Value or Value Constraint*	*Criticality*
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Critical
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	Non-Critical
CRL Distribution Points	http://crl.thawte.com/ThawtePremiumServerCA.crl	Non-Critical
Authority information Access	http://ocsp.thawte.com	Non-Critical

Table 26 –thawte SSL Web Server Certificate Extensions

7.1.2.4 SSL123 Certificates

thawte SSL123 certificates include the extensions specified in Table 27 below:

Extension	*Value or Value Constraint*	*Criticality*
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Critical
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	Non-Critical
Authority information Access	http://ocsp.thawte.com	Non-Critical

Table 27 – thawte SSL123 Certificate Extensions

7.1.2.5 SGC SuperCerts

thawte SGC SuperCerts include the extensions specified in Table 28 below:

Extension	*Value or Value Constraint*	*Criticality*
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Critical
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Netscape SGC: Unknown Key Usage (2.16.840.1.113730.4.1) In addition, Certificates issued to Microsoft IIS web servers include: Microsoft Fast SGC (1.3.6.1.4.1.311.10.3.3)	Non-Critical
CRL Distribution Points	http://crl.thawte.com/ThawteSGCCA.crl	Non-Critical
Authority information Access	http://ocsp.thawte.com	Non-Critical

Table 28 –thawte SGC SuperCert Certificate Extensions

7.1.2.6 SSL Wildcard Certificates

thawte SSL Wildcard Certificates include the extensions specified in Table 26 below:

Extension	*Value or Value Constraint*	*Criticality*
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Critical
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	Non-Critical
CRL Distribution Points	http://crl.thawte.com/ThawtePremiumServerCA.crl	Non-Critical
Authority information Access	http://ocsp.thawte.com	Non-Critical

Table 26 –thawte SSL Web Server Certificate Extensions

7.1.2.7. SSL Web Server Certificates with EV

Web Server Certificates with EV certificate extension requirements are discussed in Section 6 of Appendix A3 to this CPS.

7.1.2.8. Code Signing Certificates

thawte Code Signing certificates include the extensions specified in Table 29 below:

Extension	*Value or Value Constraint*	*Criticality*
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Critical
Enhanced Key Usage	Code Signing(1.3.6.1.5.5.7.3.3) In addition, Certificates issued for Microsoft code signing include: Microsoft Code Signing (1.3.6.1.4.1.311.2.1.22)	Non-Critical
NetscapeCertType	Signature(10)	Non-Critical
Key Usage Restriction	Cert PolicyId=1.3.6.1.4.1.311.2.1.22 Restricted Key Usage=Digital Signature(80)	Non-Critical
Subject Alternative Name	DNS Name=domain name of Subscriber's web site	Non-Critical
CRL Distribution Points	http://crl.thawte.com/ThawteCodeSigningCA.crl	Non-Critical

Table 29 –thawte Code Signing Certificate Extensions

7.1.2.9. Personal E-mail and Freemail Web of Trust Certificates

For ***thawte*** Personal E-mail (Freemail) and Freemail Web of Trust Certificates, Subscribers have the choice of accepting ***thawte's*** default extensions or configuring their certificate extensions. All ***thawte*** Personal E-mail and Freemail Web of Trust Certificates include the extensions specified in Table 30 below:

Extension	*Value or Value Constraint*	*Criticality*
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Critical
Subject Alternative Name	RFC822 Name=Subscriber's e-mail address	Non-Critical

Table 30 – Standard Freemail and Freemail Web of Trust Certificate Extensions

In addition, the Subscriber may choose to include the extensions specified in Table 31 below:

Extension	*Optional Values*	*Criticality*
Key Usage	Digital Signature Non-Repudiation Key Encipherment Data Encipherment Key Agreement Encipher Only Decipher Only	Critical
Netscape Cert Type	SSL Client Authentication SMIME	Non-Critical

Table 31 – Optional Freemail and Freemail Web of Trust Certificate Extensions

7.1.3 Algorithm Object Identifiers

thawte Certificates are signed with md5RSA or sha1RSA Certificate signatures produced using these algorithms shall comply with RFC 3279. Use of sha-1WithRSAEncryption shall be given strong preference over md5WithRSAEncryption.

7.1.4 Name Forms

thawte Certificates are populated with an Issuer and Subject Distinguished Name in accordance with CPS § 3.1.1.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

No stipulation.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.2 CRL Profile

thawte issues CRLs that conform to RFC 2459. At a minimum, ***thawte*** CRLs contain the basic fields and contents specified in Table 32 below:

Field	*Value or Value constraint*
Version	*See* CPS §7.2.1.
Signature Algorithm	Algorithm used to sign the CRL. Thawte CRLs are signed using md5RSA or sha1RSA (OID: 1.2.840.113549.1.1.4) in accordance with RFC 2459.
Issuer	Entity who has signed and issued the CRL. The CRL Issuer Name is in accordance with the Issuer Distinguished Name requirements specified in CPS § 3.1.1.
Effective	Issue date of the CRL. Thawte CRLs are effective upon issuance.

Field	*Value or Value constraint*
Date	
Next Update	Date by which the next CRL will be issued. The Next Update date for Thawte CRLs is set as follows: 3 months from the Effective Date for Thawte Non-Issuing Root CAs and 14 days from the Effective Date for other Thawte CAs. CRL issuance frequency is in accordance with the requirements of CPS § 4.4.9.
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

Table 32 – CRL Profile Basic Fields

7.2.1 Version Number(s)

thawte currently issues X.509 Version 1 CRLs.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

8. Specification Administration

8.1 Specification Change Procedures

Amendments to this CPS shall be made by the VeriSign/***thawte*** Practices Development group. Amendments shall either be in the form of a document containing an amended form of the CPS or an update. Amended versions or updates shall be linked to the Practices Updates and Notices section of the ***thawte*** Repository located at: **https://www.thawte.com/repository** Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

8.1.1 Items that Can Change Without Notification

thawte reserves the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. ***thawte's*** decision to designate amendments as material or non-material shall be within ***thawte's*** sole discretion.

8.1.2 Items that Can Change with Notification

thawte shall make material amendments to the CPS in accordance with CPS §§ 8.1.2.1-8.1.2.4.

8.1.2.1 List of Items

Material amendments are those changes that ***thawte***, under CPS § 8.1.1, considers to be material.

8.1.2.2 Notification Mechanism

The VeriSign/***thawte*** Practices Development group will post proposed amendments to the CPS in the Practices Updates and Notices section of the ***thawte*** Repository, which is located at: **https://www.thawte.com/repository**. ***thawte*** solicits proposed amendments to the CPS from other ***thawte*** PKI Participants. If ***thawte*** considers such an amendment desirable and proposes to implement the amendment, ***thawte*** shall provide notice of such amendment in accordance with this section.

Notwithstanding anything in the CPS to the contrary, if ***thawte*** believes that material amendments to the CPS are necessary immediately to stop or prevent a breach of the security of any portion of the ***thawte*** PKI, ***thawte*** shall be entitled to make such amendments by publication in the ***thawte*** Repository. Such amendments will be effective immediately upon publication.

8.1.2.3 Comment Period

Except as noted under CPS § 8.1.2.2, the comment period for any material amendments to the CPS shall be fifteen (15) days, starting on the date on which the amendments are posted on the ***thawte*** Repository. Any ***thawte*** PKI Participant shall be entitled to file comments with the VeriSign/***thawte*** Practices Development group up until the end of the comment period.

8.1.2.4 Mechanism to Handle Comments

The VeriSign/***thawte*** Practices Development group will consider any comments on the proposed amendments. ***thawte*** will either (a) allow the proposed amendments to become effective without amendment, (b) amend the proposed amendments and republish them as a new amendment under CPS § 8.1.2.2, or (c) withdraw the proposed amendments. ***thawte*** is entitled to withdraw proposed amendments by providing notice in the Practices Updates and Notices section of the ***thawte*** Repository. Unless proposed amendments are amended or withdrawn, they shall become effective upon the expiration of the comment period under CPS § 8.1.2.3.

8.2 Publication and Notification Procedures

This CPS is published in electronic form within the ***thawte*** Repository at **https://www.thawte.com/cps**. The CPS is available in the ***thawte*** Repository in Adobe Acrobat format. ***thawte*** also makes the CPS available upon request sent to **CPS-requests@thawte.com**. The CPS is available in paper form from the VeriSign/***thawte*** Practices Development group upon requests sent to: VeriSign, Inc., 487 East Middlefield Road, Mountain View, CA 94043, USA, Attn: Practices Development – Thawte CPS.

8.3 CPS Approval Procedures

See CPS § 8.1.

9. Acronyms and Definitions

9.1 Table of Acronyms

Acronym	*Term*
ANSI	The American National Standards Institute.
BIS	The United States Bureau of Industry and Science of the United States Department of Commerce.
BXA	The United States Bureau of Export Administration of the United States Department of Commerce.
CA	Certification Authority.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
EV	Extended Validation
FIPS	United States Federal Information Processing Standards.
ICC	International Chamber of Commerce.
OFAC	Office of Foreign Assets Control
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
RA	Registration Authority.
RFC	Request for comment.
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.

9.2 Definitions

Term	*Definition*
Administrator	A Trusted Person that performs validation and other CA or RA functions at ***thawte***.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.

Term	*Definition*
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the ***thawte*** PKI.
Certification Practice Statement (CPS)	A statement of the practices that ***thawte*** or a customer employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates. In the context of this CPS, "CPS" refers to this document.
Code Signing Certificates	Certificates which secure delivery of code and content to browsers over the Internet.
Compliance Audit	A periodic audit that the ***thawte*** PKI or its Customer undergoes to determine its conformance with ***thawte*** requirements that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CPS § 2.8.1.
Customer	An individual or organization that has purchased a product or service from ***thawte*** and/or its representatives.
EV Certificate	A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the guidelines.
Freemail	A low assurance type of Certificate for S/MIME and client authentication that does not include the Subscriber's name.
Freemail Web of Trust	A low assurance type of Certificate for S/MIME and client authentication that includes the Subscriber's authenticated name.
High Assurance	Certificates issued to organizations and sole proprietors to provide stringent 3 step authentication; message, software, and content integrity; and confidentiality encryption.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Reseller Partner Program	A program that allows Resellers to enroll for SSL Web Server Certificates, SSL Wildcard Certificates, SSL123 Certificates and SGC SuperCerts on behalf of end-user Subscribers who are customers of the Reseller.

Term	*Definition*
Key Generation Ceremony	A procedure whereby a CA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Low Assurance	Individual Certificates, whose validation procedures are based on assurances that a certain e-mail address is associated with a public key (for Personal E-mail Certificates/Freemail) and authentication of the Subscriber's name (for Freemail Web of Trust Certificates).
Medium Assurance	Certificates that are issued to Domains to provide confidentiality encryption. ***thawte*** validates that the person enrolling for the certificate has control of the domain by requiring the person to respond to an e-mail hosted at that domain. No organization authentication is performed on the owner of the domain.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a ***thawte*** Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Nonverified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS #7	Public-Key Cryptography Standard #7, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The ***thawte*** PKI consists of systems that collaborate to provide and implement the Thawte PKI.

Term	*Definition*
Referee	An individual who is permitted by the Thawte PKI to validate the identity of a Web of Trust subscriber in the event that a ***thawte*** Web of Trust Notary is not available. The referee must be a bank manager, registered lawyer, or registered CPA (accountant).
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Reseller	An entity marketing services on behalf of ***thawte*** to specific markets (e.g., the country representatives).
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CPS § 6.2.2.
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
SSL123 Certificates	Medium Assurance domain validated SSL certificates capable of 256-bit encryption and issued within minutes used to support SSL sessions between web browsers and servers. Delays in issuance can be caused if the domain is not registered with an accredited online registrar.
SSL Web Server Certificates	High Assurance secure SSL certificates with stringent 3 step authentication capable of 256-bit encryption used to support SSL sessions between web browsers and servers.
Subject	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.

Term	*Definition*
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
SGC SuperCerts	High Assurance Premium Server Gated Cryptography SSL certificates with stringent 3 step authentication, automatic 128-bit step-up encryption and capable of 256-bit encryption * used to support SSL sessions between web browsers and web servers. * With browsers IE 4.X or Netscape 4.06 and later
Superior Entity	An entity above a certain entity within the ***thawte*** PKI.
thawte PKI Participants	An individual or organization that is one or more of the following within the ***thawte*** PKI: ***thawte***, a Customer, a Reseller, a Subscriber, or a Relying Party.
thawte Repository	***thawte's*** database of relevant ***thawte*** PKI information accessible on-line.
thawte Security Policy	The highest-level document describing ***thawte's*** security policies.
thawte Web of Trust Notary	An individual who perform the RA function for low assurance "Freemail Web of Trust" certificates which contain the subscriber's authenticated name.
Trusted Person	An employee, contractor, or consultant of an entity within the ***thawte*** PKI responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CPS § 5.2.1.
Trusted Position	The positions within a ***thawte*** PKI entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
Web Host	An entity hosting the web site of another, such as an Internet service provider, a systems integrator, a Reseller, a technical consultant, and application service provider, or similar entity.

Term	*Definition*
Web of Trust	A low assurance individual "Freemail" certificate program for S/MIME and client authentication that allows the Subscriber's name to be included in the certificate after the requisite Thawte Web of Trust Notarization process has been completed.
Wildcard Certificates	Secure SSL certificates with stringent 3 step authentication capable of 256-bit encryption that secure multiple hosts on a single domain on the same server.

Appendix A1
Supplemental Validation Procedures for Extended Validation SSL Certificates

TABLE OF CONTENTS

Page

24. Final Cross-Correlation and Due Diligence
25. Certificate Renewal Verification Requirements

G. CERTIFICATE STATUS CHECKING AND REVOCATION ISSUES

26. EV Certificate Status Checking
27. EV Certificate Revocation
28. EV Certificate Problem Reporting and Response Capability

H. EMPLOYEE AND THIRD PARTY ISSUES

29. Trustworthiness and Competence
30. Delegation of Functions to Registration Authorities and Subcontractors

I. DATA AND RECORD ISSUES

31. Documentation and Audit Trail Requirements
32. Document Retention
    - (a) Audit Log Retention
    - (b) Retention of Documentation
33. Reuse and Updating Information and Documentation
    - (a) Use of Documentation to Support Multiple EV Certificates
    - (b) Use of Pre-Existing Information or Documentation
34. Data Security

J. COMPLIANCE

35. Audit Requirements
    - (a) Pre-Issuance Readiness Audit
    - (b) Regular Self Audits
    - (c) Annual Independent Audit
    - (d) Auditor Qualifications
    - (e) Root Key Generation

K. OTHER CONTRACTUAL COMPLIANCE

36. Privacy Issues
37. Limitations on EV Certificate Liability
    - (a) CA Liability

A. INTRODUCTION

1. Introduction

These procedures for Extended Validation Certificates document supplemental procedures to ***thawte***'s currently published CPS procedures for issuing Extended Validation Certificates ("EV Certificates") in terms of the Guidelines for Extended Validation Certificates ("Guidelines").. The Guidelines describe certain of the minimum requirements that a Certificate Authority (CA) must meet in order to issue Extended Validation Certificates ("EV Certificates"). Organization information from Valid EV Certificates may be displayed in a special manner by certain software applications (e.g., browser software) in order to provide users with a trustworthy confirmation of the identity of the entity that controls the website they are accessing.

B. BASIC CONCEPT OF THE EV CERTIFICATE

2. Purpose of EV Certificates.

EV Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols.

(a) Primary Purposes

Per the guidelines, the primary purposes of an EV Certificate are to:

- Identify the legal entity that controls a website: Provide a reasonable assurance to the user of an Internet browser that the website the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation, and Registration Number; and
- Enable/encrypted communications with a website: Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a website.

(b) Secondary purposes

The secondary purpose of an EV Certificate are to help establish the legitimacy of a business claiming to operate a website by confirming its legal and physical existence, and to provide a vehicle that can be used to assist in addressing problems related to phishing and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the owner of a website, EV Certificates may help to:

- Make it more difficult to mount phishing and other online identity fraud attacks using SSL certificates;
- Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves and their legitimate websites to users; and
- Assist law enforcement in investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

(c) Excluded Purposes

EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, an EV Certificate is ***not*** intended to provide any assurances, or otherwise represent or warrant:

- That the Subject named in the EV Certificate is actively engaged in doing business;
- That the Subject named in the EV Certificate complies with applicable laws;
- That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or
- That it is "safe" to do business with the Subject named in the EV Certificate.

3. EV Certificate Warranties and Representations

(a) By *thawte*

Beneficiaries of EV CertifiactesCertificates may be:

- The Subscriber entering into the Subscriber Agreement for the EV Certificate;
- The Subject named in the EV Certificate;
- All Application Software Vendors with whom the CA or its Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Vendors;
- All Relying Parties that actually rely on such EV Certificate during the period when it is Valid.

When ***thawte*** issues an EV Certificate, it represents and warrants to the EV Certificate Beneficiaries, during the period when the EV Certificate is Valid, that the it has followed the requirements of the Guidelines and its EV Policies in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate ("EV Certificate Warranty"). This EV Certificate Warranty specifically includes, but is not limited to, the following warranties:

- Legal Existence: ***thawte*** has confirmed with the Incorporating Agency in the Subject's Jurisdiction of Incorporation that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation;
- Identity: ***thawte*** has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating Agency in the Subject's Jurisdiction of Incorporation, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
- Right to Use Domain Name: ***thawte*** has taken all steps reasonably necessary in terms of the Guidelines to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate owns or has the exclusive right to use the domain name listed in the EV Certificate;
- Authorization for EV Certificate: ***thawte*** has taken all steps reasonably necessary in terms of the Guidelines to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate;
- Accuracy of Information: ***thawte*** has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;
- Subscriber Agreement: The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with ***thawte*** that satisfies the requirements of the Guidelines;

- Status: ***thawte*** will follow the requirements of these Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or revoked; and

- Revocation: ***thawte*** will follow the requirements of the Guidelines and promptly revoke the EV Certificate upon the occurrence of any revocation event as specified in the Guidelines and this Appendix.

EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, when issuing an EV Certificate, ***thawte*** does not provide any assurances, or otherwise represent or warrant:

- That the Subject named in the EV Certificate is actively engaged in doing business;
- That the Subject named in the EV Certificate complies with applicable laws;
- That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or
- That it is "safe" to do business with the Subject named in the EV Certificate.

(b) By the Subscriber

thawte will require, as part of the Subscriber Agreement, that the Subscriber make the commitments and warranties set forth in Subscriber Agreement Requirements section of these Guidelines, for the benefit of ***thawte*** and the EV Certificate Beneficiaries.

C. COMMUNITY AND APPLICABILITY

4. Issuance of EV Certificates

When issuing EV Certificates, ***thawte*** satisfies the following requirements as required by the Guidelines:

(a) Compliance

thawte shall at all times:

(1) Comply with all law applicable to its business and the certificates it issues in each jurisdiction where it operates;

(2) Comply with the requirements of the EV Guidelines;

(3) Comply with the requirements of (i) the then-current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum; and

(4) Be licensed as a CA in each jurisdiction where it operates if licensing is required by the law of such jurisdiction for the issuance of EV Certificates.

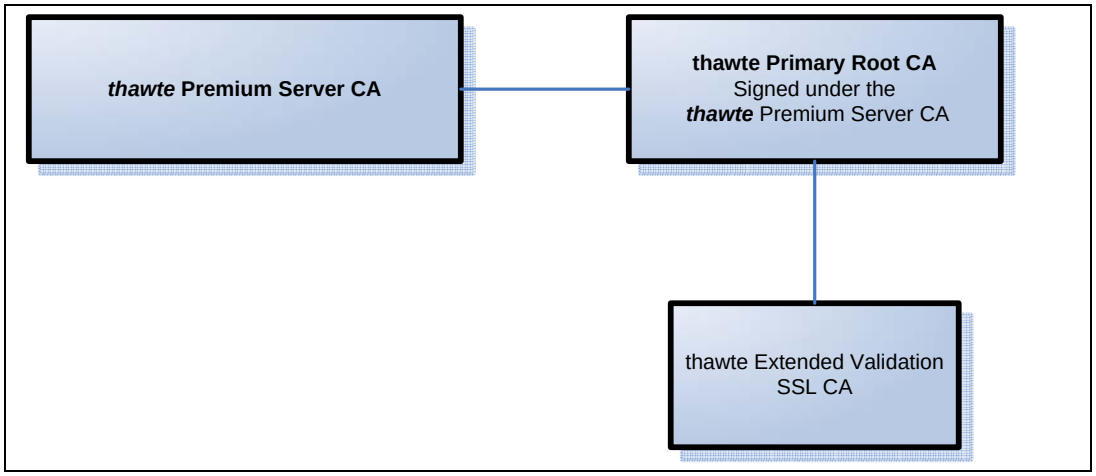
(b) EV Policies

(1) **Implementation**
The ***thawte*** CPS together with this Appendix A to the ***thawte*** CPS:

(A) Implement the requirements of the Guidelines as they are revised from time-to-time;

(B) Implement the requirements of (i) the then current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum;

(C) Specify the CA's and its Root CA's entire root certificate hierarchy including all roots that its EV Certificates depend on for proof of those EV Certificates' authenticity. ***thawte***'s root hierarchy structure is outlined below:



thawte publicly discloses its EV Policies through this CPS that is available on a 24x7 basis from the ***thawte*** online repository. ***thawte***'s CPS is structured according to the RFC 3647 format.

(3) **Commitment to Comply with Guidelines**
thawte conforms to the current version of the ***CA/Browser Forum Guidelines for Extended Validation Certificates*** ("Guidelines") published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

In addition, ***thawte*** will include (directly or by reference) the applicable requirements of these Guidelines in all contracts with subordinate CAs, RAs, Enterprise RAs, and subcontractors, that involve or relate to the issuance or maintenance of EV Certificates. The CA MUST enforce compliance with such terms.

(c) Insurance

thawte maintains the following insurance, with companies with companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide, related to its performance and obligations under the EV Guidelines as follows:

- Commercial General Liability insurance (occurrence form) with policy limits of at least $2 million in coverage, and
- Professional Liability/Errors & Omissions insurance, with policy limits of at least $5 million in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury

5. Obtaining EV Certificates

In terms of the Guidelines, EV Certificates can only be issued to Private Organizations and Government Entities that satisfy the requirements specified below:

(a) Private Organization Subjects

thawte may issue EV Certificates to Private Organizations that satisfy the following requirements:

(1) The organization MUST be a legally recognized entity whose existence was created by a filing with (or an act of) the Incorporating Agency, or Governing Body in its Jurisdiction of Incorporation (e.g., by issuance of a certificate of incorporation);

(2) The organization MUST have designated with the Incorporating Agency, or Governing Body a Registered Agent, Registered Office (as required under the laws of the Jurisdiction of Incorporation) or equivalent;

(3) The organization MUST not be designated on the records of the Incorporating Agency, or Governing Body by labels such as" inactive," "invalid," "not current," or the equivalent;

(4) The organization's Jurisdiction of Incorporation and/or its Place of Business MUST NOT be in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and

(5) The organization MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

(b) Government Entity Subjects

thawte may issue EV Certificates to Government Entities that satisfy the following requirements:

(1) The legal existence of the Government Entity is established by the law of the Jurisdiction of Incorporation. Government agencies and entities (for example State owned Universities) may be verified via the appropriate Government Entity established by the law of the Jurisdiction of Incorporation;

(2) The Government Entity MUST NOT be in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and

(3) The Government Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

(c) Excluded Subjects

Until additional criteria for validation are defined by the Guidelines, ***thawte*** can NOT issue EV Certificates to any person or any organization or entity that does not satisfy the requirements above, including but not limited to the following:

(1) General partnerships

(2) Unincorporated associations

(3) Sole proprietorships

(4) Individuals (natural persons)

D. EV CERTIFICATE CONTENT AND PROFILE

6. EV Certificate Content Requirements

This section sets forth minimum requirements for the content of the EV Certificate as they relate to the identity of the CA and the Subject of the EV Certificate.

(a) Subject Organization Information

Subject to the requirements of the Guidelines, the EV Certificate include the following information about the Subject organization in the fields listed ("Subject Organization Information"):

(1) Organization name

The validated organization name is included in the organizationName field (OID 2.5.4.10)

This field contains the Subject's full legal organization name as listed in the official records of the Incorporating Agency in the Subject's Jurisdiction of Incorporation. In addition, an assumed name or d/b/a name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis. If the combination of the full legal organization name and the assumed or d/b/a name exceeds 64 bytes as defined by RFC 3280, ***thawte*** will use only the full legal organization name in the certificate.

(2) Domain name

The validated domain name is included in the subject: commonName field (OID 2.5.4.3) and/or SubjectAlternativeName as a dNS Name.

This field contains one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject's publicly accessible server. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV certificates.

(3) Jurisdiction of Incorporation

thawte will include the Subject's validated jurisdiction of incorporation using the fields shown in Table 1 below.

Address Part	Required/Optional	Certificate Field
City or Town	If any	jurisdictionOfIncorporationLocalityName (1.3.6.1.4.1.311.60.2.1.1) ASN.1 - X520LocalityName as specified in RFC 3280
State or province (if any)	If any	jurisdictionOfIncorporationStateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2) ASN.1 - X520StateOrProvinceName as specified in RFC 3280
Country	Required	jurisdictionOfIncorporationCountryName ASN.1 - X520countryName as specified in RFC 3280

Table 1. Jurisdiction of Incorporation Certificate Fields

These fields contain information only to the level of the Incorporating Agency – e.g., the Jurisdiction of Incorporation for an Incorporating Agency at the country level would include country information but may not include state or province or city or town information; the Jurisdiction of Incorporation for an Incorporating Agency at the state or province level would include both country and state or province information, but may not include city or town information; and so forth. Country information MUST be specified using the applicable ISO country code. State or province information, and City or town information (where applicable) for the Subject's Jurisdiction of Incorporation MUST be specified using the full name of the applicable jurisdiction.

(4) Registration Number

thawte EV Certificates include the unique Registration Number assigned to the Subject by the Incorporating Agency in its Jurisdiction of Incorporation (for Private Organization Subjects only) in the serialNumber field (OID 2.5.4.5), unless the jurisdiction does not assign a unique registration number, in which case the field will include the date of incorporation...

(5) Physical Address of Place of Business

thawte EV certificates will include an address of a verified physical location of the Subject's Place of Business, in terms of the table below.

Address Part	Required/Optional	Certificate Field
Number & street	Optional	streetAddress (OID 2.5.4.9)
City or Town	Required	localityName (OID 2.5.4.7)
State or province (if any)	Required	stateOrProvinceName (OID 2.5.4.8)
Country	Required	countryName (OID 2.5.4.6)
Postal code (optional)	Optional	postalCode (2.5.4.17)

Table 2. Physical address of Place of Business Certificate Fields

7. EV Certificate Policy Identification Requirements

(a) EV Subscriber Certificates

Each EV Certificate issued by ***thawte*** to a Subscriber will include ***thawte***'s EV OID in the certificate's certificatePolicies extension. ***thawte***s EV OID used for this purpose is 2.16.840.1.113733.1.7.48.1

(b) EV Subordinate CA Certificate

The ***thawte*** Class 3 High Assurance CA contains ***thawte***'s EV OID as well as the the special anyPolicy OID (2.5.29.32.0) in the certificatePolicies extension

(c)Root CA Certificates

thawte's Root CA Certificate for EV Certificates is the VeriSign Class 3 Primary Certification Authority. This Root CA does not contain the certificatePolicies or extendedKeyUsage fields

8. Maximum Validity Period

(a) For EV Certificate

The maximum validity period for an EV Certificate is twenty seven (27) months.

(b) For Validated Data

The maximum validity period for validated data that can be used to support issuance of an EV Certificate (before revalidation is required) is as follows:

- Legal existence and identity – one (1) year;
- Assumed name – one (1) year;
- Address of Place of Business – one (1) year, but thereafter data may be refreshed by checking a Qualified Independent Information Source, even where a site visit was originally required;
- Telephone number for Place of Business – one (1) year;
- Bank account verification – one (1) years;
- Domain name – one (1) year;
- Identity and authority of Certificate Approver – one (1) year, unless a contract is in place between ***thawte*** and the Applicant that specifies a different term, in which case, the term specified in such contract will control. For example, the contract may use terms that allow the assignment of roles that are perpetual until revoked, or until agreement expires or terminated

9. Other Technical Requirements for EV Certificates

See Appendix A2 and Appendix A3 attached.

E. EV CERTIFICATE REQUEST REQUIREMENTS

10. General Requirements

(a) Documentation Requirements

Prior to the issuance of an EV Certificate, ***thawte*** obtains from the Applicant the following documentation, in compliance with the requirements of these Guidelines:

- EV Certificate Request

- Subscriber Agreement
- Additional documentation required by ***thawte*** to satisfy its verification obligations under the Guidelines

(b) Role Requirements

The following Applicant roles are required for the issuance of an EV Certificate

- **Certificate Requester** – A Certificate Requester is a natural person who is employed and authorized by the Applicant, or an authorized agent who has express authority to represent the Applicant or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.

  A Certificate Requestor may be either a Corporate or a Technical Contact.

- **Certificate Approver** – The EV Certificate Request MUST be approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.

  For thawte EV Certificates, the Corporate Contact also takes on the role of the Certificate Approver.

- **Contract Signer** – A Subscriber Agreement applicable to the requested EV Certificate MUST be signed by an authorized Contract Signer. A Contract Signer is a natural person who is employed by the Applicant, or an authorized agent who has express authority to represent the Applicant who has authority on behalf of the Applicant to sign Subscriber Agreements on behalf of the Applicant.

  For thawte EV Certificates, the Corporate Contact also takes on the role of the Contract Signer.

  One person MAY be authorized by the Applicant to fill one, two, or all three of these roles, provided that in all cases the Certificate Approver and Contract Signer must be an employee of Applicant. An Applicant MAY also authorize more than one person to fill each of these roles.

11. EV Certificate Request Requirements

(a) General

Prior to the issuance of an EV Certificate, ***thawte*** obtains from the Applicant (via a Certificate Requester authorized to act on Applicant's behalf) a properly completed and signed EV Certificate Request that complies with these Guidelines.

(b) Request and Certification

The EV Certificate Request contains a request from or on behalf of the Applicant for the issuance of an EV Certificate, and a certification by or on behalf of the Applicant that all of the information contained therein is true and correct**.**

(c) Information Requirements

The EV Certificate Request MAY include all factual information about the Applicant to be included in the EV Certificate, and such additional information as is necessary for ***thawte*** to comply with these Guidelines and ***thawte***'s own policies. In cases where the EV Certificate Request does not contain all necessary information about the Applicant, ***thawte*** MUST obtain the remaining information from either the Certificate Approver or Contract Signer, before it can process the EV Certificate request.

Before issuing an EV Certificate ***thawte*** must obtain the following information:

- Organization Name: Applicant's formal legal organization name to be included in EV Certificate, as recorded with the Incorporating Agency in Applicant's Jurisdiction of Incorporation (for Private

Organizations), or as specified in the law of Applicant's Jurisdiction of Incorporation (for Government Entities);

- Assumed Name (Optional): Applicant's assumed name (e.g., d/b/a name) to be included in the EV Certificate, as recorded in the jurisdiction of Applicant's Place of Business, if applicable;
- Domain Name: Applicant's fully qualified domain name to be included in the EV Certificate;
- Jurisdiction of Incorporation: Applicant's Jurisdiction of Incorporation to be included in EV Certificate, and consisting of:
    (a) City or town (if any),
    (b) State or province (if any), and
    (c) Country.
- Incorporating Agency: The name of the Applicant's Incorporating Agency;
- Registration Number: The unique registration number assigned to Applicant by the Incorporating Agency in Applicant's Jurisdiction of Incorporation and to be included in EV Certificate (for Private Organization Applicants only).
- Applicant Address: The address of Applicant's Place of Business, including –
    (a) Building number and street,
    (b) City or town,
    (c) State or province (if any),
    (d) Country,
    (e) Postal code (zip code), and
    (f) Main telephone number.
- Certificate Approver: Name and contact information of the Certificate Approver submitting and signing, or that has authorized the Certificate Requester to submit and sign, the EV Certificate Application on behalf of the Applicant; and
- Certificate Requester: Name and contact information of the Certificate Requester submitting the EV Certificate Request on behalf of the Applicant, if other than the Certificate Approver.

12. Subscriber Agreement Requirements

(a) General

Prior to the issuance of the EV Certificate, ***thawte*** obtains the Applicant's agreement to a legally enforceable Subscriber Agreement for the express benefit of Relying Parties and Application Software Vendors. The Subscriber Agreement must be signed by an authorized Contract Signer acting on behalf of the Applicant, and must apply to the EV Certificate to be issued pursuant to the EV Certificate Request. A separate Subscriber Agreement may be used for each EV Certificate Request for retail certificates, or a single Subscriber Agreement may be used to cover multiple future EV Certificate Requests.

(b) Agreement Requirements

The Applicant's agreement to the Subscriber Agreement shall, at a minimum, specifically name both the Applicant and the individual Contract Signer signing the Agreement on the Applicant's behalf. The Subscriber Agreement shall contain, among other things, provisions imposing on the Applicant the following obligations and warranties:

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to ***thawte***, both in the EV Certificate Request and as otherwise requested by ***thawte*** in connection with the issuance of the EV Certificate(s) to be supplied by ***thawte***;
- Protection of Private Key: An obligation and warranty by the subscriber or a subcontractor (e.g. hosting provider) to take all reasonable measures necessary to maintain sole control of, keep confidential, and

properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested EV Certificate(s) (and any associated access information or device – e.g., password or token);

- Acceptance of EV Certificate: An obligation and warranty that it will not install and use the EV Certificate(s) until it has reviewed and verified the accuracy of the data in each EV Certificate;

- Use of EV Certificate: An obligation and warranty to install the EV Certificate only on the server accessible at the domain name listed on the EV Certificate, and to use the EV Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscriber Agreement;

- Reporting and Revocation Upon Compromise: An obligation and warranty to promptly cease using an EV Certificate and its associated Private Key, and promptly request ***thawte*** to revoke the EV Certificate, in the event that: (a) any information in the EV Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key listed in the EV Certificate;

- Termination of Use of EV Certificate. An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in an EV Certificate upon expiration or revocation of that EV Certificate.

F. INFORMATION VERIFICATION REQUIREMENTS

13. General Overview

This part of ***thawte***'s procedures for issuing EV Certificates sets forth the Verification Requirements required in the Guidelines and the procedures used by ***thawte*** to satisfy the requirements.

Before issuing an EV Certificate, ***thawte*** ensures that all Subject organization information in the EV Certificate conforms to the requirements of, and has been verified in accordance with, the Guidelines and matches the information confirmed and documented by ***thawte*** pursuant to its verification processes.

14. Verification of Applicant's Legal Existence and Identity

To verify Applicant's legal existence and identity, ***thawte*** verifies that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) directly with the Incorporating Agency in Applicant's Jurisdiction of Incorporation, and designated on the records of the Incorporating Agency by labels such as "active," "valid," "current," or the equivalent. Where no such designation is available ***thawte*** will confirm the Organization is active before approving the organization.

thawte verifies that the Applicant's formal legal name as recorded with the Incorporating Agency in Applicant's Jurisdiction of Incorporation matches Applicant's name in the EV Certificate Request.

thawte obtains and records the specific unique Registration Number assigned to Applicant by the Incorporating Agency in the Applicant's Jurisdiction of Incorporation.

thawte will further obtain and record the identity and address of the Applicant's Registered Agent or Registered Office (as applicable) in the Applicant's Jurisdiction of Incorporation.

15. Verification of Applicant's Legal Existence and Identity – Assumed Name

If, in addition to the Applicant's formal legal name as recorded with the Incorporating Agency in Applicant's Jurisdiction of Incorporation, Applicant's identity as asserted in the EV Certificate is to contain any assumed name or "d/b/a" name under which Applicant conducts business, ***thawte*** will verify, through use of a Qualified Government Information Source operated by or on behalf of such government agency, or by direct contact with such government agency, that: (i) the Applicant has registered its use of the assumed name or "d/b/a" name with the appropriate state, or local government agency for such filings in the jurisdiction of its Place of Business (as verified in accordance with these Guidelines), and (ii) that such filing continues to be valid.

Alternatively, ***thawte*** may verify the assumed name through use of a Qualified Independent Information Source provided that the QIIS has verified the assumed name with the appropriate government agency, or by relying on a Verified Legal Opinion, or a Verified Accountant's Opinion that indicates the assumed name under which Applicant conducts business, the government agency such assumed name is registered with, and that such filing continues to be valid

16. Verification of Applicant's Physical Existence

(a) Address of Applicant's Place of Business

To verify Applicant's physical existence and business presence, ***thawte*** verifies that the physical address provided by Applicant is an address where Applicant conducts business operations (e.g., not a mail drop or P.O. Box), and is the address of Applicant's Place of Business.

The primary method ***thawte*** uses to obtain such verification is by requiring the Applicant to obtain a verified legal opinion or a Verified Accountant's Opinion letter attesting to this fact.

In the absence of a verified legal opinion, ***thawte*** may verify the address independently following the below procedure.

(A) For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation:

(1) For Applicants listed at the same Place of Business address in the current version of at least one (1) Qualified Independent Information Source, ***thawte*** confirms that the Applicant's address as listed in the EV Certificate Request is a valid business address for Applicant by reference to such Qualified Independent Information Sources, and may rely on Applicant's representation that such address is its Place of Business;

(2) For Applicants who are not listed at the same Place of Business address in the current version of at least one (1) Qualified Independent Information Source, ***thawte*** may confirm that the address provided by the Applicant in the EV Certificate Request is in fact the Applicant's business address by obtaining documentation of a site visit to the business address. When used, the site visit will be performed by a reliable individual or firm. The documentation of the site visit will:

(a) Verify that the Applicant's business is located at the exact address stated in the EV Certificate Request (e.g., via permanent signage, employee confirmation, etc.);

(b) Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location;

(c) Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant

(d) Indicate whether there is evidence that Applicant is conducting ongoing business activities at the site (e.g., that it is not just a mail drop, P.O. box, etc.), and

(e) Include one or more photos of (i) the exterior of the site (showing signage indicating the Applicant's name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace.

(B) For Applicants whose Place of Business is not in the same country as the Applicant's Jurisdiction of Incorporation, ***thawte*** requires a Verified Legal Opinion that indicates the address of Applicant's Place of Business and that business operations are conducted there.

(b) Telephone Number for Applicant's Place of Business

To further verify Applicant's physical existence and business presence, as well as to assist in confirming other verification requirements, ***thawte*** verifies a telephone number that is a main phone number for Applicant's Place of Business.

thawte may require a verified legal opinion, or a Verified Accountant's Opinion attesting to the telephone number.

In the absence of a verified legal opinion, ***thawte*** may verify Applicant's telephone number by:

(A) Confirming the telephone number is listed as the Applicant's telephone number for the verified address of its Place of Business in records provided by the applicable phone company or alternatively in at least one (1) Qualified Independent Information Source; *or*

(B) During a site visit, the person who is conducting the site visit MUST confirm the Applicant's main telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that the Applicant is reachable by telephone at the number dialed.

During the telephone verification process detailed in Section 21 below ***thawte*** shall call this number and obtain an affirmative response sufficient to enable a reasonable person to conclude that the Applicant is reachable by telephone at the number dialed.

17. Verification of Applicant's Operational Existence

Verification Requirements. If the records of the incorporating agency indicates that the Applicant has been in existence for less than three (3) years, and the applicant's address cannot be verified using the records of the incorporating agency, or other Qualified Independent Information Source, ***thawte*** verifies that the Applicant has the ability to engage in business.

The primary method ***thawte*** uses to verify operational existence is by requiring the Applicant to obtain a verified legal opinion letter, or a Verified Accountant's Opinion attesting to the fact that the Applicant has an active current Demand Deposit Account with a regulated financial institution.

In the absence of a verified legal opinion, ***thawte*** may verify Applicant's operational existence by performing one of the following:

(1) A successfully completed site visit, or

(2) Verify the Applicant has an active current Demand Deposit Account with a regulated financial institution, by receiving authenticated documentation directly from a regulated financial institution verifying that the Applicant has an active current Demand Deposit Account with the institution.

18. Verification of Applicant's Domain Name

thawte verifies Applicant's registration of the domain name(s) to be listed in the EV Certificate, satisfy the following requirements:

(1) The domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA);

(2) Domain registration information in the WHOIS database SHOULD be public and SHOULD show the name, physical address, and administrative contact information for the organization.

(3) The Applicant is the registered holder of the domain name or has been granted the exclusive right to use the domain name by the registered holder of the domain name

(4) The Applicant is aware of its registration or exclusive control of the domain name;

thawte performs a WHOIS inquiry on the Internet for the domain name supplied by the Applicant, to verify that the Applicant is the entity to whom the domain name is registered. Where the WHOIS record indicates otherwise, ***thawte*** will require the WHOIS record to be updated to reflect the Applicant as the registered holder of the domain.

In cases where Applicant is not the registered holder of the domain name, or domain registration information cannot be obtained from WHOIS, ***thawte*** may obtain positive confirmation from the registered domain holder that the applicant has been granted the exclusive right to use the requested Fully Qualified Domain Name (FQDN). In these circumstances, ***thawte*** also verifies the Applicant‘s exclusive right to use the domain name using one of the following methods:

(A) Relying on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet; or

(B) Relying on a representation from the Contract Signer, or the Certificate Approver if expressly authorized in a mutually agreed upon contract, coupled with a practical demonstration by the Applicant establishing that it controls the confirmed domain name by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier containing the Applicant’s FQDN.

In cases where the registered domain holder cannot be contacted, ***thawte*** shall:

- Rely on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet, ***and***
- Rely on a representation from the Contract Signer, or the Certificate Approver if expressly authorized in a mutually agreed upon contract, coupled with a practical demonstration by the Applicant establishing that it controls the confirmed domain name by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier containing the Applicant’s FQDN;

The primary method ***thawte*** uses to verify the Applicant is aware that it has exclusive control and/or ownership of the domain name is by requiring the Applicant to obtain a verified legal opinion letter attesting to this fact.

In the absence of a verified legal opinion, ***thawte*** may verify the Applicant is aware that it has exclusive control and/or ownership of the domain name by obtaining a Confirmation from Corporate Contact verifying that the Applicant is aware that it has exclusive control of the domain name.

19. Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

For both the Contract Signer and the Certificate Approver, ***thawte*** verifies the following:

(1) Name, Title and Agency. ***thawte*** verifies the name and title of the Contract Signer and the Certificate Approver, as applicable, as well as the fact that they are agents representing the Applicant.

(2) Authorization of Contract Signer. ***thawte*** verifies, through a source other than the Contract Signer, that the Contract Signer is expressly authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of Applicant (“Signing Authority”).

(3) Authorization of Certificate Approver. ***thawte*** verifies, through a source other than the Certificate Approver, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Certificate Request:

(a) Submit, and if applicable authorize a Certificate Requester to submit, the EV Certificate Request on behalf of the Applicant; and

(b) Provide, and if applicable authorize a Certificate Requester to provide, the information requested from the Applicant by ***thawte*** for issuance of the EV Certificate; and

(c) Approve EV Certificate Requests submitted by a Certificate Requester

Where the Contract Signer and Certificate Approver are the same person then the authorization of the Contract Signer shall include authorization as Certificate Approver.

The primary method ***thawte*** uses to verify the name, title, and authorization of the Contract Signer is to obtain a verified legal opinion letter or a Verified Accountant's Opinion letter attesting to these facts.

In cases where a Certificate Approver is a different person from the Contract Signer ***thawte*** verifies the name, title, agency status (as appropriate) and authorization of the Certificate Approver with the authorized Contract Signer.

In the absence of a verified legal opinion, ***thawte*** may verify agency of the Certificate Approver and/or employment of the Contract Signer by:

(A) Contacting the Applicant's Human Resources Department by phone or mail (at the phone number or address for Applicant's Place of Business, verified in accordance with these Guidelines) and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee; or

(B) Obtaining an Independent Confirmation From Applicant verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has been otherwise been appointed as an agent of Applicant.

In the absence of a verified legal opinion or a Verified Accountant's Opinion, ***thawte*** may verify the Authority of the Contract Signer by using one of the following methods:

(1) **Corporate Resolution:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by reliance on a properly authenticated corporate resolution that confirms that the person has been granted such Signing Authority, provided that such resolution is (1) certified by the appropriate corporate officer (e.g., secretary), and (2) ***thawte*** can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification.

(2) **Independent Confirmation from Applicant:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, may be verified by obtaining an Independent Confirmation From Applicant.

(3) **Contract between CA and Applicant:** The EV Authority of the Certificate Approver may be verified by reliance on a contract between ***thawte*** and the Applicant that designates the Certificate Approver with such EV Authority, provided the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer has been verified.

(4) **Pre-Authorized Certificate Approver.** Where ***thawte*** and the Applicant contemplate the submission of multiple future EV Certificate Requests, then, after ***thawte***:

- Has verified the name and title of the Contract Signer and that he/she is an employee or agent of the Applicant, and
- Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in the preceding Subsection (c) above;

the Applicant may agree in writing, signed by the Contract Signer on behalf of the Applicant, to expressly authorize one or more designated Certificate Approver(s) to exercise EV Authority with respect to each future EV Certificate Application submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s).

In these circumstances the Applicant shall be obligated under the Subscriber Agreement for all EV Certificates issued at the request of, or approved by, such Certificate Approver(s) until such EV Authority is revoked, and MUST include mutually agreed-upon provisions for (i) authenticating the Certificate Approver when EV Certificate Requests are approved, (ii) periodic re-confirmation of the EV Authority of the Certificate Approver, (iii) secure procedure by which the Applicant can notify ***thawte*** that the EV Authority of any such Certificate Approver is revoked, and (iv) such other appropriate precautions as are reasonably necessary.

20. Verification of Signature on Subscriber Agreement and EV Certificate Requests

For retail EV SSL certificates, The Subscriber Agreement for each EV Certificate Request MUST be signed by an authorized Contract Signer on behalf of the applicant. If the Certificate requester is not also an authorized Certificate Approver, or an Authorized Contract Signer, an authorized Certificate Approver or Contract Signer MUST independently approve the EV Certificate Request. In all cases, the signature MUST be a legally valid and enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV Certificate Request), or a legally valid and enforceable electronic signature (for an electronic Subscriber Agreement and/or EV Certificate Request), that binds the Applicant to the terms of each respective document.

(a) Verification Requirements

Before issuing a retail EV SSL certificate, ***thawte*** authenticates the signature of the Contract Signer on the Subscriber Agreement on each request by contacting the Contract Signer directly using a verified telephone number for the Applicant, and asking to speak to the Contract Signer, followed by a response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant, or by using a manner that makes it reasonably certain that the person named as the signer in the applicable document is, in fact, the person who signed the document on behalf of the Applicant.

In the absence of a telephone call as described above ***thawte*** may use one of the alternative methods of authenticating the signature of the Contract Signer:

(1) A letter mailed to the Applicant's or Agent's address, as verified through independent means in accordance with these Guidelines, c/o of the Certificate Requester or Contract Signer, as applicable, followed by a phone or mail response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant.

(2) Use of a signature process that establishes the name and title of the signer in a secure manner, such as through use of an appropriately secure login process that identifies the signer before signing, or through use of a digital signature made with reference to an appropriately verified certificate.

(3) Notarization by a notary, provided that ***thawte*** independently verifies that such notary is a legally qualified notary in the jurisdiction of the Certificate Requester or Contract Signer.

21. Verification of Approval of EV Certificate Request

Before ***thawte*** may issue the requested EV Certificate, ***thawte*** verifies that an authorized Certificate Approver reviewed and approved the EV Certificate Request. ***thawte*** verifies this for retail EV SSL Certificates by contacting the Certificate Approver by phone or mail (at a verified phone number or address) and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the EV Certificate Request.

22. Verification of Certain Information Sources

(a) Verified Legal Opinion

(1) Verification Requirements. Before relying on any legal opinion, ***thawte*** verifies that such legal opinion meets the following requirements ("Verified Legal Opinion"):

(A) Status of Author. ***thawte*** verifies that the legal opinion is authored by a legal practitioner retained by and representing the Applicant (or an in-house legal practitioner employed by the Applicant) (Legal Practitioner) who is either:

(i) A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the Applicant's Jurisdiction of Incorporation or any jurisdiction where the Applicant maintains an office or physical facility. ***thawte*** verifies the professional status of the author of the legal opinion by directly contacting the authority responsible for registering or licensing such Legal Practitioner(s) in the applicable jurisdiction.

(ii) A notary that is a member of the International Union of Latin Notaries, and is licensed to practice in the country of Applicant's Jurisdiction of Incorporation or any jurisdiction where the Applicant maintains an office or physical facility (and that such jurisdiction recognizes the role of the Latin Notary).

(B) Basis of Opinion. ***thawte*** verifies that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Legal Opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the Legal Practitioner's professional judgment and expertise.

(C) Authenticity. ***thawte*** confirms the authenticity of the Verified Legal Opinion by calling or sending a copy of the legal opinion back to the Legal Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Legal Practitioner listed with the authority responsible for registering or licensing such Legal Practitioner and obtaining confirmation from the Legal Practitioner or the Legal Practitioner's assistant that the legal opinion is authentic.

(b) Verified Accountant Opinion Letter

(1) Verification Requirements. Before relying on any accountant letter submitted ***thawte*** verifies that such accountant letter meets the following requirements ("Verified Accountant Letter"):

(A) Status of Author. ***thawte*** shall directly contact the authority responsible for registering or licensing such Accounting Practitioner(s) in the applicable jurisdiction to establish that the accountant letter is authored by an independent professional accountant, who is a certified public accountant, chartered accountant, or equivalent licensed by a full member of the International Federation of Accountants (IFAC) to practice accounting in the country of the Applicant's Jurisdiction of Incorporation or any jurisdiction where the Applicant maintains an office or physical facility.

(B) Basis of Opinion. The Accounting Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Accountant Letter are based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the Accounting Practitioner's professional judgment and expertise.

(C) Authenticity. To confirm the authenticity of the accountant's opinion, ***thawte*** will call or send a copy of the accountant letter back to the Accounting Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Accounting Practitioner listed with the authority responsible for registering or licensing such Accounting Practitioner and obtain confirmation from the Accounting Practitioner or the Accounting Practitioner's assistant that the accountant letter is authentic.

(c) Independent Confirmation from Applicant

An "Independent Confirmation From Applicant" is a confirmation of a particular fact (e.g., knowledge of its exclusive control of a domain name, confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the EV Authority of a Certificate Approver, etc.) that is:

(i) Received by ***thawte*** from a person employed by the Applicant (other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact ("Confirming Person"), and who represents that he/she has confirmed such fact;

(ii) Received by ***thawte*** in a manner that authenticates and verifies the source of the confirmation; and

(iii) Binding on the Applicant.

An Independent Confirmation From Applicant may be obtained via the following procedure:

(1) Confirmation Request: ***thawte*** will initiate an appropriate out-of-band communication requesting verification or confirmation of the particular fact in issue ("Confirmation Request") as follows:

(A) Addressee: The Confirmation Request MUST be directed to:

(i) A position within Applicant's organization that qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) and is identified by name and title in a current Qualified Government Information Source (e.g., an SEC filing) or a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant's Opinion; or

(ii) Applicant's Registered Agent or Registered Office in the Jurisdiction of Incorporation as listed in the official records of the Incorporating Agency, with instructions that it be forwarded to an appropriate Confirming Person.

(B) Means of Communication: The Confirmation Request MUST be directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:

(i) By paper mail, addressed to the Confirming Person at:

(a) The address of Applicant's Place of Business as verified by ***thawte*** in accordance with these procedures; or

(b) The business address for such Confirming Person specified in a current government-operated Qualified Information Source (e.g., an SEC filing), a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant's Opinion; or

(c) The address of Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation.

(ii) By e-mail addressed to the Confirming Person at the business e-mail address for such person listed in a current Qualified Government Information Source or a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant's Opinion; or

(iii) By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of Applicant's Place of Business (verified in accordance with these Guidelines) and asking to speak to such person, and a person taking the call identifies himself as such person; or

(iv) By facsimile to the Confirming Person at the Place of Business. The facsimile number must be listed in a current Qualified Government Information Source or a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant's Opinion. The cover page must be clearly addressed to the Confirming Person.

(2) Confirmation Response: ***thawte*** must receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact in issue. Such response may be provided by telephone, by e-mail, or by paper mail, so long as ***thawte*** can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

(d) Qualified Independent Information Sources (QIIS)

Commercial Information Sources used by ***thawte*** for verifying EV certificate application information meet the databases requirements required by the Guidelines.

(e) Qualified Government Information Source (QGIS)

Government Information Sources used by ***thawte*** for verifying EV certificate application information meet the databases requirements required by the Guidelines.

23. Other Verification Requirements

(a) High Risk Status

thawte takes reasonable steps to identify Applications that are likely to be at a high risk e.g., if they may possibly be targeted for fraudulent attacks ("High Risk Applicants"), and conducts such additional verification activity and takes such additional precautions as are reasonably necessary to ensure that such Applicants are properly verified under these Guidelines.

thawte maintains an internal database that includes previously revoked SSL certificates, including EV Certificates and previously rejected EV Certificate Requests, due to suspected phishing or other fraudulent usage. This information is used to flag suspicious new EV Certificate Requests. If an Applicant is flagged as a High Risk Applicant, ***thawte*** performs reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization.

(b) Denied Lists and Other Legal Black Lists

thawte will not issue any EV Certificate to the Applicant, without first taking appropriate steps for obtaining clearance from the relevant government agency, if either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant's Jurisdiction of Incorporation or Place of Business is:

(a) Identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of ***thawte***'s jurisdiction(s) of operation; and

(b) Has its Jurisdiction of Incorporation or Place of Business in any country with which the laws of ***thawte***'s jurisdiction prohibit doing business

thawte takes reasonable steps to verify EV Certificate applications with the following lists and regulations:

(A) If the CA has operations in the U.S., ***thawte*** MUST take reasonable steps to verify with the following US Government Denied lists and regulations:
(B) BIS Denied Persons List
(C) BIS Denied Entities List
(D) US Treasury Department List of Specially Designated Nationals and Blocked Persons
(E) US Government export regulations

24. Final Cross-Correlation and Due Diligence

thawte requires that after all of the verification processes and procedures are completed, an EV verification specialist who is not responsible for the collection of information reviews that ***thawte*** has performed all verification steps. That person may also be responsible for placing the final verification call to the Contract Signer and, if successful, issue the certificate.

25. Certificate Renewal Verification Requirements.

Before renewing an EV Certificate, ***thawte*** performs all authentication and verification tasks required by the Guidelines and this procedure to ensure that the renewal request is properly authorized by the Applicant and that the information displayed in the EV Certificate is still accurate and valid.

G. CERTIFICATE STATUS CHECKING AND REVOCATION ISSUES

26. EV Certificate Status Checking.

thawte maintains an online 24/7 Repository mechanism whereby Internet browsers can automatically check online the current status of all certificates.

(1) For EV Certificates:

(A) CRLs are be updated and reissued at least every seven (7) days, and with a maximum expiration time of ten (10) days; or

(B) ***thawte***'s Online Certificate Status Protocol (OCSP) is updated at least every four (4) days, and with a maximum expiration time of ten (10) days.

(2) For ***thawte***'s subordinate CA Certificate for EV:

(A) CRLs. Are updated and reissued at least every twelve (12) months, and with a maximum expiration time of twelve (12) months; or

(B) OCSP. If used, ***thawte***'s OCSP for CA Certificates for EV will be updated at least every twelve (12) months, and with a maximum expiration time of twelve (12) months.

thawte operates and maintains its CRL and/or OCSP capability with resources sufficient to provide a commercially reasonable response time for the number of queries generated by all of the EV Certificates issued by it.

Revocation entries on a CRL or OCSP are not removed until after the expiration date of the revoked EV Certificate.

27. EV Certificate Revocation.

In addition to any revocation circumstances listed in section 4.9.1 of this CPS, ***thawte*** will revoke an EV Certificate it has issued upon the occurrence of any of the following events:

(1) The Subscriber requests revocation of its EV Certificate;

(2) The Subscriber indicates that the original EV Certificate Request was not authorized and does not retroactively grant authorization;

(3) ***thawte*** obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the EV Certificate) has been compromised, or that the EV Certificate has otherwise been misused;

(4) ***thawte*** receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement;

(5) ***thawte*** receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the EV Certificate, or that the Subscriber has failed to renew its domain name;

(6) ***thawte*** receives notice or otherwise becomes aware of a material change in the information contained in the EV Certificate;

(7) A determination, in ***thawte***'s sole discretion, that the EV Certificate was not issued in accordance with the terms and conditions of these Guidelines or ***thawte***'s EV Policies;

(8) If ***thawte*** determines that any of the information appearing in the EV Certificate is not accurate.

(9) ***thawte*** ceases operations for any reason and has not arranged for another EV CA to provide revocation support for the EV Certificate;

(10) ***thawte***'s right to issue EV Certificates under these Guidelines expires or is revoked or terminated [*unless**thawte** makes arrangements to continue maintaining the CRL/OCSP Repository*] ;

(11) ***thawte***'s Private Key for its EV issuing CA Certificate has been compromised;

(13) ***thawte*** receives notice or otherwise become aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of ***thawte***'s jurisdiction of operation.

28. EV Certificate Problem Reporting and Response Capability.

thawte provides Subscribers, Relying Parties, Application Software Vendors, and other third parties with an online form to report complaints or suspected Private Key compromise, EV Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV Certificates ("Certificate Problem Reports"), and a 24x7 capability to accept and acknowledge such Reports, to: EV-abuse@thawte.com.

thawte will begin investigation of all Certificate Problem Reports within twenty-four (24) business hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

(i) The nature of the alleged problem;
(ii) Number of Certificate Problem Reports received about a particular EV Certificate or website;
(iii) The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered); and
(iv) Relevant legislation in force.

thawte takes reasonable steps to provide continuous 24/7 ability to internally respond to any high priority Certificate Problem Report, and where appropriate, forward such complaints to law enforcement and/or revoke an EV Certificate that is the subject of such a complaint.

H. EMPLOYEE AND THIRD PARTY ISSUES

29. Trustworthiness and Competence

In addition to the procedures described in Sections 5.2 and 5.3 of ***thawte***'s CPS, any person employed by ***thawte*** for engagement in the EV Certificate process, whether as an employee, agent, or an independent contractor, is subject to following additional procedures:

> (A) The personal (physical) presence of such person before trusted persons including Notary publics, or persons who perform human resource or security functions, and
> (B) The verification of well-recognized forms of government-issued photo identification (e.g., passports and/or driver's licenses).

thawte requires all Validation Specialists to pass an internal examination on the EV Certificate validation criteria outlined in these Guidelines.

30. Delegation of Functions to Registration Authorities and Subcontractors

thawte may delegate the performance of all or any part of a requirement of these procedures and the Guidelines to a registration agent (RA) or subcontractor, except for the performance of the Final Cross-Correlation and Due Diligence requirements of Section 24 of these Guidelines.

thawte MAY contractually authorize its customers for EV Certificates to perform the approval function and authorize ***thawte*** to issue EV Certificates at third and higher domain levels that contain domain(s) and Organization names that have been verified by ***thawte*** in terms of these procedures and the Guidelines. In such case, the Subject shall be considered an Enterprise RA, and the following shall apply:

(i) No Enterprise RA MAY authorize ***thawte*** to issue an Enterprise EV Certificate for a domain not previously verified by ***thawte*** in terms of these EV procedures as belonging to a business that is owned or directly controlled by the Enterprise RA;
(ii) In all cases, the Subject of an Enterprise EV Certificate MUST be an organization verified by ***thawte*** in accordance with these Guidelines;
(iii) ***thawte*** MUST impose these limitations as a contractual requirement with the Enterprise RA and monitor compliance by an authorized Customer Administrator;
(iv) The Final Cross-Correlation and Due Diligence requirements of Section 24 of these Guidelines MAY be performed by the Enterprise RA.

thawte contractually obligates each such RA, subcontractor, and Enterprise RA to comply with all applicable requirements in the Guidelines and these procedures and to perform them as required of ***thawte*** itself. ***thawte*** shall enforce compliance with such terms.

I. DATA AND RECORD ISSUES

31. Documentation and Audit Trail Requirements

(a) ***thawte*** records every action taken to process an EV Certificate Request and to issue an EV Certificate, including all information generated or received in connection with an EV Certificate Request, and every action taken to process the Request, including time, date, and personnel involved in the action. These records are available as auditable proof of ***thawte***'s practices. This also applies to all registration agents (RAs) and subcontractors as well.

(b) The foregoing record requirements include, but are not limited to, an obligation to record the following events:

(i) CA key lifecycle management events, including:
- (a) Key generation, backup, storage, recovery, archival, and destruction; and
- (b) Cryptographic device lifecycle management events

(ii) CA and Subscriber EV Certificate lifecycle management events, including:
- (a) EV Certificate Requests, renewal and re-key requests, and revocation;
- (b) All verification activities required by these Guidelines
- (c) Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
- (d) Acceptance and rejection of EV Certificate Requests;
- (e) Issuance of EV Certificates; and
- (f) Generation of EV Certificate revocation lists (CRLs); and OCSP entries

(iii) Security events, including:
- (a) Successful and unsuccessful PKI system access attempts;
- (b) PKI and security system actions performed;
- (c) Security profile changes;
- (d) System crashes, hardware failures, and other anomalies;
- (e) Firewall and router activities; and
- (f) Entries to and exits from CA facility

(iv) Log entries MUST include the following elements:
- (a) Date and time of entry;
- (b) Identity of the persona and entity making the journal entry; and
- (ç Description of entry

32. Document Retention

(a) Audit Log Retention

Audit logs for EV Certificates are made available to independent auditors upon request. Audit logs are retained for at least seven (7) years.

(b) Retention of Documentation

thawte retains all documentation relating to all EV Certificate Requests and verification thereof, and all EV Certificates and revocation thereof, for at least seven (7) year(s) after any EV Certificate based on that documentation ceases to be valid. ***thawte*** maintains current an internal database of all previously revoked EV Certificates and previously rejected EV Certificate Requests due to suspected phishing or other fraudulent usage or concerns. Such information is flagged suspicious EV Certificate Requests.

33. Reuse and Updating Information and Documentation

(a) Use of Documentation to Support Multiple EV Certificates

thawte may issue multiple EV Certificates listing the same Subject and based on a single EV Certificate Request, subject to the aging and updating requirement in (b) below.

(b) Use of Pre-Existing Information or Documentation

(1) Each EV Certificate issued by the***thawte*** MUST be supported by a valid current EV Certificate Request and a Subscriber Agreement signed by the Applicant Representative on behalf of the Applicant.

(2) The age of information used by ***thawte*** to verify such an EV Certificate Request MUST not exceed the Maximum Validity Period for such information set forth in these procedures and the Guidelines, based on the earlier of the date the information was obtained (e.g., the date of a confirmation phone call) or the date the information was last updated by the source (e.g., if an online database was accessed by ***thawte*** on July 1, but contained data last updated by the vendor on February 1, then the date of information would be considered to be February 1).

(3) In the case of outdated information, ***thawte*** repeats the verification processes required in these Guidelines.

34. Data Security

Sections 5 and 6 of ***thawte*** CPS describe ***thawte***s Security Controls.

J. COMPLIANCE

35. Audit Requirements

(a) Pre-Issuance Readiness Audit

Before issuing EV Certificates ***thawte*** shall successfully complete a point-in-time readiness assessment audit against the WebTrust EV Program, or a point-in-time readiness assessment audit against equivalent audit procedures approved by the CA/Browser Forum.

(b) Regular Self Audits

During the period in which it issues EV Certificates, ***thawte*** will control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent (3%) of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

(c) Annual Independent Audit

thawte undergoes an annual (i) WebTrust Program for CAs audit and (ii) WebTrust EV Program audit, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum. Such audits MUST cover all CA obligations under these Guidelines regardless of whether they are performed directly by ***thawte*** or delegated to an RA or subcontractor.

The audit report is made publicly available by ***thawte***.

(d) Auditor Qualifications

All audits required under the Guidelines MUST be performed by a Qualified Auditor. A Qualified Auditor MUST:

(1) Be an independent public accounting firm that has proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function and be currently licensed to perform WebTrust for CA audits and WebTrust

EV Program audits, or to perform such alternate equivalent audits approved by the CA/Browser Forum as will be performed; and

(2) Be a member of the American Institute of Certified Public Accountants (AICPA), or by a non-US equivalent that requires that audits be completed under defined standards that include the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education; and

(3) Maintain Professional Liability/Errors & Omissions insurance, with policy limits of at least $1 million in coverage

(e) Root Key Generation

For CA root keys generated after the release of these Guidelines, ***thawte***'s Qualified Auditor may witness the root key generation ceremony in order to observe the process and the controls over the integrity and confidentiality of the CA root keys produced. The Qualified Auditor MUST then issue a report opining that ***thawte***, during its root key and certificate generation process:

- Documented its Root CA key generation and protection procedures in its Certificate Policy , version, date and its Certification Practices Statement , version, date (CP and CPS);
- Included appropriate detailed procedures and controls in a documented plan of procedures to be performed for the generation of the root certification authority key pair (the "Root Key Generation Script") for the Root CA;
- Maintained effective controls to provide reasonable assurance that the Root CA was generated and protected in conformity with the procedures described in its CP/CPS and with its Root Key Generation Script; and
- Performed, during the root key generation process, all the procedures required by its Root Key Generation Script.
- A video of the entire key generation ceremony will be recorded for auditing purposes.

K. OTHER CONTRACTUAL COMPLIANCE

36. Privacy Issues

thawte will comply with all applicable privacy laws and regulations, as well as its published privacy policy, in the collection, use and disclosure of non-public personal information as part of the EV Certificate vetting process.

37. Limitations on EV Certificate Liability

(a) CA Liability

(1) Subscribers and Relying Parties

In cases where ***thawte*** has issued and managed the EV Certificate in compliance with the Guidelines and its CPS, ***thawte*** shall not be liable to the EV Certificate Subscribers or Relying Parties or any other third parties for any losses suffered as a result of use or reliance on such EV Certificate. In cases where ***thawte*** has not issued or managed the EV Certificate in complete compliance with the Guidelines and this CPS, ***thawte***'s liability to the Subscriber for legally recognized and provable claims for losses or damages suffered as a result of the use or reliance on such EV Certificate shall be the greater of (a) the damages recoverable under the Netsure Protection plan or (b) $2,000. ***thawte***'s liability to Relying Parties or any other third parties for legally recognized and provable claims for losses or damages suffered as a result of the use or reliance on such EV Certificate shall not exceed $2,000.

(2) Indemnification of Application Software Vendors

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, ***thawte*** understands and acknowledges that the Application Software Vendors who have a root certificate distribution agreement in place with ***thawte*** do not assume any obligation or potential liability of ***thawte*** under these Guidelines or that otherwise might exist because of the issuance or maintenance of EV Certificates or reliance thereon by Relying Parties or others. ***thawte*** shall defend, indemnify, and hold harmless each Application Software Vendor for any and all claims, damages, and losses suffered by such Application Software Vendor related to an EV Certificate issued by ***thawte***, regardless of the cause of action or legal theory involved. This shall not apply, however, to any claim, damages, or loss suffered by such Application Software Vendor related to an EV Certificate issued by ***thawte*** where such claim, damage, or loss was directly caused by such Application Software Vendor's software displaying as not trustworthy an EV Certificate that is still valid, or displaying as trustworthy: (1) an EV Certificate that has expired, or (2) an EV Certificate that has been revoked (but only in cases where the revocation status is currently available from ***thawte*** online, and the browser software either failed to check such status or ignored an indication of revoked status).

Appendix A2

Minimum Cryptographic Algorithm and Key Sizes for EV Certificates

1. Root CA Certificates

	Certificate issued on or before 31 Dec 2010	**Certificate issued after 31 Dec 2010**
Digest algorithm	MD5 (NOT RECOMMENDED), SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	1024 bit	2048 bit
ECC	224, 233, 256 or 283 bits	224, 233, 256 or 283 v

2. Subordinate CA Certificates

	Certificate issued on or before 31 Dec 2010	**Certificate issued after 31 Dec 2010**
Digest algorithm	SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	1024 bit or 2048 bit	2048 bit
ECC	224, 233, 256 or 283 bits	224, 233, 256 or 283 bits

3. Subscriber Certificates

	Certificate issued on or before 31 Dec 2010	**Certificate issued after 31 Dec 2010**
Digest algorithm	SHA-1	SHA1*, SHA-256, SHA-384 or SHA-512
RSA	1024 bit or 2048 bit (Note: subscriber certificates containing a 1024 bit RSA key MUST expire on or before 31 Dec 2010)	2048 bit
ECC	224, 233, 256 or 283 bits	224, 233, 256 or 283 bits

*SHA-1 should be used until SHA-256 is supported widely by browsers used by a majority of relying parties worldwide.

Appendix A3

EV Certificates Required Certificate Extensions

1. Root CA Certificate

Root certificates generated after October 2006 MUST be X.509 v3.

(a) basicConstraints

If the certificate is v3 and is created after October 2006, this extension MUST appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present.

(b) keyUsage

If the certificate is v3 and is created after October 2006, this extension MUST be present and MUST be marked critical. Bit positions for CertSign and cRLSign MUST be set. All other bit positions SHOULD NOT be set.

All other fields and extensions set in accordance to RFC 3280.

2. Subordinate CA Certificate

(a) certificatePolicies

MUST be present and SHOULD NOT be marked critical. The set of policy identifiers MUST include the identifier for ***thawte***'s extended validation policy if the certificate is issued to a subordinate CA that is not controlled by ***thawte***.

certificatePolicies:policyIdentifier (Required)
- anyPolicy if subordinate CA is controlled by Root CA
- explicit EV policy OID(s) if subordinate CA is not controlled by Root CA

The following fields MUST be present if the Subordinate CA is not controlled by ***thawte***.

certificatePolicies:policyQualifiers:policyQualifierId
- id-qt 2 [RFC 3280]

certificatePolicies:policyQualifiers:qualifier
- URI to the Certificate Practice Statement

(b) cRLDistributionPoint

MUST be present and MUST NOT be marked critical. If present, it MUST contain the HTTP URL of ***thawte***'s CRL service.

(c) authorityInformationAccess

SHOULD be present and MUST NOT be marked critical. SHALL contain the HTTP URL of ***thawte***'s OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod MAY be included for ***thawte***'s certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

(d) basicConstraints

This extension MUST appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. The CA field MUST be set true. The pathLenConstraint field MAY be present.

(e) keyUsage

This extension MUST be present and MUST be marked critical. Bit positions for CertSign and cRLSign MUST be set. All other bit positions MUST NOT be set.

All other fields and extensions set in accordance to RFC 3280.

3. Subscriber Certificate

(a) certificate Policies

MUST be present and SHOULD NOT be marked critical. The set of policyIdentifiers MUST include the identifier for ***thawte***'s extended validation policy.

certificatePolicies:policyIdentifier (Required)
- EV policy OID

certificatePolicies:policyQualifiers:policyQualifierId (Required)
- id-qt 2 [RFC 3280]

certificatePolicies:policyQualifiers:qualifier (Required)
- URI to the Certificate Practice Statement

(b) cRLDistributionPoint

SHOULD be present and MUST NOT be marked critical. If present, it will contain the HTTP URL of ***thawte***'s CRL service. This extension MUST be present if the certificate does not specify OCSP responder locations in an authorityInformationAccess extension. See section 26(b) for details.

(c) authorityInformationAccess

SHOULD be present and MUST NOT be marked critical. SHALL contain the HTTP URL of ***thawte***'s's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod MAY be included for ***thawte*** 'sCA certificate (accessMethod = 1.3.6.1.5.5.7.48.2). This extension MUST be present if the certificate does not contain a cRLDistributionPoint extension. See section 26(b) for details.

(d) basicConstraints (optional)

If present, the CA field MUST be set false.

(e) keyUsage (optional)

If present, bit positions for CertSign and cRLSign MUST NOT be set.

All other fields and extensions set in accordance to RFC 3280.