thawte
Certification Practice Statement

Version 3.7.8

January 15, 2013
thawte Certification Practice Statement

© 2013 thawte, Inc. All rights reserved.
Printed in the United States of America.

Revision date: January 15, 2015

Trademark Notices

thawte is a registered mark of Thawte Inc. The thawte logo is a trademark and service mark of thawte. Other trademarks and service marks in this document are the property of their respective owners. Thawte Inc. is a wholly owned subsidiary of Symantec Corporation.

Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of thawte.

Notwithstanding the above, permission is granted to reproduce and distribute this thawte Certification Practice Statement on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to thawte.

Requests for any other permission to reproduce this thawte Certification Practice Statement (as well as requests for copies) must be addressed to Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043 USA Attn: Practices Development, Tel: +1 650.527.8000, Fax: +1 650.527.8050 Net: practices@symantec.com.

Acknowledgement

thawte acknowledges the assistance of many reviewers of the document specializing in diverse areas of business, law, policy, and technology.
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS .......... 42

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT .......... 42
8.2 IDENTIFICATION QUALIFICATIONS OF ASSESSOR ......... 42
8.3 ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY .......... 42
8.4 TOPICS COVERED BY ASSESSMENT .................. 42
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY .......... 42
8.6 COMMUNICATION OF RESULTS .................. 43

9. OTHER BUSINESS AND LEGAL MATTERS .......... 44

9.1 FEES .................................. 44
9.1.1 Certificate Issuance or Renewal Fees .................. 44
9.1.2 Certificate Access Fees ................................ 44
9.1.3 Revocation or Status Information Access Fees .......... 44
9.1.4 Fees for Other Services ................................ 44
9.1.5 Refund Policy .................................. 44
9.2 FINANCIAL RESPONSIBILITY .......................... 45
9.2.1 Insurance Coverage .................................. 45
9.2.2 Other Assets .................................. 45
9.2.3 Insurance or Warranty Coverage for End-Entities ....... 45
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION ....... 45
9.3.1 Scope of Confidential Information .................. 45
9.3.2 Information Not Within the Scope of Confidential Information .............. 45
9.3.3 Responsibility to Protect Confidential Information ..... 45
9.4 PRIVACY OF PERSONAL INFORMATION .................. 46
9.4.1 Privacy Plan .................................. 46
9.4.2 Information Treated as Private .................. 46
9.4.3 Information Not Deemed Private .................. 46
9.4.4 Responsibility to Protect Private Information ....... 46
9.4.5 Notice and Consent to Use Private Information ...... 46
9.4.6 Disclosure Pursuant to Judicial or Administrative Process ......... 46
9.4.7 Other Information Disclosure Circumstances ......... 46
9.5 INTELLECTUAL PROPERTY RIGHTS .................. 46
9.5.1 Property Rights in Certificates and Revocation Information .............. 46
9.5.2 Property Rights in the CPS .......................... 46
9.5.3 Property Rights in Names ................................ 46
9.5.4 Property Rights in Keys and Key Material .............. 47
9.6 REPRESENTATIONS AND WARRANTIES .................. 47
9.6.1 CA Representations and Warranties .............. 47
9.6.2 RA Representations and Warranties .............. 47
9.6.3 Subscriber Representations and Warranties .............. 47
9.6.4 Relying Party Representations and Warranties ....... 48
9.6.5 Representations and Warranties of Other Participants .... 48
9.7 DISCLAIMERS OF WARRANTIES .................. 49
9.8 LIMITATIONS OF LIABILITY .......................... 49
9.8.1 Certification Authority Liability .................. 49
9.8.2 Registration Authority Liability .................. 50
9.8.3 Subscriber Liability .......................... 50
9.8.4 Relying Party Liability .................. 50
9.9 INDEMNITIES .................................. 50
9.9.1 Indemnification by Subscribers .................. 50
9.9.2 Indemnification by Relying Parties .............. 51
9.9.3 Indemnification of Application Software Suppliers ....... 51
9.10 TERM AND TERMINATION .......................... 51
9.10.1 Term .................................. 51
9.10.2 Termination .................................. 51
9.10.3 Effect of Termination and Survival .......... 51
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS .......... 51
9.12 AMENDMENTS .................................. 52
9.12.1 Procedure for Amendment .................. 52
9.12.2 Notification Mechanism and Period .............. 52
9.12.3 Circumstances under Which OID must be Changed .... 52
9.13 DISPUTE RESOLUTION PROVISIONS .................. 53
9.13.1 Disputes among thawte and Customers .......... 53
9.13.2 Disputes with End-User Subscribers or Relying Parties ... 53
9.14 GOVERNING LAW .................................. 53
9.15 COMPLIANCE WITH APPLICABLE LAW .............. 53
9.16 MISCELLANEOUS PROVISIONS .................. 53
9.16.1 Entire Agreement ................................ 53
9.16.2 Assignment .................................. 53
9.16.3 Severability .................................. 53
9.16.4 Enforcement (Attorney Fees and Waiver of Rights) .... 54
9.17 OTHER PROVISIONS .................................. 54

APPENDIX A: DEFINITIONS AND ACRONYMS .......... 55

APPENDIX B1: SUPPLEMENTAL VALIDATION PROCEDURES FOR EXTENDED VALIDATION (EV) SSL CERTIFICATES .......... 61

APPENDIX B2: MINIMUM CRYPTOGRAPHIC ALGORITHM AND KEY SIZES FOR EV CERTIFICATES .......... 98

APPENDIX B3: EV CERTIFICATES REQUIRING CERTIFICATE EXTENSIONS .......... 99

APPENDIX B4: FOREIGN ORGANIZATION GUIDELINES .......... 101

APPENDIX C: SUPPLEMENTAL VALIDATION PROCEDURES FOR EXTENDED VALIDATION (EV) CODE-SIGNING CERTIFICATES .......... 102

APPENDIX D: SUPPLEMENTAL BASELINE REQUIREMENTS FOR PUBLICLY TRUSTED CERTIFICATES .......... 114

APPENDIX E: CHANGE HISTORY .......... 134
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").

The thawte PKI issues certificates under the thawte Certificate Policy identified by the following object identifier (OID) values:

- thawte High Assurance with Extended Validation (EV)............. 2.16.840.1.113733.1.7.48.1
- thawte Certificates (non-EV).......................................... 2.16.840.1.113733.1.7.48.2

The thawte PKI operating under this CPS conforms to the current version of the CA/Browser Forum (CABF) requirements including:

- Guidelines for the Issuance and Management of Extended Validation (EV) Certificates,
- Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates, and,
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,

published at www.cabforum.org. In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document.

At this time, thawte's Extended Validation (EV) SSL certificates, Extended Validation (EV) Code-Signing certificates and Domain-Validated (DV) and Organization-Validated (OV) SSL Certificates issued by thawte CAs under this CPS are governed by the CABF Baseline Requirements. Such DV and OV certificates are issued containing the corresponding policy identifier(s) indicating adherence to and compliance with these requirements. thawte CAs assert that all Certificates issued containing these policy identifier(s) are issued and managed in accordance with the CABF Requirements.

Symantec has assigned a reserved OID value for asserting conformance with the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. This OID value is reserved for use by any brand of Symantec CA as a means of asserting compliance with these CABF Requirements and as such does not distinguish a particular brand or class of Certificate:

- The Symantec Reserved Certificate Policy identifier:
  Symantec/id-CABF-OVandDVvalidation .......................... 2.16.840.1.113733.1.7.54

1.1 Overview

thawte's Certification Authorities (CAs) offer distinct classes of end user subscriber certificates – High Assurance with Extended Validation, High Assurance and Medium Assurance. The distinction between these classes of Certificates is the level of Subscriber identification and authentication performed (See CPS §§ 3.2.2). In addition, specific types of certificates within these classes have specific intended uses (See CPS §1.4) 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 (see Appendix B1) published by the 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.

- 0 -
**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.

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

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Assurance Level</th>
<th>Issued to</th>
<th>Description and Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Web Server Certificates</td>
<td>High with extended validation</td>
<td>Organizations</td>
<td>High Assurance with extended validation secure SSL certificates issued by <strong>thawte</strong> in conformance with the Guidelines for Extended Validation Certificates. Capable of 256-bit encryption used to support SSL sessions between web browsers and servers.</td>
</tr>
<tr>
<td>SSL Web Server Certificates</td>
<td>High</td>
<td>Organizations</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>
<tr>
<td>Wildcard Certificates</td>
<td>High</td>
<td>Organizations</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>
<tr>
<td>SGC SuperCerts</td>
<td>High</td>
<td>Organizations</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. * Compatible with browsers IE 4.X or Netscape 4.06 and later</td>
</tr>
<tr>
<td>Code Signing Certificates</td>
<td>High</td>
<td>Organizations</td>
<td>Certificates which secure delivery of code and content to browsers over the Internet.</td>
</tr>
<tr>
<td>SSL123 Certificates</td>
<td>Medium</td>
<td>Registered Domain</td>
<td>Medium Assurance domain validated SSL certificates capable of 256-bit encryption used to support SSL sessions between web browsers and servers.</td>
</tr>
</tbody>
</table>

**Table 1 – Certificate Types within the thawte PKI**

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

<table>
<thead>
<tr>
<th>Program</th>
<th>Purpose and Benefit</th>
<th>Program Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>thawte</strong> Certificate Center Enterprise (TCCE) Program</td>
<td>The <strong>thawte</strong> Certificate Center Enterprise (TCCE), formerly the SPKI Program, allows an organization to issue multiple SSL Web Server, SGC SuperCerts and Code Signing Certificates by means of self-service.</td>
<td>TCCE Customers approve or deny certificate requests using the TCCE Account 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, <strong>thawte</strong> performs the back-end certificate issuance. Customers only issue certificates for SSL Web Server, SGC SuperCerts and Code Signing Certificates within their own organizations.</td>
</tr>
<tr>
<td>Reseller Partner Program</td>
<td>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 on behalf of their customers. <strong>thawte</strong>'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</td>
<td></td>
</tr>
</tbody>
</table>
Program Purpose and Benefit Program Description

Code Signing Certificates. enrollment process (See CPS § 4.1.2), 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.

<table>
<thead>
<tr>
<th>Program</th>
<th>Purpose and Benefit</th>
<th>Program Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>t-refer</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 2 – thawte PKI Programs

1.2 Document Name and Identification

This document is the thawte Certification Practice Statement.

This thawte 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.

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, RFC 3647 of the Internet Engineering Task Force. thawte reserves the right to vary from the RFC 3647 structure as needed, for example to enhance the quality of the CPS or its suitability to thawte PKI participants.

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.
1.3 PKI Participants

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:

<table>
<thead>
<tr>
<th>Type</th>
<th>Root Name</th>
<th>CA Description</th>
<th>Registration Authorities</th>
</tr>
</thead>
<tbody>
<tr>
<td>thawte</td>
<td>Root CAs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>thawte</td>
<td>Server CA</td>
<td>Root CA that issues medium assurance domain validated SSL Certificates until June 26, 2010</td>
<td>thawte, thawte TCCE Customers</td>
</tr>
<tr>
<td>thawte</td>
<td>Primary Root CA</td>
<td>High Assurance offline Root CA that issues:</td>
<td>thawte</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sub-CA Certificates for thawte Issuing CAs for Extended Validation, organization validated, domain validated and Code Signing certificates</td>
<td></td>
</tr>
<tr>
<td>Symantec</td>
<td>Class 3 Public Primary CA</td>
<td>High Assurance Root CA that issues:</td>
<td>Symantec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sub-CA Certificates for thawte Issuing CAs for thawte SGC SuperCert Certificates</td>
<td></td>
</tr>
<tr>
<td>thawte</td>
<td>Premium Server CA</td>
<td>High Assurance Root CA that until June 26, 2010 issued:</td>
<td>thawte</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Server Certificates</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sub-CA Certificates for thawte Issuing CAs</td>
<td></td>
</tr>
<tr>
<td>thawte</td>
<td>Time Stamping CA</td>
<td>Medium Assurance Root CA that issues:</td>
<td>thawte</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sub-CA Certificates for Symantec Issuing CA.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• End entity certificate for GeoTrust time stamping services.</td>
<td></td>
</tr>
<tr>
<td>thawte</td>
<td>Primary Root CA – G2</td>
<td>Currently inactive</td>
<td>thawte</td>
</tr>
<tr>
<td>thawte</td>
<td>Primary Root CA – G3</td>
<td>Currently inactive</td>
<td>thawte</td>
</tr>
</tbody>
</table>

Table 3 – CAs within the thawte PKI

The thawte Root CAs issue certificates only to subordinate CAs, with the exception of the thawte Server CA which issues end-user Subscriber certificates.

Note: Refer to the thawte Repository at 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:

<table>
<thead>
<tr>
<th>Registration Authority</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>thawte</td>
<td>thawte performs the RA function for all high assurance certificates and medium assurance certificates.</td>
</tr>
<tr>
<td>TCCE Customers</td>
<td>TCCE Customers perform identification and authentication of high assurance Certificate subscribers within the TCCE Customer’s organization as described in CPS §1.1.</td>
</tr>
</tbody>
</table>

Table 4 – RAs within the thawte PKI

1.3.3 Subscribers

Subscribers within the thawte PKI include the following:
<table>
<thead>
<tr>
<th>Class</th>
<th>Issued to</th>
<th>Types of Subscribers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Medium Assurance</strong></td>
<td>Registered Domains</td>
<td>Any person who has control of a domain referring to a device including, but not limited to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web servers, mail servers and web traffic management devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Intranet device utilizing IP addresses</td>
</tr>
<tr>
<td><strong>High Assurance</strong></td>
<td>Organizations</td>
<td>Organizations (including agencies, Educational Institutions, Government Departments, etc.) that control a device including, but not limited to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web servers, mail servers and web traffic management devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Devices digitally signing code or other content.</td>
</tr>
<tr>
<td>Sole Proprietors</td>
<td>Small Office Home Office (“SOHO”) clients that are typically individuals who run a sole proprietor online or development business.</td>
<td></td>
</tr>
<tr>
<td><strong>High Assurance with extended validation</strong></td>
<td>Organizations</td>
<td>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 B1 of this CPS.</td>
</tr>
</tbody>
</table>

Table 5 – Subscribers within the thawte PKI

As 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 Relying Parties

No stipulation.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

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 and Medium Assurance Certificates within the thawte PKI. Each type of Certificate is generally appropriate for use with the applications set forth in CPS §§ 1.4.1 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, 1.4.1. Any such usage, however, shall be limited to such entities and subject to CPS §§ 9.8.1.2, 9.8.2, and these entities shall be solely responsible for any harm or liability caused by such usage.

1.4.1 Appropriate Certificate Uses

1.4.1.1 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.

1.4.1.2 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 § 6.1.7. 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.

 1.4.2 Prohibited Certificate Uses

 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.

 1.5 Policy Administration

 1.5.1 Organization Administering the Document

 The organization administering this CPS is Symantec Corporation. Inquiries should be addressed as follows:

 Symantec Corporation
 350 Ellis Street
 Mountain View, CA 94043, USA
 Attn: Practices Development – thawte CPS
 +1 (650) 527.8000 (voice)
 +1 (650) 527.8050 (fax)
 practices@symantec.com

 1.5.2 Contact Person

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

 Symantec Corporation
 350 Ellis Street
 Mountain View, CA 94043 USA
 Attn: Practices Development – thawte CPS
 +1 (650) 527.8000 (voice)
 +1 (650) 527.8050 (fax)
 practices@symantec.com
1.5.3 Person Determining CPS Suitability for the Policy
The Symantec/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.

1.5.4 CPS Approval Procedures
See CPS § 9.12.

1.6 Definitions and Acronyms
See Appendix A.
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

See CPS § 9.6.5.1.

2.2 Publication of Certification 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 www.thawte.com/repository.

thawte publishes Certificates in accordance with Table 6 below.

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Publication Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>thawte Root CA Certificates</td>
<td>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.</td>
</tr>
<tr>
<td>thawte Issuing CA Certificates</td>
<td>Provided to Subscribers as part of the Certificate Chain provided with the end-user Subscriber Certificate.</td>
</tr>
<tr>
<td>End-User Subscriber Certificates</td>
<td>Not publicly published by thawte. Provided to Subscribers upon certificate issuance.</td>
</tr>
</tbody>
</table>

Table 6 – Certificate Publication Requirements

thawte publishes Certificate status information in accordance with CPS § 4.9.7.

2.3 Time or Frequency of Publication

This CPS is published in electronic form within the thawte Repository at www.thawte.com/repository. 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 Symantec/thawte Practices Development group upon requests sent to: Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043, USA, Attn: Practices Development – thawte CPS.

Amendments to this CPS are processed in accordance with CPS § 9.12. 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 § 2.9.7.

2.4 Access Controls on Repositories

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.
3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

3.1.1.1 CA Certificates

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

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name (CN)</td>
<td>CA Name</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>Optional</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>“Thawte Consulting cc” or “Thawte Consulting” or “Thawte” or “Thawte Inc.”</td>
</tr>
<tr>
<td>Locality (L)</td>
<td>“California” or another locality where thawe legally conducts business, or not used.</td>
</tr>
<tr>
<td>State or Province (P)</td>
<td>&quot;California&quot; or another locality where thawe legally conducts business, or not used.</td>
</tr>
<tr>
<td>Country (C)</td>
<td>“US” (except for Thawte Code Signing CA which omit this attribute). Note that while existing CA certificates may contain the legacy attribute value “ZA”, this value may not be used for new CA certificate issuances.</td>
</tr>
<tr>
<td>E-Mail (E)</td>
<td>May be used for Root CAs to include a contact e-mail address for the CA.</td>
</tr>
</tbody>
</table>

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.

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

Table 8 – Distinguished Name Attributes in Server Certificates

EV SSL certificate content and profile requirements are discussed in Section 6 of Appendix B3 to this CPS

3.1.1.3 Certificate Subject details –SSL123

3.1.1.3.1 Certificate subject details – SSL123 Certificates

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name (CN)</td>
<td>Registered domain name</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>“Domain Validated”</td>
</tr>
<tr>
<td>Organization (OU)</td>
<td>Go to <a href="https://www.thawte.com/repository/index.html">https://www.thawte.com/repository/index.html</a></td>
</tr>
<tr>
<td>Organization (OU)</td>
<td>thawe SSL123 Certificate</td>
</tr>
</tbody>
</table>

- 8 -
Table 9 – Distinguished Name Attributes in SSL123 Certificates

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization (O)</td>
<td>Registered domain name</td>
</tr>
<tr>
<td>Locality (L)</td>
<td>Not used</td>
</tr>
<tr>
<td>State or Province (P)</td>
<td>Not used</td>
</tr>
<tr>
<td>Country (C)</td>
<td>Not used</td>
</tr>
<tr>
<td>E-Mail (E)</td>
<td>Not used</td>
</tr>
</tbody>
</table>

3.1.1.3.2 Certificate subject details- SSL123 Certificates for Intranet

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

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name (CN)</td>
<td>Server, Intranet name or IP address within the private range for intranets as specified by RFC 1597</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>“Validated for Intranet Usage”</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>Go to <a href="https://www.thawte.com/repository/index.html">https://www.thawte.com/repository/index.html</a></td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>thawte SSL123 Certificate</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Server, Intranet name or IP address</td>
</tr>
<tr>
<td>Locality (L)</td>
<td>Not used</td>
</tr>
<tr>
<td>State or Province (P)</td>
<td>Not used</td>
</tr>
<tr>
<td>Country (C)</td>
<td>Not used</td>
</tr>
<tr>
<td>E-Mail (E)</td>
<td>Not used</td>
</tr>
</tbody>
</table>

3.1.1.3.3 Code Signing Certificates

Table 11 – Distinguished Name Attributes in Code Signing Certificates

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name (CN)</td>
<td>Authenticated organization name</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>“Secure Application Development” or Subscriber-provided department or division name</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Authenticated organization name</td>
</tr>
<tr>
<td>Locality (L)</td>
<td>Set based on subscriber locality</td>
</tr>
<tr>
<td>State or Province (P)</td>
<td>Set based on subscriber state or province</td>
</tr>
<tr>
<td>Country (C)</td>
<td>Set based on subscriber country</td>
</tr>
<tr>
<td>E-Mail (E)</td>
<td>Not used</td>
</tr>
</tbody>
</table>

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

The authenticated common name value included in the Subject distinguished names of organizational Certificates is either:
- a domain name (in the case of Server Certificates) or
- the legal name of the organization (in the case of Code Signing Certificates).

3.1.1.3.4 SSL Web Server Certificates with EV
“SSL Web Server Certificates with EV distinguished name attributes are discussed in Section 6 of Appendix B3 to this CPS.”

3.1.1.3.5 CABF Naming Requirements

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the thawte Supplemental Procedures, in section 9 of Appendix B1, Appendix C and Appendix D, respectively.

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.

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 Anonymity or Pseudonymity of Subscribers

No stipulation.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 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.

3.1.6 Recognition, Authentication, and Role of Trademarks

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.

3.2 Initial Identity Validation

3.2.1 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.

3.2.2 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 Non-verified 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 § 3.2.1.
3.2.2.1 Authentication of the Identity of Organizational End-User Subscribers

\textit{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 12 below.

Where a domain name or e-mail address is included in the certificate \textit{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 12 below.

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Additional Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL123 Certificate</td>
<td>\textit{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.</td>
</tr>
<tr>
<td>SSL123 for Intranet Certificate</td>
<td>\textit{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 \textit{thawte} validates that the IP address is within the private range for intranets as specified by RFC 1597.</td>
</tr>
<tr>
<td>SGC SuperCert and Code Signing Certificates</td>
<td>\textit{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 (&quot;BIS&quot;) (formerly known as the Bureau of Export Administration (&quot;BXA&quot;)), OFAC and Denied Entities.</td>
</tr>
<tr>
<td>SSL Web Server Certificates with EV</td>
<td>\textit{thawte}'s procedures for issuing Extended Validation SSL Certificates are described in Appendix B1 to this CPS.*</td>
</tr>
</tbody>
</table>

*Table 12 – Specific Authentication Procedures

With respect to \textit{thawte} Certificate Center Enterprise (TCCE), formerly SPKI, Customers, the identity confirmation process begins with \textit{thawte}'s confirmation of the identity of the TCCE Customer itself in accordance with this section. Following such confirmation, the TCCE 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.

3.2.2.1.1 CABF Verification Requirements for Organization Applicants

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the \textit{thawte} Supplemental Procedures, in Section 11 of Appendix B1, Appendix C and Appendix D, respectively.

3.2.3 Authentication of Individual Identity

No stipulation.

3.2.4 Non-Verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

No stipulation.
3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Identification and authentication for routine re-key is described via the processing certificate renewal requests in section 4.6.

3.3.2 Identification and Authentication for Re-Key After Revocation

Rekey after revocation is not be permitted if:

- revocation occurred because the Certificate was issued to a person other than the one named as the Subject of the Certificate, or
- the 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 13 below.

<table>
<thead>
<tr>
<th>Timing</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior to Certificate expiration</td>
<td>For replacement of a Certificate following revocation of the Certificate, <strong>thawte</strong> 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 § 4.6. Other than this procedure, the requirements for the validation of an original Certificate Application in CPS § 3.2.2 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.</td>
</tr>
<tr>
<td>After Certificate expiration</td>
<td>In this scenario, the requirements specified in CPS § 3.2.2 for the authentication of an original Certificate Application shall be used for replacing an end-user Subscriber Certificate.</td>
</tr>
</tbody>
</table>

Table 13 – Requirements for Certificate Replacement after Revocation

3.4 Identification and Authentication for 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.

-thawte-
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The Certificate Application is submitted by the end user Subscriber. Reseller Partners may submit Certificate Applications on behalf of their customers pursuant to the Reseller Partner Program (See CPS § 1.1).

4.1.2 Enrolment Process and Responsibilities

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 § 3.2.1 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.

Certificate Applications are submitted either to thawte or a TCCE 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 14 below.

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Entity Processing Certificate Applications</th>
<th>Entity Issuing Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Assurance with extended validation – SSL Web Server Certificates with EV</td>
<td>thawte</td>
<td>thawte</td>
</tr>
<tr>
<td>High Assurance – SSL Web Server Certificates and Code Signing</td>
<td>• thawte</td>
<td>thawte</td>
</tr>
<tr>
<td>• TCCE Customers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium Assurance – SSL123 Certificates</td>
<td>thawte</td>
<td>thawte</td>
</tr>
</tbody>
</table>

Table 14 – Entities Receiving Certificate Applications

4.1.2.1 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 strictly by authorized thawte personnel through a controlled process that requires the participation of multiple trusted individuals.

4.2 Certificate Application Processing

The procedures of this section are also used for issuance of Certificates in connection with the submission of a request to replace (i.e., renew or rekey) a Certificate.

4.2.1 Performing Identification and Authentication Functions

After a Certificate Applicant submits a Certificate Application, thawte (See CPS § 4.1.2) attempts to confirm the information in the Certificate Application (other than Non-Verified Subscriber Information) pursuant to CPS § 3.2.2.

4.2.1.1 CABF Certificate Application Requirements

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the thawte Supplemental Procedures, in Section 10 of Appendix B1, Appendix C and Appendix D, respectively.
4.2.2 Approval or Rejection of Certificate Applications

Upon successful performance of all required authentication procedures pursuant to CPS § 3.1.1 and 3.2.2, 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.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

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.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

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

4.3.3 Certificate Issuance by a Root CA

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.

4.3.3.1 CABF Requirements for Certificate Issuance by a Root CA

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the thawte Supplemental Procedures, in Section 12 of Appendix B1, Appendix C and Appendix D, respectively.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber’s acceptance of the Certificate.

4.4.2 Publication of the Certificate by the CA

No stipulation.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.
4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the Private key corresponding to the public key in the certificate shall only be permitted once the Subscriber has agreed to the Subscriber Agreement and accepted the certificate. The certificate shall be used lawfully in accordance with thawte’s Subscriber Agreement and the terms of this CPS. Subscriber obligations are set forth in section 9.6.3.

Certificate use must be consistent with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate must not be used for signing). Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate. Parties other than the Subscriber shall not archive the Subscriber Private Key except as set forth in section 4.12.

4.5.2 Relying Party Public Key and Certificate Usage

See section 9.6.4.

4.6 Certificate 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 15 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 15 below.

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Routine Rekey and Renewal Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Signing Certificates (excluding Java Code Signing Certificates)</td>
<td>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.</td>
</tr>
<tr>
<td>Server Certificates and Java Code Signing Certificates</td>
<td>Subscriber key pairs are generated outside of the online enrolment 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.</td>
</tr>
<tr>
<td>CA Certificates</td>
<td>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 § 5.6. Accordingly, for thawte CA Certificates both rekey and certificate renewal are supported.</td>
</tr>
</tbody>
</table>

Table 15 – Routine Rekey and Renewal Requirements
4.6.1 Circumstances for Certificate Renewal
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.

4.6.2 Who May Request Renewal
The Subscriber may request renewal of the Certificate.

4.6.3 Processing Certificate Renewal Requests
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. As an alternative to using a password, thawte may send an e-mail message to the e-mail address associated with the verified corporate contact for the certificate being renewed, requesting confirmation of the Certificate renewal order and authorization to issue the Certificate.

Upon receipt of confirmation authorizing issuance of the Certificate, thawte will issue the Certificate if the enrollment information (including Corporate and Technical contact information) has not changed.

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 §3.2.2 for the authentication of an original Certificate Application.

4.6.4 Notification of New Certificate Issuance to Subscriber
See section 4.3.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate
See section 4.4.

4.6.6 Publication of the Renewal Certificate by the CA
No stipulation.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities
No stipulation.

4.7 Certificate Re-Key
See section 4.6.

4.8 Certificate Modification
No stipulation.
4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation
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 was issued to a person other than the one named as the Subject of the Certificate,
- the 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 non-verified Subscriber Information, is incorrect or has changed,
- The Subscriber requests revocation of the Certificate in accordance with CPS § 3.4, or
- 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 § 4.9.3.

**thawte** will revoke a CA Certificate 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.

4.9.1.1 CABF Requirements for Reasons for Revocation
EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the **thawte** Supplemental Procedures, in Section 13 of Appendix B1, Appendix C and Appendix D, respectively.

4.9.2 Who Can Request Revocation
The following entities may request revocation of an end-user Subscriber Certificate:

- **thawte** or the TCCE Customer that approved the Subscriber’s Certificate Application may request the revocation of any end-user Subscriber Certificate in accordance with CPS § 4.9.1.
- 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.

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 for reasons as set forth in CPS § 4.9.1.
4.9.3 Procedure for Revocation Request

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.

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.

4.9.3.1 CABF Requirements for Certificate Revocation Process

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the thawte Supplemental Procedures, in Section 13 of Appendix B1 and C and section 13.1 of Appendix D, respectively.

4.9.4 Revocation Request Grace Period

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

4.9.5 Time within Which CA Must Process the Revocation Request

thawte takes commercially reasonable steps to process revocation requests without delay.

4.9.6 Revocation Checking Requirement for Relying Parties

See section 9.6.4.

4.9.7 CRL Issuance Frequency (If Applicable)

thawte publishes CRLs showing the revocation of thawte Certificates in accordance with the schedule in Table 16 below:

<table>
<thead>
<tr>
<th>CA Type</th>
<th>CA Name</th>
<th>CRL Issuance Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root CAs (Non-Issuing)</td>
<td>thawte Personal Freemail CA (terminated)</td>
<td>At least quarterly and upon Sub-CA certificate revocation</td>
</tr>
<tr>
<td></td>
<td>thawte Primary Root CA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>thawte Primary Root CA – G2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>thawte Primary Root CA – G3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>thawte Time Stamping CA</td>
<td></td>
</tr>
<tr>
<td>Root CAs (Issuing CAs)</td>
<td>thawte Server CA</td>
<td>At least daily</td>
</tr>
<tr>
<td></td>
<td>thawte Premium Server CA</td>
<td></td>
</tr>
<tr>
<td>Subordinate Issuing CAs</td>
<td>thawte Personal Freemail Issuing CA (terminated)</td>
<td>At least daily</td>
</tr>
<tr>
<td></td>
<td>thawte Code Signing CA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>thawte Extended Validation SSL CA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>thawte Extended Validation SSL SGC CA</td>
<td></td>
</tr>
</tbody>
</table>

Table 16 – CRL Issuance Frequency

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

4.9.7.1 CABF Requirements for CRL Issuance

CRL issuance for EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the thawte Supplemental Procedures, in Section 13 of Appendix B1 and C, and section 13.2.2 of Appendix D, respectively.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation.
4.9.9 On-Line Revocation/Status Checking Availability

4.9.9.1 CABF Requirements for OCSP Availability
OCSP availability for EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the thawte Supplemental Procedures, in Section 13 of Appendix B1 and C, and section 13.2.2 of Appendix D, respectively.

4.9.10 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.

4.9.11 Other Forms of Revocation Advertisements Available
No stipulation.

4.9.12 Special Requirements Regarding Key Compromise
In addition to the procedures described in CPS § 4.9.7–4.9.10, 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.

4.9.13 Circumstances for Suspension
thawte does not offer suspension services for Certificates.

4.9.14 Who Can Request Suspension
No stipulation.

4.9.15 Procedure for Suspension Request
No stipulation.

4.9.16 Limits on Suspension Period
No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics
No stipulation.

4.10.2 Service Availability
Certificate Status Services are available 24×7 without scheduled interruption.

Certificate status services for EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, conform to the CA / Browser Forum requirements as set forth in the thawte Supplemental Procedures, in Section 13 of Appendix B1 and C and section 13.2.3 of Appendix D, respectively.

4.10.3 Operational Features
No stipulation.
4.11 End of Subscription
A Subscriber may end a subscription for a thawte certificate by revoking the certificate or by allowing the certificate to expire without replacing the certificate by renewal or re-keying.

4.12 Key Escrow and Recovery
4.12.1 Key Escrow and Recovery Policy and Practices
No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices
No stipulation.
5. FACILITY, MANAGEMENT AND OPERATIONAL 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 Delaware, 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 Symantec 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 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 (HVAC) 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 § 6.2.8.

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.

### 5.2.4 Roles Requiring Separation of Duties

Access controls are invoked to maintain split control over both physical and logical access to a CA cryptographic device. Also see section 5.2.2.

### 5.3 Personnel Controls

#### 5.3.1 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.

5.3.3.1 CABF Requirements for Training and Skill Level

For EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, personnel training is provided as set forth in the _Thawte_ Supplemental Procedures, in Section 14.1 of Appendix B1, Appendix C and Appendix D, respectively.

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 Independent Contractor 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_ employee 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.

5.4 Audit Logging Procedures

5.4.1 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
  - All verification activities stipulated in this CPS,
  - Date, time, phone number used, persons spoken to, and end results of verification telephone calls,
  - Successful or unsuccessful (rejected) 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
- Description/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.

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA /Browser Forum requirements as set forth in the thawte Supplemental Procedures in section 15, Appendix B1, Appendix C and Appendix D, respectively.

5.4.2 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.

5.4.3 Retention Period for Audit Log

Audit logs are retained onsite at least two (2) months after processing and thereafter archived in accordance with CPS § 5.5.2.

5.4.4 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.

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed weekly.
5.4.6 Audit Collection System (Internal vs. External)
Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by thawte personnel.

5.4.7 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.

5.4.8 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.

5.5 Records Archival

5.5.1 Types of Records Archived
In addition to the audit logs specified in CPS § 5.4, 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
- the identity of persons requesting Certificate revocation,
- 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 § 8.

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

5.5.2 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.

5.5.3 Protection of Archive
thawte protects its archived records compiled under CPS § 5.5.1 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 § 5.5.2.

5.5.4 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 § 5.5.1 are maintained in an off-site facility in accordance with CPS § 5.7.4.

5.5.5 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.
5.5.6 Archive Collection System (Internal vs. External)
No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information
See CPS § 5.5.3.

5.6 Key Changeover

5.6.1 Routine Rekey and Renewal of CA Certificate
_thawte_ CA Certificates may be renewed periodically within the parameters specified in CPS § 6.3.2. _thawte_ CA key pairs are retired from service at the end of their respective maximum lifetimes.

_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. 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.

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.

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.

5.6.2 Key Changeover Procedures
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.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures
_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 § 5.7.4 and Key Compromise response procedures described in CPS § 5.7.3. _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.

5.7.2 Computing Resources, Software and/or Data are Corrupted
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.
5.7.3 Entity Private Key Compromise Procedures

Upon the suspected or known Compromise of a thawte CA private key, thawte and Symantec’s Key Compromise Response procedures are enacted by the Symantec/thawte Compromise Incident Response Team. This team, which includes Symantec and thawte Security, Cryptographic Business Operations, Production Services personnel, and other Symantec and thawte management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from Symantec 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 § 4.9.7,
- 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 § 5.6, except where the CA is being terminated in accordance with CPS § 5.8.

5.7.4 Business Continuity Capabilities After a Disaster

thawte has implemented a disaster recovery site separate from thawte’s principal secure facilities. thawte has developed and implemented a Disaster Recovery Plan (DRP) 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.

The DRP identifies conditions for activating the plan and what constitutes an acceptable system outage and recovery time. Disaster recovery plans address the restoration of information systems, services and key business functions following interruption to or failure of critical business processes by using backup data and backup copies of the thawte keys.

Additionally, for EV SSL Certificates, EV Code Signing, and Organization-Validated and Domain-Validated SSL Certificates, thawte’s DRP includes the CA / Browser Forum requirements as set forth in the Supplemental Procedures, in Section 16 of Appendix B1 and C and section 16.4 of Appendix D, respectively.

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.

5.8 CA or RA 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 § 5.5,
- 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.

5.9 Data Security

For the issuance of EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, thawte conforms to the CA / Browser Forum requirements for Data Security as set forth in the thawte Supplemental Procedures, in Section 16 of Appendix B1, Appendix C and Appendix D, respectively.
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 most Code Signing Certificates, the Subscriber uses a cryptographic module provided with their browser software for key generation. For server Certificates and Java Code Signing 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).

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.

Supplementary practices in Appendix B and C identify additional requirements for Certificates conforming to the CA/Browser Forum requirements.

6.1.2 Private Key Delivery to Subscriber

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 Relying Parties

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 have a minimum key size equivalent in strength to 2048 bit RSA. thawte recommends that RAs and end-user Subscribers generate 2048 bit RSA key pairs. thawte will continue to approve end entity certificates generated with a key pair size of less than 2048 bit RSA but will phase out all 1024-bit RSA by December 31, 2013. In rare circumstances thawte permits 512 bit RSA key pairs to support certain legacy applications and web servers.
6.1.5.1 CABF Requirements for Key Sizes

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA/Browser Forum requirements as set forth in the thawte Supplemental Procedures, in Section 9.5, Appendix B1, Appendix C and Appendix D, respectively.

**thawte** Root CA Certificates meet the following requirements for algorithm type and key size:

<table>
<thead>
<tr>
<th>Validity period</th>
<th>Validity period</th>
</tr>
</thead>
<tbody>
<tr>
<td>beginning on or before 31 Dec 2010</td>
<td>beginning after 31 Dec 2010</td>
</tr>
<tr>
<td>Digest algorithm</td>
<td>MD5: Not Recommended, SHA-1, SHA-256, SHA-384 or SHA-512</td>
</tr>
<tr>
<td>Minimum RSA modulus size (bits)</td>
<td>2048**</td>
</tr>
<tr>
<td>Minimum DSA modulus size (bits)</td>
<td>N/A</td>
</tr>
<tr>
<td>ECC curve</td>
<td>NIST P-256, P-384 or P-521</td>
</tr>
</tbody>
</table>

*Table 17A – Algorithms and key sizes for Root CA Certificates*

**thawte** Subordinate CA Certificates meet the following requirements for algorithm type and key size:

<table>
<thead>
<tr>
<th>Validity period</th>
<th>Validity period</th>
</tr>
</thead>
<tbody>
<tr>
<td>beginning on or before 31 Dec 2010 and ending on or before 31 Dec 2013</td>
<td>beginning after 31 Dec 2010 or ending after 31 Dec 2013</td>
</tr>
<tr>
<td>Digest algorithm</td>
<td>SHA-1, SHA-256, SHA-384 or SHA-512</td>
</tr>
<tr>
<td>Minimum RSA modulus size (bits)</td>
<td>1024</td>
</tr>
<tr>
<td>Minimum DSA modulus size (bits)</td>
<td>N/A</td>
</tr>
<tr>
<td>ECC curve</td>
<td>NIST P-256, P-384 or P-521</td>
</tr>
</tbody>
</table>

*Table 17B – Algorithms and key sizes for Subordinate CA Certificates*

**thawte** CAs shall only issue Subscriber certificates with keys containing the following algorithm types and key sizes.

<table>
<thead>
<tr>
<th>Validity period</th>
<th>Validity period</th>
</tr>
</thead>
<tbody>
<tr>
<td>ending on or before 31 Dec 2013</td>
<td>ending after 31 Dec 2013</td>
</tr>
<tr>
<td>Digest algorithm</td>
<td>SHA-1*, SHA-256, SHA-384 or SHA-512</td>
</tr>
<tr>
<td>Minimum RSA modulus size (bits)</td>
<td>1024</td>
</tr>
<tr>
<td>Minimum DSA modulus size (bits)</td>
<td>2048</td>
</tr>
<tr>
<td>ECC curve</td>
<td>NIST P-256, P-384 or P-521</td>
</tr>
</tbody>
</table>

*Table 17C – Algorithms and key sizes for Subscriber Certificates*

* SHA-1 may be used until SHA-256 is supported widely by browsers used by a substantial portion of relying parties worldwide.
** A Root CA Certificate issued prior to 31 Dec 2010 with an RSA key size less than 2048 bits may still serve as a trust anchor Subscriber Certificates issued in accordance with these Requirements.

**thawte** CAs shall reject a certificate request if the requested Public Key does meet the minimum algorithm key sizes set forth in this section.

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.
6.1.7 Key Usage Purposes (as per x509v3 field)

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

6.2 Private Key Protection & Cryptographic Module Engineering Controls

*thawte* has implemented a combination of physical, logical, and procedural controls to ensure the security of *thawte* CA private keys. *thawte* shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part. Protection of the Private Key outside the validated cryptographic module must consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key. *thawte* shall implement physical and logical safeguards to prevent unauthorized certificate issuance.

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. Parties other than the Subscriber shall not archive the Subscriber Private Key.

6.2.1 Cryptographic Module Standards and Controls

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 3.

6.2.2 Private Key (n out of m) 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 § 5.7.4.

*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 Transfer Into or From a 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 Private Key Storage on Cryptographic Module

*thawte* CA Private keys are stored within cryptographic modules that meet the requirements specified in CPS § 6.2.1.

### 6.2.8 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.

#### 6.2.8.1 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.

#### 6.2.8.2 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 are 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.

#### 6.2.8.3 CA Private Key

*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.

### 6.2.9 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 §§ 9.6.3, 6.4.1.

6.2.10 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.

6.2.11 Cryptographic Module Rating
See Section 6.2.1.

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 Certificate Operational Periods and Key Pair Usage Periods
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 18 below. End-user Subscriber Certificates that are renewals of existing subscriber certificates may have a longer validity period (up to 3 months).

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.

<table>
<thead>
<tr>
<th>Certificate Issued By:</th>
<th>Operational Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root CAs</td>
<td>Up to 25 years</td>
</tr>
<tr>
<td>Root CA to Sub-CA</td>
<td>Up to 10 years</td>
</tr>
<tr>
<td>CA to end-user Subscriber</td>
<td>Up to 5 years¹</td>
</tr>
</tbody>
</table>

Table 18 – Certificate Operational Periods

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

6.3.2.1 CABF Certificate Validity Period Requirements
EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA /Browser Forum requirements as set forth in the thawte Supplemental Procedures, in Section 9.4 of Appendix B1, Appendix C and Appendix D, respectively.

¹ At a minimum, the Distinguished Name of 4 and 5 year validity SSL certificates is re-verified after three years from date of issuance. There is no requirement to re-verify the Distinguished Name of 4 and 5 year SSL123 certificates during the validity period of the certificate.
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.

6.5.1.1 CABF Requirements for System Security
EV SSL Certificates, EV Code Signing, and domain validated and organization validated SSL Certificates conform to the CA /Browser Forum requirements as set forth in the thawte Supplemental Procedures, in Section 16.5 of Appendix B1, Appendix C and Appendix D, respectively.

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 Symantec in accordance with thawte and Symantec 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 Controls

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 Time-Stamping

No stipulation.
7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile


_thawte_ issues X.509 version 3 certificates which contain the standard fields specified in Table 19 below:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value or Value constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Version 3</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Unique value per Issuer DN that exhibits at least 20 bits of entropy</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>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>Issuer Distinguished Name</td>
<td>Common Name (CN) = CA Name</td>
</tr>
<tr>
<td></td>
<td>Organizational Unit (OU) = Optional</td>
</tr>
<tr>
<td></td>
<td>Organization (O) = “Thawte Consulting cc” or “Thawte Consulting” or “Thawte”</td>
</tr>
<tr>
<td></td>
<td>Locality (L) = “California” or another locality where <em>thawte</em> legally conducts business or not used.</td>
</tr>
<tr>
<td></td>
<td>State or Province (P) = “California” or another locality where Thawte legally conducts business, or not used.</td>
</tr>
<tr>
<td></td>
<td>Country (C) = “US” (except for <em>thawte</em> Code Signing CA which omits this attribute).</td>
</tr>
<tr>
<td></td>
<td>Note that while existing CA certificates may contain the legacy attribute value “ZA”, this value may not be used for new CA certificate issuances.</td>
</tr>
<tr>
<td></td>
<td>E-Mail (E) = May be used for Root CAs to include a contact e-mail address for the CA.</td>
</tr>
<tr>
<td>Valid From</td>
<td>Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 2459.</td>
</tr>
<tr>
<td>Valid To</td>
<td>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.</td>
</tr>
<tr>
<td>Subject Distinguished Name</td>
<td>Populated in accordance with CPS §3.1.1.</td>
</tr>
<tr>
<td>Subject Public Key</td>
<td>Encoded in accordance with RFC 2459 using the RSA algorithm and key lengths in accordance with CPS § 6.1.5.</td>
</tr>
<tr>
<td>Signature</td>
<td>Generated and encoded in accordance with RFC 2459.</td>
</tr>
</tbody>
</table>

Table 19 – Certificate Profile Basic Fields

SSL Web Server Certificates with EV standard certificate profiles are discussed in Section 6 of Appendix B3 to this CPS.

7.1.1 Version Number(s)

See section 7.1.

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.
EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the thawte Supplemental Procedures, in Section 9.3 of Appendix B1, Appendix C, and Appendix D, respectively.

### 7.1.2.1 Root CA Certificates

**thawte** Root CA certificates include the extensions specified in Table 20 below:

<table>
<thead>
<tr>
<th>Extension</th>
<th>Value or Value Constraint</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Constraints</td>
<td>Subject Type=CA</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>Path Length Constraint= None</td>
<td></td>
</tr>
</tbody>
</table>

**Table 20 – Root CA Certificate Extensions**

### 7.1.2.2 Subordinate CA Certificates

**thawte** Subordinate CA certificates include the extensions specified in Table 21 below:

<table>
<thead>
<tr>
<th>Extension</th>
<th>Value or Value Constraint</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Usage</td>
<td>Certificate Signing</td>
<td>Non-Critical</td>
</tr>
<tr>
<td></td>
<td>Off-line CRL Signing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CRL Signing(06)</td>
<td></td>
</tr>
<tr>
<td>Basic Constraints</td>
<td>Subject Type=CA</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>Path Length Constraint=0</td>
<td></td>
</tr>
<tr>
<td>Subject Alternative Name</td>
<td>Contains a reference to the CA key</td>
<td>Non-Critical</td>
</tr>
</tbody>
</table>

**Table 21 – Subordinate CA Certificate Extensions**

### 7.1.2.3 SSL Web Server Certificates

**thawte** SSL Web Server certificates include the extensions specified in Table 22 below:

<table>
<thead>
<tr>
<th>Extension</th>
<th>Value or Value Constraint</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Constraints</td>
<td>Subject Type=End Entity</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>Path Length Constraint= None</td>
<td></td>
</tr>
<tr>
<td>Enhanced Key Usage</td>
<td>Server Authentication (1.3.6.1.5.5.7.3.1)</td>
<td>Non-Critical</td>
</tr>
<tr>
<td></td>
<td>Client Authentication (1.3.6.1.5.5.7.3.2)</td>
<td></td>
</tr>
<tr>
<td>Authority information</td>
<td><a href="http://ocsp.thawte.com">http://ocsp.thawte.com</a></td>
<td></td>
</tr>
<tr>
<td>Access</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 22 – thawte SSL Web Server Certificate Extensions**

### 7.1.2.4 SSL123 Certificates

**thawte** SSL123 certificates include the extensions specified in Table 23 below:

<table>
<thead>
<tr>
<th>Extension</th>
<th>Value or Value Constraint</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Constraints</td>
<td>Subject Type=End Entity</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>Path Length Constraint= None</td>
<td></td>
</tr>
<tr>
<td>Enhanced Key Usage</td>
<td>Server Authentication (1.3.6.1.5.5.7.3.1)</td>
<td>Non-Critical</td>
</tr>
<tr>
<td></td>
<td>Client Authentication (1.3.6.1.5.5.7.3.2)</td>
<td></td>
</tr>
<tr>
<td>Authority information</td>
<td><a href="http://ocsp.thawte.com">http://ocsp.thawte.com</a></td>
<td></td>
</tr>
<tr>
<td>Access</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 23 – thawte SSL123 Certificate Extensions**

### 7.1.2.5 SGC SuperCerts

**thawte** SGC SuperCerts include the extensions specified in Table 24 below:

<table>
<thead>
<tr>
<th>Extension</th>
<th>Value or Value Constraint</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Constraints</td>
<td>Subject Type=End Entity</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>Path Length Constraint= None</td>
<td></td>
</tr>
<tr>
<td>Enhanced Key Usage</td>
<td>Server Authentication (1.3.6.1.5.5.7.3.1)</td>
<td>Non-Critical</td>
</tr>
</tbody>
</table>

**Table 24 – thawte SGC SuperCerts Certificate Extensions**
### 7.1.2.6 SSL Wildcard Certificates

**thawte** SSL Wildcard Certificates include the extensions specified in Table 25 below:

<table>
<thead>
<tr>
<th>Extension</th>
<th>Value or Value Constraint</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<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>Authority information Access</td>
<td><a href="http://ocsp.thawte.com">http://ocsp.thawte.com</a></td>
<td>Non-Critical</td>
</tr>
</tbody>
</table>

Table 25 – *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 B3 to this CPS.

### 7.1.2.8 Code Signing Certificates

**thawte** Code Signing certificates include the extensions specified in Table 26 below:

<table>
<thead>
<tr>
<th>Extension</th>
<th>Value or Value Constraint</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<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>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)</td>
<td>Non-Critical</td>
</tr>
<tr>
<td>NetscapeCertType</td>
<td>Signature(10)</td>
<td>Non-Critical</td>
</tr>
<tr>
<td>Key Usage Restriction</td>
<td>Cert PolicyId=1.3.6.1.4.1.311.2.1.22, Restricted Key Usage=Digital Signature(80)</td>
<td>Non-Critical</td>
</tr>
<tr>
<td>Subject Alternative Name</td>
<td>DNS Name=&lt;domain name of Subscriber’s web site&gt;</td>
<td>Non-Critical</td>
</tr>
</tbody>
</table>

Table 26 – *thawte* Code Signing Certificate Extensions

### 7.1.3 Algorithm Object Identifiers

**thawte** Certificates are signed with sha1RSA Certificate signatures produced using these algorithms shall comply with RFC 3279.
7.1.4 Name Forms

*thawte* Certificates are populated with an Issuer and Subject Distinguished Name in accordance with CPS § 3.1.1. The Issuer Name shall be populated in each Certificate issued containing the Country, Organization Name and the Common Name of the Issuer CA.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

**7.1.6.1 CABF Requirements for Certificate Policy Identifier**

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA/Browser Forum requirements as set forth in the *thawte* Supplemental Procedures, in Section 9.3 of Appendix B1, Appendix C and Appendix D, respectively.

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 Policies Extension

No stipulation.

7.2 CRL Profile

*thawte* issues CRLs that conform to RFC 5280. As applicable to the Certificate type, corresponding CRLs conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. At a minimum, *thawte* CRLs contain the basic fields and contents specified in Table 27 below:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value or Value constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>See CPS §7.2.1.</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Algorithm used to sign the CRL. <em>thawte</em> CRLs are signed using sha1RSA (OID: 1.2.840.113549.1.1.4) in accordance with RFC 2459.</td>
</tr>
<tr>
<td>Issuer</td>
<td>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.</td>
</tr>
<tr>
<td>Effective Date</td>
<td>Issue date of the CRL. <em>thawte</em> CRLs are effective upon issuance.</td>
</tr>
<tr>
<td>Next Update</td>
<td>Date by which the next CRL will be issued. The Next Update date for <em>thawte</em> CRLs is set as follows: 3 months from the Effective Date for <em>thawte</em> Non-Issuing Root CAs and 28 days from the Effective Date for other <em>thawte</em> CAs. CRL issuance frequency is in accordance with the requirements of CPS § 4.9.7.</td>
</tr>
<tr>
<td>Revoked Certificates</td>
<td>Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.</td>
</tr>
</tbody>
</table>

*Table 27 – 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.

7.3 OCSP Profile
OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate.

CABF Requirement for OCSP Signing
For EV SSL Certificates, EV Code Signing, and domain-valided and organization-validated SSL Certificates, thawte provides OCSP responses as set forth in the thawte Supplemental Procedures, in Section 13 of Appendix B1 and C, and section 13.2.5 and Appendix D, respectively.

7.3.1 Version Number(s)
No stipulation.

7.3.2 OCSP Extensions
No stipulation.
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

A WebTrust for Certification Authorities ("WebTrust for CAs") version 2.0 or later examination is performed of the thawte CAs on an annual basis. In addition, thawte is entitled to perform audits of its TCCE Customers and thawte Web of Trust Notaries.

CABF Requirement for Self-Audits

For EV SSL Certificates, EV Code Signing, and Organization Validated and Domain Validated SSL Certificates, thawte shall conduct self-audits as set forth in the thawte Supplemental Procedures, in Section 17.5 of Appendix B1 and C, and section 17.8 of Appendix D, respectively.

8.1 Frequency or Circumstances of Assessment

Compliance audits are performed on an annual basis at the sole expense of thawte. Audits shall be conducted over unbroken sequences of audit periods with each period no longer than one year duration.

8.2 Identity/Qualifications of Assessor

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

- Demonstrates proficiency in conducting the WebTrust for Certification Authorities v2.0 or later,
- 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.
- Is bound by law, government regulation, or professional code of ethics; and
- Maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

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.

8.5 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.
8.6 Communication of Results

Results of the compliance audit of thawte’s operations may be released at the discretion of thawte management. Such results shall be available no later than three (3) months after the end of the audit period. In the event of a delay greater than three months, Symantec shall provide an explanatory letter signed by the Qualified Auditor.
9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 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.

9.1.3 Revocation or Status Information Access Fees

thawte does not charge a fee as a condition of making the CRL’s required by CPS § 4.9.7 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.

9.1.4 Fees for Other Services

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.

9.1.5 Refund Policy

9.1.5.1 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.

9.1.5.2 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.

9.1.5.3 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 3.2.2.

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.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Symantec shall 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.

9.2.2 Other Assets

thawte, Inc. is a wholly owned subsidiary of Symantec Corporation. Symantec's financial resources are set forth in disclosures appearing at: http://investor.symantec.com/phoenix.zhtml?c=89422&p=irol

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records of Subscribers are, subject to CPS § 9.3.2, kept confidential and private (“Confidential/Private Information”):

- CA application records, whether approved or disapproved,
- Certificate Application records (subject to CPS § 9.3.2),
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by thawte or Symantec
- 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.

9.3.2 Information Not Within the Scope of Confidential Information

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 § 9.3.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

thawte secures private information from compromise and disclosure to third parties.
9.4 Privacy of Personal Information

9.4.1 Privacy Plan

thawte has implemented a privacy policy, which is located at: https://www.thawte.com/privacy/index.html

9.4.2 Information Treated as Private

See section 9.3.1.

9.4.3 Information Not Deemed Private

See section 9.3.2.

9.4.4 Responsibility to Protect Private Information

See section 9.3.3.

9.4.5 Notice and Consent to Use Private Information

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.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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.

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.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 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 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 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.

9.5.2 Property Rights in the CPS

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

9.5.3 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.
9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CA's and end-user Subscribers are the property of the CA's 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.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

CA's 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 §§ 9.8, 9.2, 9.13, 9.14 and 9.16.3.

9.6.1.1 CABF Warranties and Obligations

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the *thawte* Supplemental Procedures, in Sections 7.1 and 18 of Appendix B1 and C, and sections 7.1 (CA Warranties) and 18.3 (Root CA Obligations) of Appendix D, respectively.

9.6.2 RA Representations and Warranties

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, TCCE Customers and *thawte* Web of Trust Notaries.

9.6.3 Subscriber Representations and Warranties

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: 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 § 1.4. 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 § 4.9.1.1 and request revocation of the Certificate in accordance with CPS §§ 4.9, 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.

9.6.4 Relying Party Representations and Warranties

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: 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 § 1.4.1.2 and for purposes prohibited in CPS § 1.4.2.

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 § 4.9.10. 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.

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 Repository Representations and Warranties

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 §§ 2.2 and 4.9.7.
9.7 Disclaimers of Warranties

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

9.8 Limitations of Liability

9.8.1 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 section 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 § 9.6.1. 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.

9.8.1.1 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.

9.8.1.2 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.

9.8.1.3 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 B1 to this CPS. Notwithstanding anything to the contrary in the foregoing, to the extent thawte has issued and managed the Certificate(s) at issue in compliance with its Certification Practice Statement, thawte shall have no liability to the
Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s).

9.8.1.4 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.

9.8.1.5 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.

9.8.2 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.

9.8.3 Subscriber Liability

9.8.3.1 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.

9.8.3.2 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 § 6.2.8 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.

9.8.4 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 § 9.6.4.

9.9 Indemnities

9.9.1 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.

9.9.2 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.

9.9.3 Indemnification of Application Software Suppliers
Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the thawte Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others.

Thus the CA shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier’s software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 Term and Termination

9.10.1 Term
The CPS becomes effective upon publication in the thawte repository. Amendments to this CPS become effective upon publication in the thawte repository.

9.10.2 Termination
This CPS as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival
Upon termination of this CPS, thawte PKI Participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants
Unless otherwise specified by agreement between the parties, thawte PKI Participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.
9.12 Amendments

9.12.1 Procedure for Amendment
Amendments to this CPS shall be made by the Symantec/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: www.thawte.com/repository Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

thawte's decision to designate amendments as material or non-material shall be within thawte's sole discretion.

9.12.1.1 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.

9.12.1.2 Material Amendments
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.

9.12.2 Notification Mechanism and Period

9.12.2.1 Notification
The Symantec/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: 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.

9.12.2.2 Comment Period
Except as noted under CPS § 9.12.2.1, 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 Symantec/thawte Practices Development group up until the end of the comment period.

9.12.2.3 Mechanism to Handle Comments
The Symantec/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 § 9.12.2.1, 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 § 9.12.2.2.

9.12.3 Circumstances under Which OID must be Changed
No stipulation.

9.13.1 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.

9.13.2 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 the State of 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.

9.14 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 section 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. CAs shall be licensed in each jurisdiction where it operates where licensing is required by the law of such jurisdiction for the issuance of Certificates.

9.15 Compliance with 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. Symantec/thawte licenses its CAs in each jurisdiction that it operates where licensing is required by the law of such jurisdiction for the issuance of Certificates.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement
No stipulation.

9.16.2 Assignment
No stipulation.

9.16.3 Severability
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.

9.16.4 Enforcement (Attorney Fees and Waiver of Rights)

No stipulation.

9.17 Other Provisions

No stipulation.
## APPENDIX A: Definitions and Acronyms

### Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>A Trusted Person that performs validation and other CA or RA functions at thawte.</td>
</tr>
<tr>
<td>Affiliate</td>
<td>A leading trusted third party, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with Symantec as a distribution and services channel within a specific territory. In the CAB Forum context, the term &quot;Affiliate&quot; refers to:  A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.</td>
</tr>
<tr>
<td>Applicant</td>
<td>The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.</td>
</tr>
<tr>
<td>Applicant Representative</td>
<td>A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.</td>
</tr>
<tr>
<td>Application Software Supplier</td>
<td>A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.</td>
</tr>
<tr>
<td>Attestation Letter</td>
<td>A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.</td>
</tr>
<tr>
<td>Audit Report</td>
<td>A report from a Qualified Auditor stating the Qualified Auditor’s opinion on whether an entity’s processes and controls comply with the mandatory provisions of these Requirements.</td>
</tr>
<tr>
<td>Certificate</td>
<td>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.</td>
</tr>
<tr>
<td>Certificate Applicant</td>
<td>An individual or organization that requests the issuance of a Certificate by a CA.</td>
</tr>
<tr>
<td>Certificate Application</td>
<td>A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.</td>
</tr>
<tr>
<td>Certificate Chain</td>
<td>An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.</td>
</tr>
<tr>
<td>Certificate Data</td>
<td>Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA’s possession or control or to which the CA has access.</td>
</tr>
<tr>
<td>Certificate Revocation List (CRL)</td>
<td>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.</td>
</tr>
<tr>
<td>Certificate Signing Request</td>
<td>A message conveying a request to have a Certificate issued.</td>
</tr>
<tr>
<td>Certification Authority (CA)</td>
<td>An entity authorized to issue, manage, revoke, and renew Certificates in the thawte PKI.</td>
</tr>
<tr>
<td>Certificate Management Process</td>
<td>Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.</td>
</tr>
<tr>
<td>Certification Practice Statement (CPS)</td>
<td>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.</td>
</tr>
<tr>
<td>Certificate Problem Report</td>
<td>Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates</td>
</tr>
<tr>
<td>Code Signing Certificates</td>
<td>Certificates which secure delivery of code and content to browsers over the Internet.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Compliance Audit</td>
<td>A periodic audit that the thawte PKI or its Customer undergoes to determine its conformance with thawte requirements that apply to it.</td>
</tr>
<tr>
<td>Compromise</td>
<td>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.</td>
</tr>
<tr>
<td>Confidential/Private Information</td>
<td>Information required to be kept confidential and private.</td>
</tr>
<tr>
<td>Country</td>
<td>A Country shall mean a Sovereign state as defined in the Guidelines.</td>
</tr>
<tr>
<td>Cross Certificate</td>
<td>A certificate that is used to establish a trust relationship between two Root CAs.</td>
</tr>
<tr>
<td>Customer</td>
<td>An individual or organization that has purchased a product or service from thawte and/or its representatives.</td>
</tr>
<tr>
<td>Delegated Third Party</td>
<td>A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.</td>
</tr>
<tr>
<td>Domain Authorization</td>
<td>Correspondence or other documentation provided by a Domain Name Registrant attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The label assigned to a node in the Domain Name System.</td>
</tr>
<tr>
<td>Domain Namespace</td>
<td>The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.</td>
</tr>
<tr>
<td>Domain Name Registrant</td>
<td>Sometimes referred to as the “owner” of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the “Registrant” by WHOIS or the Domain Name Registrar.</td>
</tr>
<tr>
<td>Domain Name Registrar</td>
<td>A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).</td>
</tr>
<tr>
<td>Expiry Date</td>
<td>The “Not After” date in a Certificate that defines the end of a Certificate’s validity period.</td>
</tr>
<tr>
<td>EV Certificate</td>
<td>A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the guidelines.</td>
</tr>
<tr>
<td>Fully-Qualified Domain Name</td>
<td>A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.</td>
</tr>
<tr>
<td>Government Entity</td>
<td>A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).</td>
</tr>
<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>
<tr>
<td>Intellectual Property Rights</td>
<td>Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.</td>
</tr>
<tr>
<td>International Organization</td>
<td>An International Organization is an organization founded by a constituent document, e.g., charter, treaty, convention, or similar document, signed by, or on behalf of, a minimum of two or more Sovereign State governments.</td>
</tr>
<tr>
<td>Internal Server Name</td>
<td>A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.</td>
</tr>
<tr>
<td>Issuing CA</td>
<td>In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.</td>
</tr>
<tr>
<td>Key Compromise</td>
<td>A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.</td>
</tr>
<tr>
<td>Key Generation Ceremony</td>
<td>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.</td>
</tr>
<tr>
<td>Key Generation Script</td>
<td>A documented plan of procedures for the generation of a CA Key Pair.</td>
</tr>
<tr>
<td>Key Pair</td>
<td>The Private Key and its associated Public Key.</td>
</tr>
<tr>
<td>Legal Entity</td>
<td>An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country’s legal system.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Medium Assurance</td>
<td>Certificates that are issued to Domains to provide confidentiality encryption. <em>thawte</em> 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>
<tr>
<td>Non-repudiation</td>
<td>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 <em>thawte</em> Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.</td>
</tr>
<tr>
<td>Nonverified Subscriber Information</td>
<td>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.</td>
</tr>
<tr>
<td>Object Identifier</td>
<td>A unique alphanumeric or numeric identifier registered under the International Organization for Standardization’s applicable standard for a specific object or object class.</td>
</tr>
<tr>
<td>OCSP Responder</td>
<td>An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.</td>
</tr>
<tr>
<td>Operational Period</td>
<td>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.</td>
</tr>
<tr>
<td>Parent Company</td>
<td><strong>Parent Company</strong>: A parent company is defined as a company that owns a majority of the Subsidiary Company and this can be verified by referencing a QIIS or from financial statement supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.</td>
</tr>
<tr>
<td>PKCS #7</td>
<td>Public-Key Cryptography Standard #7, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.</td>
</tr>
<tr>
<td>PKCS #10</td>
<td>Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.</td>
</tr>
<tr>
<td>PKCS #12</td>
<td>Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.</td>
</tr>
<tr>
<td>Principal Individual(s)</td>
<td>Individuals of a Private Organization, Government Entity or Business Entity that are either owners, partners, managing members, directors or officers, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance and use of EV Certificates.</td>
</tr>
<tr>
<td>Private Key</td>
<td>The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.</td>
</tr>
<tr>
<td>Public Key</td>
<td>The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder’s corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder’s corresponding Private Key.</td>
</tr>
<tr>
<td>Public Key Infrastructure (PKI)</td>
<td>The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The <em>thawte</em> PKI consists of systems that collaborate to provide and implement the <em>thawte</em> PKI.</td>
</tr>
<tr>
<td>Publicly-Trusted Certificate</td>
<td>A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.</td>
</tr>
<tr>
<td>Qualified Auditor</td>
<td>A natural person or Legal Entity that meets the Auditor Qualifications).</td>
</tr>
<tr>
<td>Referee</td>
<td>An individual who is permitted by the <em>thawte</em> PKI to validate the identity of a Web of Trust subscriber in the event that a <em>thawte</em> Web of Trust Notary is not available. The referee must be a bank manager, registered lawyer, or registered CPA (accountant).</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Registered Domain Name</td>
<td>A Domain Name that has been registered with a Domain Name Registrar.</td>
</tr>
<tr>
<td>Registration Agency</td>
<td>A Governmental Agency that registers business information in connection with an entity’s business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include, but is not limited (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Comptroller of Currency (OCC) or Office of Thrift Supervision (OTC)</td>
</tr>
<tr>
<td>Registration Authority (RA)</td>
<td>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.</td>
</tr>
<tr>
<td>Reliable Method of Communication</td>
<td>A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.</td>
</tr>
<tr>
<td>Relying Party</td>
<td>An individual or organization that acts in reliance on a certificate and/or a digital signature.</td>
</tr>
<tr>
<td>Relying Party Agreement</td>
<td>An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.</td>
</tr>
<tr>
<td>Repository</td>
<td>An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.</td>
</tr>
<tr>
<td>Reseller</td>
<td>An entity marketing services on behalf of thawte to specific markets (e.g., the country representatives).</td>
</tr>
<tr>
<td>Reseller Partner Program</td>
<td>A program that allows Resellers to enroll for SSL Web Server Certificates, SSLWildcard Certificates, SSL123 Certificates and SGC SuperCerts on behalf of end-user Subscribers who are customers of the Reseller.</td>
</tr>
<tr>
<td>Reserved IP Address</td>
<td>An IPv4 or IPv6 address that the IANA has marked as reserved: <a href="http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml">http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml</a> <a href="http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml">http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml</a></td>
</tr>
<tr>
<td>Root CA</td>
<td>The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.</td>
</tr>
<tr>
<td>Root Certificate</td>
<td>The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.</td>
</tr>
<tr>
<td>RSA</td>
<td>A public key cryptographic system invented by Rivest, Shamir, and Adelman.</td>
</tr>
<tr>
<td>Secret Share</td>
<td>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.</td>
</tr>
<tr>
<td>Secret Sharing</td>
<td>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.</td>
</tr>
<tr>
<td>Sovereign State</td>
<td>A Sovereign state is a state, or country, that administers its own government, and is not dependent upon, or subject to, another power.</td>
</tr>
<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>
<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>
<tr>
<td>Subject</td>
<td>The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject and 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.</td>
</tr>
<tr>
<td>Subject Identity Information</td>
<td>Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Subordinate CA</strong></td>
<td>A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.</td>
</tr>
<tr>
<td><strong>Subscriber</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Subscriber Agreement</strong></td>
<td>An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.</td>
</tr>
<tr>
<td><strong>Subsidiary Company</strong></td>
<td>A subsidiary company is defined as a company that is majority owned by Applicant as verified by referencing a QIIS or from financial statement supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.</td>
</tr>
<tr>
<td><strong>SGC SuperCerts</strong></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>
<tr>
<td><strong>Superior Entity</strong></td>
<td>An entity above a certain entity within the thawte PKI.</td>
</tr>
<tr>
<td><strong>Terms of Use</strong></td>
<td>Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA.</td>
</tr>
<tr>
<td><strong>thawte PKI Participants</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>thawte Repository</strong></td>
<td>thawte’s database of relevant thawte PKI information accessible on-line.</td>
</tr>
<tr>
<td><strong>thawte Security Policy</strong></td>
<td>The highest-level document describing thawte’s security policies.</td>
</tr>
<tr>
<td><strong>Trusted Person</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Trusted Position</strong></td>
<td>The positions within a thawte PKI entity that must be held by a Trusted Person.</td>
</tr>
<tr>
<td><strong>Trustworthy System</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Unregistered Domain Name</strong></td>
<td>A Domain Name that is not a Registered Domain Name.</td>
</tr>
<tr>
<td><strong>Valid Certificate</strong></td>
<td>A Certificate that passes the validation procedure specified in RFC 5280.</td>
</tr>
<tr>
<td><strong>Validation Specialists</strong></td>
<td>Someone who performs the information verification duties specified by these Requirements.</td>
</tr>
<tr>
<td><strong>Validity Period</strong></td>
<td>The period of time measured from the date when the Certificate is issued until the Expiry Date.</td>
</tr>
<tr>
<td><strong>Web Host</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Wildcard Certificates</strong></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. A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.</td>
</tr>
<tr>
<td>Acronym</td>
<td>Term</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>AICPA</td>
<td>American Institute of Certified Public Accountants.</td>
</tr>
<tr>
<td>ANSI</td>
<td>The American National Standards Institute.</td>
</tr>
<tr>
<td>BIS</td>
<td>The United States Bureau of Industry and Science of the United States Department of Commerce.</td>
</tr>
<tr>
<td>BXA</td>
<td>The United States Bureau of Export Administration of the United States Department of Commerce.</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority.</td>
</tr>
<tr>
<td>ccTLD</td>
<td>Country Code Top-Level Domain</td>
</tr>
<tr>
<td>CICA</td>
<td>Canadian Institute of Chartered Accountants</td>
</tr>
<tr>
<td>CPS</td>
<td>Certification Practice Statement.</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List.</td>
</tr>
<tr>
<td>DBA</td>
<td>Doing Business As</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>EV</td>
<td>Extended Validation</td>
</tr>
<tr>
<td>FIPS</td>
<td>United States Federal Information Processing Standards.</td>
</tr>
<tr>
<td>FQDN</td>
<td>Fully Qualified Domain Name</td>
</tr>
<tr>
<td>ICC</td>
<td>International Chamber of Commerce.</td>
</tr>
<tr>
<td>IM</td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Numbers Authority</td>
</tr>
<tr>
<td>ICANN</td>
<td>Internet Corporation for Assigned Names and Numbers</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>NIST</td>
<td>(US Government) National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OID</td>
<td>Object Identifier</td>
</tr>
<tr>
<td>OFAC</td>
<td>Office of Foreign Assets Control</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal identification number.</td>
</tr>
<tr>
<td>PKCS</td>
<td>Public-Key Cryptography Standard.</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure.</td>
</tr>
<tr>
<td>RA</td>
<td>Registration Authority.</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for comment.</td>
</tr>
<tr>
<td>S/MIME</td>
<td>Secure multipurpose Internet mail extensions.</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer.</td>
</tr>
<tr>
<td>TLD</td>
<td>Top-Level Domain</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>VOID</td>
<td>Voice Over Internet Protocol</td>
</tr>
</tbody>
</table>
APPENDIX B1
Supplemental Validation Procedures for Extended Validation (EV)
SSL Certificates

Reference: CA/Browser Forum Guidelines for the Issuance and Management of

Table of Contents

1. Introduction
2. Basic Concept of the EV Certificate
   2.1 Purpose of EV Certificates
      2.1.1 Primary Purposes
      2.1.2 Secondary Purposes
      2.1.3 Excluded Purposes
3. References
4. Definitions
5. Abbreviations and Acronyms
6. Conventions
7. EV Certificate Warranties and Representations
   7.1 EV Certificate Warranties
   7.2 By the Applicant
8. Community and Applicability
   8.1 Issuance of EV Certificates
   8.2 EV Policies
   8.3 Commitment to Comply
   8.4 Insurance
   8.5 Obtaining EV Certificates
      8.5.1 Private Organization Subjects
      8.5.2 Government Entity Subjects
      8.5.3 Business Entity Subjects
      8.5.4 Non-Commercial Entity Subjects
9. EV Certificate Content and Profile
   9.1 Issuer Information
   9.2 Subject Information
      9.2.1 Subject Organization name (Required)
      9.2.2 Subject Alternate name Extension (Required)
      9.2.3 Common name (Deprecated)
      9.2.4 Subject Business Category (Required)
      9.2.5 Subject Jurisdiction of Incorporation or Registration (Required)
      9.2.6 Subject Registration Number (Required)
      9.2.7 Subject Physical Address of Place of Business
      9.2.8 Other Subject Attributes
   9.3 Certificate Policy Identification
      9.3.1 EV Certificate Policy Identification Requirements
      9.3.2 EV Subscriber Certificates
      9.3.3 Root CA Certificates
      9.3.4 EV Subordinate CA Certificate
   9.4 Maximum Validity Period
   9.5. Subscriber Public Key
   9.6. Certificate Serial Number
   9.7. Other Technical Requirements for EV Certificates
10. EV Certificate Request Requirements
    10.1 General Requirements
        10.1.1 Documentation Requirements
        10.1.2 Role Requirements
    10.2 EV Certificate Request Requirements
    10.3 Subscriber Agreement Requirements
11. Information Verification Requirements

11.1 General Overview
11.2 Verification of Applicant's Legal Existence and Identity
11.3 Verification of Applicant's Legal Existence and Identity – Assumed Name
11.4 Verification of Applicant's Physical Existence
   11.4.1 Address of Applicant’s Place of Business
   11.4.2 Telephone Number for Applicant’s Place of Business
11.5 Verification of Applicant’s Operational Existence
11.6 Verification of Applicant’s Domain Name
11.7 Verification of Name, Title and Authority of Contract Signer & Certificate Approver
   11.7.1 Verification Requirements
   11.7.2 Verification – Name, Title and Agency
   11.7.3 Verification - Authority
   11.7.4 Pre-Authorized Certificate Approver
11.8 Verification of Signature on Subscriber Agreement and EV Certificate Requests
   11.8.1 Verification Requirements
   11.8.2 Methods of Signature Verification
11.9 Verification of Approval of EV Certificate Request
11.10 Verification of Certain Information Sources
   11.10.1 Verified Legal Opinion
   11.10.2 Verified Accountant Letter
   11.10.3 Face-to-Face Validation
   11.10.4 Independent Confirmation From Applicant
   11.10.5 Qualified Independent Information Sources (QIIS)
   11.10.6 Qualified Government Information Sources (QGIS)
   11.10.7 Qualified Government Tax Information Source
11.11 Other Verification Requirements
   11.11.1 High Risk Status
   11.11.2 Denied Lists and Other Legal Black Lists
   11.11.3 Parent/Subsidiary/Affiliate Relationship
11.12 Final Cross-Correlation and Due Diligence
11.13 Requirements for Re-Use of Existing Documentation
   11.13.1 For Validated Data
   11.13.2 Validation for Existing Subscribers
   11.13.3 Exceptions
   11.13.4 Validation of Re-issuance Requests

12. Certificate Issuance by a Root CA

13. Certificate Revocation and Status Checking

14. Employee and Third Party Issues
   14.1 Trustworthiness and Competence
      14.1.1 Identity and Background Verification
      14.1.2 Training and Skill Level
      14.1.3 Separation of Duties
   14.2 Delegation of Functions to Registration Authorities and Subcontractors
      14.2.1 General
      14.2.2 Enterprise RAs
      14.2.3 Guideline Compliance Obligation
      14.2.4 Allocation of Liability

15. Data Records

16. Data Security

17. Audit
   17.1 Annual Independent Audit
   17.2 Audit Period
   17.3 Audit Record
   17.4 Pre-Issuance Readiness Audit
   17.5 Regular Self Audits
   17.6 Auditor Qualification
   17.7 Root CA Key Pair Generation

18. Liability and Indemnification
1. INTRODUCTION

This Appendix articulates supplemental procedures to thawte’s CPS for issuing Extended Validation Certificates (“EV Certificates”) in conformance with the Guidelines for Extended Validation Certificates (“Guidelines”), published by the CA Browser Forum at www.cabforum.org, that describe certain of the minimum requirements that a Certificate Authority (CA) must meet in order to issue Extended Validation Certificates (“EV Certificates”). This Appendix addresses EV Certificates used for SSL/TLS authentication on the Internet.

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.

2. BASIC CONCEPT OF THE EV CERTIFICATE

2.1 Purpose of EV SSL Certificates

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

2.1.1 Primary Purposes

Per the guidelines, the primary purposes of an EV SSL 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.

2.1.2 Secondary Purposes

The secondary purposes of an EV SSL 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.

2.1.3 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;
o That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or
o That it is “safe” to do business with the Subject named in the EV Certificate.

3. REFERENCES
Refer to References provided in the Baseline Requirements located at www.cabforum.org.

4. DEFINITIONS
Refer to Definitions provided in the EV Guidelines located at www.cabforum.org.

5. ABBREVIATIONS AND ACRONYMS
Refer to Abbreviations and Acronyms provided in the EV Guidelines located at www.cabforum.org.

6. CONVENTIONS
Refer to Conventions provided in the EV Guidelines located at www.cabforum.org.

7. EV CERTIFICATE WARRANTIES AND REPRESENTATIONS

7.1 EV Certificate Warranties
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 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:

A. Legal Existence: thawte has confirmed with the Incorporating or Registration Agency in the Subject’s Jurisdiction of Incorporation or Registration Incorporation or Registration or Registration Agency 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;

B. 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 or Registration 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;

C. 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(s) listed in the EV Certificate;

D. 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;

E. 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;

F. 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 or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;

G. 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
H. **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.

### 7.2 By the Applicant

`thawte` will require, as part of section 10.3 of this Appendix, that the Subscriber make the commitments and warranties set forth in Subscriber Agreement Requirements section of the Guidelines, for the benefit of `thawte` and the EV Certificate Beneficiaries.

### 8. COMMUNITY AND APPLICABILITY

#### 8.1 Issuance of EV SSL Certificates

When issuing EV Certificates, `thawte` shall at all times satisfy the requirements as required by the Guidelines and set forth in this Appendix:

`thawte` shall at all times comply with all laws applicable to its business and the certificates it issues in each jurisdiction where it operates. `thawte` shall notify the CA / Browser Forum of any occasions whereby a court or government body with jurisdiction over the activities (operations or certificate issuances) that are covered by the Guidelines determines that the performance of any mandatory requirement is deemed illegal subject to the laws of that jurisdiction.

#### 8.2 EV Policies

##### 8.2.1 Implementation

The `thawte` CPS together with this Supplemental Appendix B1 to the `thawte` CPS:

- Implements the requirements of the Guidelines as they are revised from time-to-time;
- Implements 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;
- Specifies 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 depicted below:
8.2.2 Disclosure

_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.

8.3 Commitment to Comply

_thawte_ conforms to the current version of the *CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates* (“Guidelines”) published at [www.cabforum.org/documents.html](http://www.cabforum.org/documents.html). In the event of any inconsistency between this Appendix and those Guidelines, those Guidelines take precedence over this document.

In addition, _thawte_ includes (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 SSL Certificates. The CA will enforce compliance with such terms.

8.4 Insurance

_thawte_ maintains the following insurance, with a company 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:

(A) Commercial General Liability insurance (occurrence form) with policy limits of at least $2 million US dollars in coverage, and

(B) Professional Liability/Errors & Omissions insurance, with policy limits of at least $5 million US dollars 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.

8.5 Obtaining EV Certificates

8.5.1 General

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

8.5.2 Private Organization Subjects

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

(1) The entity MUST be a legally recognized entity whose existence was created by a filing with (or an act of) the Incorporating or Registration Agency, or Governing Body in its Jurisdiction of
Incorporation or Registration (e.g., by issuance of a certificate of incorporation), or is an entity that is created or recognized by a Government Agency (e.g., under a charter, treaty, convention or equivalent recognition instrument);

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

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

(4) The entity MUST have a verifiable physical existence and business presence

(5) The entity’s Jurisdiction of Incorporation, Registration, Charter, or License 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

(6) The 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.

8.5.3 Government Entity Subjects

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

1. The legal existence of the entity is established by the political subdivision in which such Government Entity operates;
2. The 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 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.

8.5.4 Business Entity Subjects

*thawte* MAY issue EV Certificates to Business Entities that satisfy the following requirements:

1) The entity MUST be a legally recognized entity whose formation included the filing of certain forms with the Registration Agency in its Jurisdiction, the issuance or approval by such Registration Agency of a charter, certificate, or license, and whose existence can be verified with that Registration Agency;

2) The entity MUST have a verifiable physical existence and business presence;

3) At least one Principal Individual associated with the entity MUST be identified and validated.

4) The identified Principal Individual MUST attest to the representations made in the Subscriber Agreement;

5) Where the entity represents itself under an assumed name, *thawte* verifies the Business Entity’s use of the assumed name pursuant to the requirements of Section 11.3 herein;

6) **The entity and the identified Principal Individual associated with the entity MUST NOT be in any country where *thawte* is prohibited from doing business or issuing a certificate by the laws of *thawte*’s jurisdiction; and**

7) **The entity and the identified Principal Individual associated with the entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of *thawte*’s jurisdiction.**

8.5.5 Non-Commercial Entity Subjects

*thawte* MAY issue EV Certificates to Non-Commercial Entities who do not qualify under subsections 8.5.2 through 8.5.4 but satisfy the following requirements:

(A) The applicant is an International Organization Entity created under a Charter, Treaty, Convention or equivalent instrument that was signed by, or on behalf of, more than one country’s government. The CA/Browser Forum may publish a listing of International Organizations that have been approved for EV eligibility, and
(B) The applicant is an International Organization Entity MUST NOT be headquartered in any country where thawte is prohibited from doing business or issuing a certificate by the laws of thawte's jurisdiction; and
(C) The applicant is an International Organization Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of thawte's jurisdiction.

Subsidiary organizations or agencies of qualified international organizations may also qualify for EV certificates issued in accordance with these Guidelines.

9. EV CERTIFICATE CONTENT AND PROFILE

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.

9.1 Issuer Information

An EV Certificate must include Issuer information as set forth in section 9.1, Issuer Information, Appendix D, Supplemental Baseline Requirements.

9.2 Subject Information

Subject to the requirements of the Guidelines, the EV Certificate and certificates issued to Subordinate CAs that are not controlled by thawte includes the following information about the Subject organization in the fields listed following:

9.2.1 Subject Organization name (Required)

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 or Registration Agency in the Subject’s Jurisdiction of Incorporation, or as otherwise verified as provided herein. thawte MAY abbreviate the organization prefixes or suffixes in the Organization name, e.g., if the QGIS shows “*Company Name* Incorporated” thawte MAY include “*Company Name*, Inc.”. thawte uses common abbreviations that are generally accepted in the Jurisdiction of Incorporation or Registration.

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 characters as defined by RFC 5280, thawte will use only the full legal organization name in the certificate.

If the Organization name by itself exceeds 64 characters, thawte MAY abbreviate parts of organization name, and/or omit non-material words in the organization name in such a way that the name in the certificate does not exceed the 64 character limit, and a Relying Party will not be misled into thinking they are dealing with a different Organization.

9.2.2 Subject Alternate Name Extension (Required)

One or more host Domain name(s) is included in the SubjectAlternativeName as DNS Names.

This extension contains one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject’s 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.

9.2.3 Common Name (Deprecated/discouraged, but not prohibited)

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 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.

9.2.4 Subject Business Category (Required)

The Business Category is included in the subject:businessCategory (OID 2.5.4.15)

This field contains one of the values contained in the table below depending whether the Subject qualifies under one of those categories.

<table>
<thead>
<tr>
<th>Subject Type</th>
<th>Business Category value</th>
<th>Legacy values for Business Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Organization</td>
<td>Private Organization</td>
<td>V1.0, Clause 5.(b)</td>
</tr>
<tr>
<td>Government Entity</td>
<td>Government Entity</td>
<td>V1.0, Clause 5.(c)</td>
</tr>
<tr>
<td>Business Entity</td>
<td>Business Entity</td>
<td>V1.0, Clause 5.(d)</td>
</tr>
<tr>
<td>Non-Commercial Entity</td>
<td>Non-Commercial Entity</td>
<td>V1.0, Clause 5.(e)</td>
</tr>
</tbody>
</table>

Table 1 Business category field content

9.2.5 Subject Jurisdiction of Incorporation or Registration (Required)

Thawte will include the Subject’s validated jurisdiction of Incorporation or Registration using the fields shown in Table 1 below.

<table>
<thead>
<tr>
<th>Address Part</th>
<th>Required/ Optional</th>
<th>Certificate Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locality</td>
<td>If Required</td>
<td>jurisdictionOfIncorporationLocalityName (OID 1.3.6.1.4.1.311.60.2.1.1) ASN.1 - X520LocalityName as specified in RFC 5280</td>
</tr>
<tr>
<td>State or province (if any)</td>
<td>If Required</td>
<td>jurisdictionOfIncorporationStateOrProvinceName (OID 1.3.6.1.4.1.311.60.2.1.2) ASN.1 - X520StateOrProvinceName as specified in RFC 5280</td>
</tr>
<tr>
<td>Country</td>
<td>Required</td>
<td>jurisdictionOfIncorporationCountryName (OID 1.3.6.1.4.1.311.60.2.1.3) ASN.1 - X520countryName as specified in RFC 5280</td>
</tr>
</tbody>
</table>

Table 2. Jurisdiction of Incorporation or Registration Certificate Fields

These fields MUST NOT contain information that is not relevant to the level of the Incorporating Agency or Registration Agency. For example, the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level MUST include the country information but MUST NOT include the state or province or locality information. Similarly, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information, but MUST NOT include locality information. And, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information. Country information MUST be specified using the applicable ISO country code. State or province or locality information (where applicable) for the Subject's Jurisdiction of Incorporation or Registration MUST be specified using the full name of the applicable jurisdiction.

9.2.6 Subject Registration Number (Required)

Thawte EV Certificates include Subject Registration Number in the serialNumber field (OID 2.5.4.5). For Private Organizations, the unique Registration Number (or similar) assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration is included unless the jurisdiction does not assign a unique registration number, in which case the field will include the date of incorporation in any one of the common date formats.
For Government Entities that do not have a Registration Number or readily verifiable date of creation, **thawte** enters appropriate language to indicate that the Subject is a Government Entity.

For Business Entities, the Registration Number that was received by the Business Entity upon government registration SHALL be entered in this field, unless the jurisdiction does not issue numbers pursuant to government registration, in which case the field will include the date of the registration in any one of the common date formats.

### 9.2.7 Subject Physical Address of Place of Business (Required)

**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.

<table>
<thead>
<tr>
<th>Address Part</th>
<th>Required/Optional</th>
<th>Certificate Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number &amp; street</td>
<td>Optional</td>
<td>streetAddress (OID 2.5.4.9)</td>
</tr>
<tr>
<td>City or Town</td>
<td>Required</td>
<td>localityName (OID 2.5.4.7)</td>
</tr>
<tr>
<td>State or province (if any)</td>
<td>Required</td>
<td>stateOrProvinceName (OID 2.5.4.8)</td>
</tr>
<tr>
<td>Country</td>
<td>Required</td>
<td>countryName (OID 2.5.4.6)</td>
</tr>
<tr>
<td>Postal code (optional)</td>
<td>Optional</td>
<td>postalCode (OID 2.5.4.17)</td>
</tr>
</tbody>
</table>

Table 3: Physical address of Place of Business Certificate Fields

### 9.2.8 Other Subject Attributes

When all other optional attributes are present within the subject field, **thawte** inserts only information that has been verified. Fully-Qualified Domain Names are not to be included in Subject attributes except as stipulated for Subject Organization name in section 9.2.1 and Subject Organization Information is included only as stipulated for Subject Information in section 9.2 of this Appendix.

Optional subfields within the Subject field either contain information verified by **thawte** or are left empty. **thawte** does not use metadata such as ".", "-", and " " characters, and/or any other indication that the field is empty, absent or incomplete.

### 9.3 Certificate Policy Identification

#### 9.3.1 EV Certificate Policy Identification Requirements

Certificates issued containing the policy identifier(s) specified following are managed by **thawte** in accordance with the CAB Forum EV Guidelines.

#### 9.3.2 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

#### 9.3.3 Root CA Certificate

**thawte**’s Root CA Certificate for EV Certificates is the **thawte** Primary Root CA. This Root CA does not contain the certificatePolicies but does contain the extendedKeyUsage field.

#### 9.3.4 EV Subordinate CA Certificate

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

### 9.4 Maximum Validity Period

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

### 9.5 Subscriber Public Key
“thawte” Certificates meet the requirements for algorithm type and key size as set forth in section 6.1.5 of this CPS. See Appendix B2 for minimum cryptographic algorithm and key sizes.

**9.6 Certificate Serial Number**

“thawte” CAs generate non-sequential certificate serial numbers that exhibit at least 20 bits of entropy.

**9.7 Other Technical Requirements for EV Certificates**

See Appendix B2 for minimum cryptographic algorithm and key sizes. See Appendix B3 for required certificate extensions for EV Certificates.

10. EV CERTIFICATE REQUEST REQUIREMENTS

10.1 General Requirements

10.1.1 Documentation Requirements

Prior to the issuance of an EV Certificate, “thawte” obtains documentation from the Applicant as set forth in section 10.1, Appendix D, Supplemental Baseline Requirements.

10.1.2 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.

- **Applicant Representative**: In the case where the CA and the Subscriber are affiliated, Terms of Use applicable to the requested EV Certificate MUST be acknowledged and agreed to by an authorized Applicant Representative. An Applicant Representative is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to acknowledge and agree to the Terms of Use.
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.

10.2 EV Certificate Request Requirements

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 section 10.2, Appendix D, Supplemental Baseline Requirements, subject to the aging and updating requirements set forth in Section 11.13 of this Appendix.

10.3 Subscriber Agreement Requirements

Prior to the issuance of the EV Certificate, thawte obtains the Applicant's agreement to a legally enforceable Subscriber Agreement in accordance with section 10.3, Appendix D, Supplemental Baseline Requirements.

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.

Additionally, where the Certificate Request does not contain all necessary information about the Applicant, thawte confirms the data with the Certificate Approver or Contract Signer rather than the Applicant.

11. INFORMATION VERIFICATION REQUIREMENTS

11.1 General Overview

This section 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.

11.2 Verification of Applicant's Legal Existence and Identity

(1) Private Organization Subjects

Legal Existence. 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 or Registration Agency in Applicant’s Jurisdiction of Incorporation, and designated on the records of the Incorporating or Registration 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.

Organization Name. thawte verifies that the Applicant’s formal legal name as recorded with the Incorporating or Registration Agency in Applicant’s Jurisdiction of Incorporation or Registration matches Applicant’s name in the EV Certificate Request.

Registration Number. thawte obtains and records the specific unique Registration Number assigned to Applicant by the Incorporating or Registration Agency in the Applicant’s Jurisdiction of Incorporation or Registration. Where the Incorporating or Registration Agency does not assign a Registration Number, the thawte obtains and records the Applicant’s date of Incorporation or Registration.

Registration Agent. 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.
(2) Government Entity Subjects
Legal Existence, Entity Name and Registration Number. thawte verifies that the Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates, and that Applicant’s formal legal name matches Applicant’s name in the EV Certificate Request. thawte will obtain Applicant’s date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, thawte will enter appropriate language to indicate that the Subject is a Government Entity.

Government Entities are verified directly with, or obtained directly from, one of the following:
- a QGIS in the political subdivision in which such Government Entity operates; or
- A superior governing Government Entity in the same political subdivision as Applicant (e.g. a Secretary of State may verify the legal existence of a specific State Department), or
- From a judge that is an active member of the federal, state or local judiciary within that political subdivision, or
- An attorney representing the Government Entity.

Such verification MAY be by direct contact with the appropriate Government Entity in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source.

Any communication from a judge SHALL be verified in the same manner as is used for verifying factual assertions that are asserted by an Attorney as set forth in Section 11.10.1 of this Appendix.

(3) Business Entity Subjects
Legal Existence. To verify a Business Entity’s legal existence and identity thawte verifies that the Entity is engaged in business under the name submitted by Applicant in the Application.

Organization Name. thawte verifies that the Applicant’s formal legal name as recognized by the Registration Authority in Applicant’s Jurisdiction of Registration matches Applicant’s name in the EV Certificate Request.

Registration Number. thawte records the specific unique Registration Number assigned to Applicant by the Registration Agency in Applicant’s Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, the Applicant’s date of Registration will be recorded.

Principal Individual. In addition, the identity of a Principal Individual associated with the Business Entity is verified in accordance with Section 14(b)(4) of the EV Guidelines.

(4) Non-Commercial Entity Subjects (International Organization)
Legal Existence and Entity Name. thawte verifies that Applicant is a legally recognized International Organization Entity and that Applicant’s formal legal name matches Applicant’s name in the EV Certificate Request.

Registration Number. thawte will also obtain Applicant’s date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances where this information is not available, thawte will enter appropriate language to indicate that the Subject is an International Organization Entity.

The International Organization Entity is verified either:
- With reference to the constituent document under which the International Organization was formed; or
- Directly with a signatory country's government in which thawte is permitted to do business. Such verification may be obtained from an appropriate government agency or from the laws of that country, or by verifying that the country's government has a mission to represent it at the International Organization; or
• directly against any current list of qualified entities that the CA/Browser Forum may maintain at www.cabforum.org.

• In cases where the International Organization applying for the EV certificate is an organ or agency - including a non-governmental organization (NGO) of a verified International Organization, then thawte may verify the International Organization applicant directly with the verified umbrella International Organization of which the applicant is an organ or agency.

11.3 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 or Registration 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.

11.4 Verification of Applicant’s Physical Existence

11.4.1 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 or a Parent/Subsidiary Company conducts business operations (e.g., not a mail drop or P.O. Box), and is the address of Applicant’s Place of Business.

For Government Entity Applicants, the address contained in the records of the QGIS in Applicant’s Jurisdiction shall be regarded as the verified address.

For other entities, 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, or a Qualified Governmental Tax Information Source(QGTIS), thawte confirms that the Applicant’s address as listed in the EV Certificate Request is a valid business address for Applicant or a Parent/Subsidiary Company by reference to such Qualified Independent Information Sources, or a QGTIS, 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, or a QGTIS, thawte may confirm that the address provided by the Applicant in the EV Certificate Request is in fact the Applicant’s or a Parent/Subsidiary Company 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 or Registration, thawte requires a Verified Legal Opinion that indicates the address of Applicant’s or a Parent/Subsidiary Company’s Place of Business and that business operations are conducted there.

11.4.2 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. A listing in a Parent/Subsidiary Company’s name at that address is acceptable.

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 a Qualified Governmental Tax Information Source; or

(B) During a site visit, the person who is conducting the site visit MUST confirm the Applicant’s or Parent/Subsidiary Company’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.

For Government Entity Applicants, thawte may rely on the telephone number contained in the records of the QGIS in Applicant’s Jurisdiction.

During the telephone verification process detailed in Section 11.8.1 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.

11.5 Verification of Applicant’s Operational Existence

If the records of the Incorporating or Registration Agency indicates that the Applicant has been in existence for less than three (3) years, and the Applicant is not listed in either the current version of one (1) Qualified Independent Information Source or a Qualified Governmental Tax Information Source, thawte verifies that the Applicant has the ability to engage in business. If the Applicant is a Subsidiary or Affiliate of an entity that thawte has successfully verified as in existence for three or more years, then thawte MAY rely on the existence of the Parent or Affiliate as verification of the Applicant’s operational existence.

In the absence of a verified legal or Accountant opinion confirming an active current Demand Deposit Account with a regulated financial institution, 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.
11.6 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.
   For Government Entity Applicants, the CA MAY rely on the domain name listed for that entity in the records of the QGIS in Applicant’s Jurisdiction to verify Domain Name.
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. Confirmation that the registered owner of the domain name is a Parent/Subsidiary Company of Applicant, or a registered trading name of Applicant is sufficient to establish that Applicant is the registered owner of the domain name.

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\(^2\) 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, that it controls the confirmed domain name.

In cases where the registered domain holder cannot be contacted, _thawte_ shall:
   o 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**
   o 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;

_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.

11.7 Verification of Name, Title and Authority of Contract Signer and Certificate Approver

11.7.1 Verification Requirements

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

---

\(^2\) If the Top-Level Domain is a generic top-level domain (gTLD) such as .com, .net, or .org in accordance with RFC 1591, _thawte_ MUST obtain positive confirmation from the second-level domain registration holder. If the Top-Level Domain is a 2 letter Country Code Top-Level Domain (ccTLD), _thawte_ MUST obtain positive confirmation from the domain holder at the appropriate domain level, based on the rules of the ccTLD.
(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) **Signing Authority 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) **EV Authority 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.

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.

### 11.7.2 **Verification – Name, Title and Agency**

In the absence of a verified legal opinion, *thawte* may verify the 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.

### 11.7.3 **Verification – Authority**

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) **Prior Equivalent Authority:** The signing authority of the Contract Signer, and/or the EV authority of
the Certificate Approver, MAY be verified by relying on a demonstration of Prior Equivalent
Authority.

Prior Equivalent Authority of a Contract Signer MAY be relied upon for confirmation or verification
of the signing authority of the Contract Signer when the Contract Signer has executed a binding
contract between *thawte* and/or its parents or Subsidiaries and the Applicant with a legally valid
and enforceable seal or handwritten signature and only when the contract was executed more
than 90 days prior to the EV certificate application. *thawte* will record sufficient details of the
previous agreement to correctly identify it and associate it with the EV application. Such details
MAY include any of the following:

1. Agreement title Date of Contract Signer's signature
2. Contract reference number
3. Filing location

Prior Equivalent Authority of a Certificate Approver MAY be relied upon for confirmation or
verification of the EV authority of the Certificate Approver when the Certificate Approver has
performed one or more of the following:

(1) Under contract to *thawte* and/or a Parent/Subsidiary, has served (or is serving) as an
Enterprise RA for the Applicant

(2) Has participated in the approval of one or more SSL certificates issued by the CA, which are
currently in use on public servers operated by the Applicant. In this case *thawte* and/or a
Parent/Subsidiary MUST have contacted the Certificate Approver by phone at a previously
validated phone number or have accepted a signed and notarized letter approving the
certificate request.

11.7.4 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.

11.8 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.

11.8.1 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.

11.8.2 Methods of Signature Verification

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.

11.9 Verification of Approved 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.

11.10 Verification of Certain Information Sources

11.10.1 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 Registration 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 Registration 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. In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the CA in Section 11.10.1(1)(A), Status of Author of Legal Opinion, no further verification of authenticity is required.

11.10.2 Verified Accountant Letter

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 Registration 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. In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the CA in Section 11.10.2(1)(A), Status of Author of Accountant Letter, no further verification of authenticity is required.

11.10.3 Face-to-Face Validation of Principal Individual

Before relying on any face-to-face vetting documents *thawte* verifies that the Third-Party Validator meets the following requirements:

(A) Qualification of Third-Party Validator. *thawte* independently verifies that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in Applicant’s jurisdiction), Lawyer, or Accountant in the jurisdiction of the individual’s residency, by directly contacting the authority responsible for registering or licensing such Third-Party Validators in the applicable jurisdiction.

(B) Document chain of custody. *thawte* verifies that that the Third-Party Validator viewed the Vetting Documents in a face-to-face meeting with the individual being validated. The Third party validator must attest that they obtained the Vetting Documents submitted to the CA for the individual during a face-to-face meeting with the individual.

(C) Verification of Attestation. If the Third-Party Validator is not a Latin Notary, then *thawte* confirms the authenticity of the attestation and vetting documents, by making a telephone call to the Third-
Party Validator and obtaining confirmation from them or their assistant that they performed the face-to-face validation. *thawte* may rely upon self-reported information obtained from the Third-Party Validator for the sole purpose of performing this verification process. In circumstances where the attestation is digitally signed, in a manner that confirms the authenticity of the documents, and the identity of the signer as verified by *thawte* in Section 11.10.3(A), Qualification of Third-Party Validator above, no further verification of authenticity is required.

### 11.10.4 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) Addresssee:** 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 or Registration as listed in the official records of the Incorporating or Registration Agency, with instructions that it be forwarded to an appropriate Confirming Person.

   (iii) A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting Applicant’s Human Resources Department by phone or mail (at the verified phone number or address for Applicant’s Place of Business)

   **(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 Qualified Government Tax 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.

**thawte** MAY rely on a verified Confirming Person to confirm their own contact information: email address, telephone number, and facsimile number. **thawte** may rely on this verified contact information for future correspondence with the Confirming Person if:

1. The domain of the e-mail address is owned by the Applicant and is the Confirming Person's own e-mail address and not a group e-mail alias,
2. The Confirming Person's telephone/fax number is verified by **thawte** to be a telephone number that is part of the organization's telephone system, and is not the personal phone number for the person.

**11.10.5 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.

**11.10.6 Qualified Government Information Sources (QGIS)**

Government Information Sources used by **thawte** for verifying EV certificate application information meet the databases requirements required by the Guidelines. **thawte** may use third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.

**11.10.7 Qualified Government Tax Information Sources (QGTIS)**

A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g. the I.R.S. in the United States).

**11.11 Other Verification Requirements**

**11.11.1 High Risk Status**

**thawte** processes High Risk requests in accordance with Section 11.5, Appendix D, Supplemental Baseline Requirements.

**11.11.2 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 Registration 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 Registration or Place of Business in any country with which the laws of **thawte**’s jurisdiction prohibit doing business

- 91 -
thawte takes reasonable steps to verify EV Certificate applications with the following lists and regulations:

(A) For CA operations in the U.S., thawte takes reasonable steps to verify with the following US Government Denied lists and regulations:
   (i) BIS Denied Persons List, www.bis.doc.gov/dpl/thedeniallist.asp
   (ii) BIS Denied Entities List, www.bis.doc.gov/Entities/Default.htm
   (iv) US Government export regulations

(B) When operating in a country other than the U.S., thawte takes reasonable steps to verify with all equivalent denied lists and export regulations in such country.

11.11.3 Parent/Subsidiary/Affiliate Relationship

thawte verifies an Applicant based on information of the Applicant's Parent, Subsidiary or Affiliate, as set forth in Sections 11.4.1, 11.4.2, 11.5 and 11.6 of this Appendix. Such Applicant relationships shall be validated using the following sources:

1) QIIS or QGIS: The relationship between the Applicant and the Parent, Subsidiary, or Affiliate is identified in a QIIS or QGIS;
2) Independent Confirmation from the Parent, Subsidiary, or Affiliate: thawte MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by obtaining an Independent Confirmation from the appropriate Parent, Subsidiary, or Affiliate (as described in Section 11.10.4 of this Appendix);
3) Contract between CA and Parent, Subsidiary, or Affiliate: thawte MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a contract between the CA and the Parent, Subsidiary, or Affiliate that designates the Certificate Approver with such EV Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;
4) Legal Opinion: thawte MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a Verified Legal Opinion (as described in Section 11.10.1 of this Appendix);
5) Accountant Letter: thawte MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a Verified Accountant Letter (as described in Section 11.10.2 of this Appendix); or
6) Corporate Resolution: thawte MAY verify the relationship between an Applicant and a Subsidiary by relying on a properly authenticated corporate resolution that approves creation of the Subsidiary or the Applicant, provided that such resolution is (i) certified by the appropriate corporate officer (e.g., secretary), and (ii) the CA 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.

11.12 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.

11.13 Requirements for Re-Use of Existing Documentation

11.13.1 For Validated Data

1) 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 – 13 months;
- Assumed name – 13 months;
- Address of Place of Business – 13 months, 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 – 13 months;
- Bank account verification – 13 months;
- Domain name – 13 months;
- Identity and authority of Certificate Approver – 13 months, 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.

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) 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 stated above. Each EV Certificate issued by thawte is supported by a valid and current EV Certificate Request and a Subscriber Agreement signed by the appropriate Applicant Representative on behalf of the Applicant or Terms of Use acknowledged by the appropriate Applicant Representative.

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

11.13.2 Validation of Existing Subscribers

In conjunction with an EV Certificate Request placed by an Applicant who is already a customer of thawte, thawte performs all authentication and verification tasks required by this CPS to ensure that the request is properly authorized by Applicant and that the information in the EV Certificate is still accurate and valid.

11.13.3 Exceptions

Notwithstanding the requirements set forth in Section 11.13.1 and 11.13.2 (Use of Pre-Existing Information or Documentation and Maximum Validity Period), thawte, when performing the authentication and verification tasks for renewal of an EV Certificate previously issued by thawte MAY:

(1) Rely on its prior authentication and verification of:

(A) A Principal Individual of a Business Entity under Section 11.2.2(4) of the EV Guidelines if the Principal Individual is the same as the Principal Individual verified by the CA in connection with the previously issued EV Certificate,

(B) Applicant's Place of Business under Section 11.4.1,

(C) The verification of telephone number of Applicant's Place of Business required by Section 11.4.2, but still MUST perform the telephone verification required by Section 11.4.2(B) such that a reasonable person may conclude that the Applicant is reachable by telephone at the number dialed,

(D) Applicant's Operational Existence under Section 11.5,

(E) The name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester under Section 11.7, except where a contract is in place between thawte and Applicant that specifies a specific term for the authority of the Contract Signer, and/or the Certificate Approver, and/or Certificate Requester in which case, the term specified in such contract will control,

(F) The prior verification of the email address used by thawte for independent confirmation from applicant under Section 11.10.4(1)(B)(ii), Communication by Email.
(2) Rely on prior Verified Legal/Accountant Opinion that established:

(A) Applicant's exclusive right to use the specified domain name under Section 11.6.2 (2)(A)(i) and 11.6.2 (2)(B)(i) of the EV Guidelines, provided that thawte verifies that either:

(i). The WHOIS record still shows the same registrant as indicated when thawte received the prior Verified Legal Opinion, or

(ii). The Applicant establishes domain control via a practical demonstration as detailed in Section 11.6.2 (2)(B)(ii) of the EV Guidelines.

(B) Verification that Applicant is aware that it has exclusive control of the domain name, under Section 11.6.2 (3) of the EV Guidelines.

11.13.4 Validation for Re-issuance Requests

thawte may rely on previously verified information to issue a replacement certificate where:

(1) The expiration date of the replacement certificate is the same as the expiration date of the currently valid EV Certificate that is being replaced, and

(2) The Subject of the Certificate is the same as the Subject in the currently valid EV Certificate that is being replaced.

12. CERTIFICATE ISSUANCE BY A ROOT CA

thawte enforces multi-person controls for certificate issuance by the Root CA. The Root CA Private Keys are not used to sign EV Certificates.

13. CERTIFICATE REVOCATION AND STATUS CHECKING

EV Certificate revocation is performed in accordance with Section 13, Appendix D, Supplemental Baseline Requirements.

thawte provides the capability for CRLs for an EV Certificate chain to be downloaded in no more than three (3) seconds over an analog telephone line under normal network conditions.

14. EMPLOYEE AND THIRD PARTY ISSUES

14.1 Trustworthiness and Competence

14.1.1 Identity and Background Verification

In addition to the procedures described in Sections 5.2 and 5.3 of this 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).

14.1.2 Training and Skill Level

thawte requires all Validation Specialists to pass an internal examination on the EV Certificate validation criteria as set forth in section 14.1.2, Appendix D, Supplemental Baseline Requirements.
14.1.3 Separation of Duties

thawte enforces separation of duties in accordance with section 5.2.4 of the CPS, to ensure that one single individual validates and authorizes the issuance of an EV Certificate. All steps of the EV Certificate Application process are logged and auditable.

14.2 Delegation of Functions to Registration Authorities and Subcontractors

14.2.1 General

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 11.12 of this Appendix.

14.2.2 Enterprise RAs

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:

1. 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;
2. In all cases, the Subject of an Enterprise EV Certificate MUST be an organization verified by thawte in accordance with these Guidelines;
3. thawte will impose these limitations as a contractual requirement with the Enterprise RA and monitor compliance by an authorized Customer Administrator;
4. The Final Cross-Correlation and Due Diligence requirements of Section 11.12 of this Appendix MAY be performed by the Enterprise RA, and;
5. When thawte does NOT maintain control of the Root CA Private Key or Subordinate Issuing CA Private key, the Enterprise RA SHALL be audited in accordance with section 17.1

14.2.3 Guideline Compliance Obligation

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.

14.2.4 Allocation of Liability

As specified in Section 14.2.3, Appendix D, Supplemental Baseline Requirements.

15. DATA RECORDS

Data Records are captured and retained for EV Certificates in accordance with Section 15, Appendix D, Supplemental Baseline Requirements.

16. DATA SECURITY

thawte enforces data security in accordance with Section 16, Appendix D, Supplemental Baseline Requirements.
17. AUDIT

17.1 Annual Independent Audit

_thawte_ undergoes an annual

(i) WebTrust Program for CAs v2.0 or later audit as set forth in section 8 of this CPS, and
(ii) WebTrust EV Program audit, or
(iii) an equivalent for both (i) and (ii) as approved by the CA/Browser Forum.

Such audits will cover all CA obligations under the CA/Browser Forum Guidelines regardless of whether they are performed directly by _thawte_ or delegated to an RA or subcontractor.

17.2 Audit Period

_thawte_ undergoes an annual audit as set forth in Section 17.1

17.3 Audit Record

The audit report is made publicly available by _thawte_ as set forth in section 8.6 of this CPS.

17.4 Pre-Issuance Readiness Audit

Before issuing EV Certificates _thawte_ shall successfully complete a point-in-time readiness assessment audit against the WebTrust EV Program.

17.5 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.

17.6 Auditor Qualifications

All audits required under the Guidelines are performed by a Qualified Auditor as set forth in section 8.2 of this CPS. Such 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

17.7 Root CA Key Pair Generation

For CA root keys generated after the release of these Guidelines, _thawte_ ensures that the Qualified Auditor is present to 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 opinion that _thawte_, during its root key and certificate generation process:
(1) 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);
(2) 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;
(3) 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
(4) 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 is recorded for auditing purposes.

18. LIABILITY AND INDEMNIFICATION

As specified in Section 18, Appendix D, Supplemental Baseline Requirements.
APPENDIX B2: Minimum Cryptographic Algorithm and Key Sizes for EV Certificates

1. Root CA Certificates

<table>
<thead>
<tr>
<th>Digest algorithm</th>
<th>Key sizes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-1*, SHA-256, SHA-384 or SHA-512</td>
<td>RSA 2048 bit</td>
</tr>
<tr>
<td>ECC</td>
<td>256 or 384 bits</td>
</tr>
</tbody>
</table>

2. Subordinate CA Certificates

<table>
<thead>
<tr>
<th>Digest algorithm</th>
<th>Key sizes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-1*, SHA-256, SHA-384 or SHA-512</td>
<td>RSA 2048 bit</td>
</tr>
<tr>
<td>ECC</td>
<td>256 or 384 bits</td>
</tr>
</tbody>
</table>

3. Subscriber Certificates

<table>
<thead>
<tr>
<th>Digest algorithm</th>
<th>Key sizes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA1*, SHA-256, SHA-384 or SHA-512</td>
<td>RSA 2048 bit</td>
</tr>
<tr>
<td>ECC</td>
<td>256 or 384 bits</td>
</tr>
</tbody>
</table>

*SHA-1 shall be used until SHA-256 is supported widely by browsers used by a majority of Relying Parties worldwide.
APPENDIX B3: EV Certificates Requiring 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.

(c) certificatePolicies

This extension SHOULD NOT be present.

(d) extendedKeyUsage

This extension is not present.

All other fields and extensions set in accordance to RFC 5280.

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 EV policy if the certificate is issued to a subordinate CA that is not controlled by thawte.

certificatePolicies:policyIdentifier (Required)
   o The anyPolicy identifier if subordinate CA is controlled by thawte
   o explicit EV policy OID(s) if subordinate CA is not controlled by thawte

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

   certificatePolicies:policyQualifiers:policyQualifierId
      o id-qt 2 [RFC 5280]

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

(b) cRLDistributionPoint

is always present and NOT marked critical. It contains the HTTP URL of thawte’s CRL service.

(c) authorityInformationAccess

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

(d) basicConstraints
This extension MUST be present and MUST be marked critical 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 MUST be set in accordance to RFC 5280.

3. **Subscriber Certificate**

(a) **certificatePolicies**

MUST be present and SHOULD NOT be marked critical. The set of policyIdentifiers MUST include the identifier for thawte’s EV policy.

```
certificatePolicies:policyIdentifier (Required)
  ○ EV policy OID

certificatePolicies:policyQualifiers:policyQualifierId (Required)
  ○ id-qt 2 [RFC 5280]
certificatePolicies:policyQualifiers:qualifier (Required)
  ○ URI to the Certificate Practice Statement
```

(b) **cRLDistributionPoint**

is always present and NOT marked critical.

(c) **authorityInformationAccess**

is always present and NOT 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 CA certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

(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.

(f) **extKeyUsage**

Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. Other values SHOULD NOT be present.

(f) **SubjectAltName**

populated in accordance with RFC5280 and criticality is set to FALSE.

All other fields and extensions set in accordance to RFC 5280.
APPENDIX B4: Foreign Organization Guidelines

NOTE: This appendix is only relevant to EV applications from countries that do not have Latin character organization name registrations. More specific information for particular countries may be added to this appendix in the future.

Where an EV Applicant's organization name is not registered with a QGIS in Latin characters and the applicant's foreign character organization name and registration have been verified with a QGIS in accordance with these Guidelines, thawte MAY include a Latin character organization name in the EV certificate. In such a case, thawte will follow the procedures laid down in this appendix.

Romanized Names
In order to include a transliteration/Romanization of the registered name, the Romanization will be verified by the CA using a system officially recognized by the Government in the Applicant's jurisdiction of incorporation.

If thawte can not rely on a transliteration/Romanization of the registered name using a system officially recognized by the Government in the Applicant's jurisdiction of incorporation, then it MUST rely on one of the options below, in order of preference:

- A system recognized by the International Standards Organization (ISO),
- A system recognized by the United Nations or
- A Lawyers Opinion confirming the Romanization of the registered name.

English Name
In order to include a Latin character name that is not a Romanization of the registered name in the EV certificate, thawte will verify that the Latin character name is:

- Included in the Articles of Incorporation (or equivalent document) filed as part of the organization registration, or
- Recognized by a QGTIS in the Applicant's Jurisdiction of Incorporation as the applicant's recognized name for tax filings, or
- Confirmed with a QIIS to be the name associated with the registered organization, or
- Confirmed by a lawyer's opinion letter to be the trading name associated with the registered organization.

Country Specific Procedures

F-1. Japan
In addition to the procedures set out above:

- The Hepburn method of Romanization is acceptable for Japanese Romanizations.
- thawte MAY verify the Romanized transliteration of Applicant's formal legal name with either a QIIS or a lawyer's opinion letter.
- thawte MAY use the Financial Services Agency to verify an English Name. When used, thawte will verify that the English name is recorded in the audited Financial Statements filed with the Financial Services Agency.
- When relying on Articles of Incorporation to verify an English Name, the Articles of Incorporation MUST be accompanied either: by a document, signed with the original Japanese Corporate Stamp, that proves that the Articles of Incorporation are authentic and current, or by a lawyer's opinion letter. thawte will verify the authenticity of the Corporate Stamp.
APPENDIX C
Supplemental Validation Procedures for Extended Validation (EV)
Code-Signing Certificates

Reference: CA/Browser Forum Guidelines for the Issuance and Management of

TABLE OF CONTENTS

1 Scope
2 Purpose
3 References
4 Definitions
5 Abbreviations and Acronyms
6 Conventions
7 Certificate Warranties and Representations
   7.1 EV Code Signing Certificate Warranties
   7.2 By the Applicant
8 Community and Applicability
   8.1 Issuance of EV Code Signing Certificates
   8.2 EV Code Signing Policies
   8.3 Commitment to Comply with Recommendations
   8.4 Insurance
   8.5 Obtaining EV Code Signing Certificates
9 EV Certificate Content and Profile
   9.1 Issuer Information
   9.2 Subject Information
      9.2.1 Subject Organization name
      9.2.2 Subject Alternate name Extension
      9.2.3 Common name
      9.2.4 Subject Business Category
      9.2.5 Subject Jurisdiction of Incorporation or Registration
      9.2.6 Subject Registration Number
      9.2.7 Subject Physical Address of Place of Business
      9.2.8 Other Subject Attributes
   9.3 Certificate Policy Identification
   9.4 Maximum Validity Period For EV Code Signing Certificate
   9.5 Subscriber Public Key
   9.6 Certificate Serial Number
   9.7 Additional Technical Requirements for EV Code Signing Certificates
10 EV Code Signing Certificate Request Requirements
   10.1 General Requirements
   10.2 EV Code Signing Certificate Request Requirements
   10.3 Requirements for Subscriber Agreement and Terms of Use
      10.3.1 General
      10.3.2 Agreement Requirements
11 Verification Requirements
   11.1 General Overview
   11.2 Verification of Applicant’s Legal Existence and Identity
   11.3 Verification of Applicant’s Legal Existence and Identity – Assumed Name
   11.4 Verification of Applicant’s Physical Existence
   11.5 Verification of Applicant’s Operational Existence
   11.6 Verification of Applicant’s Domain Name
   11.7 Verification of Name, Title, and Authority of Contract Signer and Certificate Approver
   11.8 Verification of Signature on Subscriber Agreement and EV Code Signing Certificate Requests
   11.9 Verification of Approval of EV Code Signing Certificate Request
   11.10 Verification of Certain Information Sources
   11.11 Other Verification Requirements
   11.12 Final Cross-Correlation and Due Diligence
11.13 Requirements for Re-use of Existing Documentation

12 Certificate Issuance by a Root CA

13 Certificate Revocation and Status Checking

14 Employee and third party issues
   14.1 Trustworthiness and Competence
   14.2 Delegation of Functions to Registration Authorities and Subcontractors

15 Data Records

16 Data Security

17 Audit
   17.1 Eligible Audit Schemes
   17.2 Audit Period
   17.3 Audit Record
   17.4 Pre-Issuance Readiness Audit
   17.5 Regular Self Audits
   17.6 Auditor Qualification
   17.7 Root CA Key Pair Generation

18 Liability and Indemnification
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") used for EV signatures in code-signing. Such EV code-signing attests to only one level of assurance in code.

Subject Organization information from Valid EV Code Signing Certificates may be displayed in a special manner by certain relying-party software applications in order to provide users with a trustworthy confirmation of the identity of the entity providing the code signing services.

2. PURPOSE

2.1 Purpose of EV Code Signing Certificates

EV Code Signing ("EV CS") Certificates and signatures are intended to be used to verify the identity of the certificate holder (Subscriber) and the integrity of its code. They provide assurance to a user or platform provider that code verified with the certificate has not been modified from its original form and is distributed by the legal entity identified in the EV Code Signing Certificate by name, Place of Business address, Jurisdiction of Incorporation or Registration, and other information. EV Code Signing Certificates may help to establish the legitimacy of signed code, help to maintain the trustworthiness of software platforms, help users to make informed software choices, and limit the spread of malware.

The EV Code Signing Certificate does not identify a particular software object, but only its distributor.

2.1.1 Secondary Purposes

As specified in Section 2.1, Appendix B1, EV SSL Certificates.

2.1.2 Excluded Purposes

EV CS Certificates focus only on assuring the identity of the Subscriber and that the signed code has not been modified from its original form. EV Code Signing Certificates are not intended to provide any other assurances, representations, or warranties. Specifically, EV Code Signing Certificates do not warrant that code is free from vulnerabilities, malware, bugs, or other problems. EV Code Signing Certificates do not warrant or represent that:

i. The Subject named in the EV Code Signing Certificate is actively engaged in doing business;
ii. The Subject named in the EV Code Signing Certificate complies with applicable laws;
iii. The Subject named in the EV Code Signing Certificate is trustworthy, honest, or reputable in its business dealings; or
iv. It is “safe” to install code distributed by the Subject named in the EV Code Signing Certificate.

3. REFERENCES

Refer to References provided in the CA/Browser Forum EV Code-Signing Guidelines located at http://cabforum.org/documents.html.

4. DEFINITIONS

Refer to Definitions provided in the CA/Browser Forum EV Code-Signing Guidelines located at http://cabforum.org/documents.html.
5. ABBREVIATIONS AND ACRONYMS

Refer to Abbreviations and Acronyms provided in the CA/Browser Forum EV Code-Signing Guidelines located at http://cabforum.org/documents.html.

6. CONVENTIONS

No stipulation.

7. CERTIFICATE WARRANTIES AND REPRESENTATIONS

7.1 EV Code Signing Certificate Warranties

When thawte issues an EV Code Signing Certificate, the thawte Issuing and Root CA represents and warrants to the Certificate Beneficiaries listed in Section 7.1.1, Appendix D, Supplemental Baseline Requirements, during the period when the EV Code Signing Certificate is Valid, that thawte has followed the requirements of these Guidelines and its EV Policies in issuing and managing the EV Code Signing Certificate and in verifying the accuracy of the information contained in the EV Code Signing Certificate.

These warranties specifically include, but are not limited to, the following:

(A) Legal Existence: thawte has confirmed with the Incorporating or Registration Agency in the Subject’s Jurisdiction of Incorporation or Registration that, as of the date the EV Code Signing Object was issued, the Subject of the EV Code Signing Object legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;

(B) Identity: thawte has confirmed that, as of the date the EV Code Signing Object was issued, the legal name of the Subject named in the EV Code Signing Object matches the name on the official government records of the Incorporating or Registration Agency in the Subject’s Jurisdiction of Incorporation or Registration, 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;

(C) Authorization for EV Code Signing Certificate: thawte has taken all steps reasonably necessary to verify that the Subject of the EV Code Signing Object authorized the issuance of the EV Code Signing Object;

(D) Accuracy of Information: thawte has taken all steps reasonably necessary to verify that all of the other information in the EV Code Signing Object is accurate, as of the date of issuance;

(E) Subscriber Agreement: The Subject of the EV Code Signing Object has entered into a legally valid and enforceable Subscriber Agreement with thawte that satisfies the requirements of these Guidelines or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;

(F) Status: The Issuer 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 Code Signing Object as Valid or revoked; and

(G) Revocation: thawte will follow the requirements of these Guidelines and revoke the EV Code Signing Object for any of the revocation reasons specified in these Guidelines.

7.2 By the Applicant

Applicants make the commitments and warranties set forth in Section 10.3.2 of this Appendix for the benefit of the Issuer and the Certificate Beneficiaries.
8. COMMUNITY AND APPLICABILITY

8.1 Issuance of EV Code Signing Certificates

When issuing EV CS Certificates, thawte shall at all times satisfy the requirements as required by the Guidelines and set forth in this Appendix.

thawte shall at all times comply with all laws applicable to its business and the certificates it issues in each jurisdiction where it operates. thawte shall notify the CA / Browser Forum of any occasions whereby a court or government body with jurisdiction over the activities (operations or certificate issuances) that are covered by the Guidelines determines that the performance of any mandatory requirement is deemed illegal subject to the laws of that jurisdiction.

8.2 EV Code Signing Policies

8.2.1 Implementation

The thawte CPS, together with this Supplemental Appendix C to the thawte CPS:

- Implements the requirements of the Guidelines as they are revised from time-to-time;
- Implements 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;
- Specifies thawte’s entire root certificate hierarchy including all roots that its EV Certificates depend on for proof of those EV Certificates’ authenticity. See section 8.2.1, Appendix B1 for thawte’s root hierarchy structure.

8.2.2 Disclosure

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

thawte publicly discloses its CA business practices through an annual WebTrust for CAs Audit in accordance with section 8 of this CPS.

8.3 Commitment to Comply with Recommendations

thawte conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Code Signing Certificates published at 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 includes (directly or by reference) the applicable requirements of these Guidelines in all contracts with subordinate CA, RAs, Enterprise RAs, and subcontractors, that involve or relate to the issuance or maintenance of EV Code Signing Certificates. thawte will enforce compliance with such terms.

8.4 Insurance

thawte maintains insurance as specified in Section 8.4, Appendix B1, EV SSL Certificates.

8.5 Obtaining EV Code Signing Certificates

thawte only issues EV Code Signing Certificates to Applicants that meet the requirements specified in Section 8.5, Appendix B1, EV SSL Certificates.
9. EV CERTIFICATE CONTENT AND PROFILE

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

9.1 Issuer Information

An EV Code Signing Certificate MUST include Issuer information as specified by Baseline Requirements for publicly trusted Certificates and set forth in section 9.1, Issuer Information, Appendix D, Supplemental Baseline Requirements.

9.2 Subject Information

EV Code Signing Objects issued to Subscribers MUST include the following information about the Subject organization in the fields listed:

9.2.1 Subject Organization Name Field

As specified in Section 9.2.1 of Appendix B1, EV SSL Certificates.

9.2.2 Subject Alternative Name Extension

This field should not be included in the EV Code Signing Objects.

9.2.3 Subject Common Name Field

Certificate field: subject:commonName (OID: 2.5.4.3)

Required/Optional: Deprecated (Discouraged, but not prohibited)
Contents: If present, this field MUST NOT contain a Domain Name.

9.2.4 Subject Business Category Field

As specified in Section 9.2.4 of Appendix B1, EV SSL Certificates.

9.2.5 Subject Jurisdiction of Incorporation or Registration Field

As specified in Section 9.2.5 of Appendix B1, EV SSL Certificates.

9.2.6 Subject Registration Number Field

As specified in Section 9.2.6, Appendix B1, EV SSL Certificates.

9.2.7 Subject Physical Address of Place of Business Field

As specified in Section 9.2.7, Appendix B1, EV SSL Certificates.

9.2.8 Other Subject Attributes

All other optional attributes, when present within the subject field, MUST contain information that has been verified by thawte. Optional subfields within the Subject field MUST either contain information verified by the Issuer or MUST be left empty. Metadata such as ‘.’, ‘-‘, and ‘‘ characters, and/or any other indication that the field is empty, absent or incomplete, MUST not be used.

9.3 Certificate Policy Identification

As specified in Section 9.3, Appendix B1, EV SSL Certificates.

9.4 Maximum Validity Period For EV Code Signing Certificate

The validity period for an EV Code Signing Certificate issued to a Subscriber MUST NOT exceed thirty-nine (39) months.
9.5 Subscriber Public Key

_thawte_ Certificates meet the requirements for algorithm type and key size as set forth in section 6.1.5 of this CPS. See Appendix B2 for minimum cryptographic algorithm and key sizes.

9.6 Certificate Serial Number

_thawte_ CAs generate non-sequential certificate serial numbers that exhibit at least 20 bits of entropy.

9.7 Additional Technical Requirements for EV Code Signing Certificates

As specified in Section 9.7, Appendix B1, EV SSL Certificates, with the following exceptions:

(A) the Domain Name as required for EV SSL Certificates SHALL be omitted;

(B) the Certificate MUST include a **SubjectAltName:permanentIdentifier** which MUST contain the following:

1) The ISO 3166-2 country code corresponding Subject’s Jurisdiction of Incorporation or Registration (CC), as specified in the **subject:jurisdictionOfIncorporationCountryName** field;

2) If applicable, the state, province, or locality of the Subject’s Jurisdiction of Incorporation in uppercase characters as specified in the **subject:jurisdictionOfIncorporationStateorProvinceName** or **subject:jurisdictionOfIncorporationLocalityName** field, expressed in an unabbreviated format (STATE);

3) The first one of the following that applies:
   a. The Registration Number as included in the **Subject:serialNumber** field (REG), or
   b. A date of Incorporation or Registration in YYYY-MM-DD format (DATE) and the Subject’s Organization Name as included in the **organizationName** field (ORG), or
   c. A verifiable date of creation in YYYY-MM-DD format (DATE) and the Subject’s Organization Name as included in the **organizationName** field (ORG), or
   d. the Subject’s Organization Name as included in the **organizationName** field (O).

_thawte_ formats data in the **SubjectAltName:permanentIdentifier** extension using Unicode as follows: CC-STATE (if applicable)- REG or DATE (if available)-ORG (if REG is not present). Characters representing the organization name MUST be uppercase Unicode. Any included “-” characters MUST be Unicode 002D and any included spaces in REG, STATE, or ORG MUST be Unicode 0020.

_thawte_ MAY truncate or abbreviate an organization name included in this field to ensure that the combination does not exceed 64 characters provided that _thawte_ has checked this field in accordance with section 11, Appendix B1, EV SSL Certificates such that a Relying Party will not be misled into thinking that they are dealing with a different organization. If this is not possible, _thawte_ MUST NOT issue the EV Code Signing Certificate.

(C) the **keyUsage** extension MUST be set as follows:
   This extension MUST be present and MUST be marked critical. The bit position for **digitalSignature** MUST be set. All other bit positions SHOULD NOT be set; AND

(D) the extended **keyUsage** extension MUST be set as follows:
   This extension MUST be present, and the value **id-kp-codeSigning** MUST be present. Other values SHOULD NOT be present.

10. EV CODE SIGNING CERTIFICATE REQUEST REQUIREMENTS

10.1 General Requirements

As specified in Section 10.1, Appendix B1, EV SSL Certificates.
10.2 EV Code Signing Certificate Request Requirements

As specified in Section 10.2, Appendix B1, EV SSL Certificates.

10.3 Requirements for Subscriber Agreement and Terms of Use

10.3.1 General

Prior to issuing an EV Code Signing Certificate, thawte obtains, for the express benefit of the Issuer and the Certificate Beneficiaries, either:

1. The Applicant’s agreement to the Subscriber Agreement with the Issuer, or
2. The Applicant’s agreement to the Terms of Use agreement.

Prior to the issuance of the EV Code Signing 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 Code Signing Certificate to be issued pursuant to the Certificate Request. A separate Subscriber Agreement may be used for each Certificate Request, or a single Subscriber Agreement may be used to cover multiple future Certificate Requests and resulting Certificates.

10.3.2 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:

1. **Accuracy of Information**: An obligation and warranty to provide accurate and complete information at all times to thawte, both in the certificate request and as otherwise requested by thawte in connection with the issuance of the Certificate(s) to be supplied by thawte;

2. **Protection of Private Key**: An obligation and warranty by the Applicant to take all reasonable measures 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 Certificate(s) (and any associated activation data or device, e.g. password or token);

3. **Acceptance of Certificate**: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;

4. **Use of the Certificate**: An obligation and warranty to not knowingly sign software that contains Suspect Code and use the EV Code Signing Certificate as follows:
   a. only to sign code that complies with the requirements set forth in these Guidelines;
   b. solely in compliance with all applicable laws;
   c. solely for authorized company business; and
   d. solely in accordance with the Subscriber Agreement;

5. **Reporting and Revocation**: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request thawte to revoke the Certificate, in the event that:
   a. there is evidence that the certificate was used to sign suspect code;
   b. any information in the Certificate is, or becomes, incorrect or inaccurate; or
   c. there is any actual or suspected misuse or compromise of either the key activation data or the Subscriber’s Private Key associated with the Public Key included in the Certificate;

6. **Termination of Use of Certificate**: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that
Certificate for reasons of Key Compromise.

7. **Responsiveness**: An obligation to respond to thawte’s instructions concerning Key Compromise or Certificate misuse within a specified time period.

8. **Acknowledgment and Acceptance**: An acknowledgment and acceptance that thawte is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Forum Guideline Agreement or if thawte discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

11. **VERIFICATION REQUIREMENTS**

11.1 **General Overview**

This section sets forth Verification Requirements and Acceptable Methods of Verification for each such Requirement and the procedures used by thawte to satisfy the requirements.

Before issuing an EV Code Signing Certificate, thawte ensures that all Subject organization information included in the EV Code Signing Certificate conforms to the requirements of, and has been verified in accordance with the EV Guidelines and matches the information confirmed and documented by thawte pursuant to its verification processes set forth in sub-sections 11.2 through 11.13 following.

11.2 **Verification of Applicant’s Legal Existence and Identity**

As specified in Section 11.2 of Appendix B1, EV SSL Certificates.

11.3 **Verification of Applicant’s Legal Existence and Identity – Assumed Name**

As specified in Section 11.3 of Appendix B1, EV SSL Certificates.

11.4 **Verification of Applicant’s Physical Existence**

As specified in Section 11.4 of Appendix B1, EV SSL Certificates.

11.5 **Verification of Applicant’s Operational Existence**

As specified in Section 11.5 of Appendix B1, EV SSL Certificates.

11.6 **Verification of Applicant’s Domain Name**

Code Signing Certificates SHALL NOT include a Domain Name.

11.7 **Verification of Name, Title and Authority of Contract Signer and Certificate Approver**

As specified in Section 11.7 of Appendix B1, EV SSL Certificates.

11.8 **Verification of Signature on Subscriber Agreement and EV Code Signing Certificate Requests**

As specified in Section 11.8 of Appendix B1, EV SSL Certificates.

11.9 **Verification of Approval of EV Code Signing Certificate Request**

As specified in Section 11.9 of Appendix B1, EV SSL Certificates.

11.10 **Verification of Certain Information Sources**

As specified in Section 11.10 of Appendix B1, EV SSL Certificates.
11.11 Other Verification Requirements
As specified in Section 11.11 of Appendix B1, EV SSL Certificates.

11.12 Final Cross-Correlation and Due Diligence
As specified in Section 11.12 of Appendix B1, EV SSL Certificates.

11.13 Requirements for Re-use of Existing Documentation
As specified in Sections 9.7 and 11.13 of Appendix B1, EV SSL Certificates.

12. CERTIFICATE ISSUANCE BY A ROOT CA
thawte enforces multi-person controls for certificate issuance by the Root CA. The Root CA Private Keys are not used to sign EV Code Signing Certificates.

13. CERTIFICATE REVOCATION AND STATUS CHECKING
As specified in Section 13 of Appendix B1, EV SSL Certificates, and additionally:

(A) **Revocation Reasons**: Subscribers are expected to not intentionally include Suspect Code in their signed software. Intentionally signing Suspect Code is a violation of the terms of the Subscriber Agreement, and will likely result in revocation of the EV Code Signing Object.

(B) **Revocation Status Information**: thawte provides accurate and up-to-date revocation status information for at least one year following the expiration of the associated certificate, and, upon request, for a period not less than one year beyond expiry of the EV Code Signing Certificate.

(C) **Revocation Processing**: Whenever practical, platforms should check the revocation status of the certificates that they rely upon. However, this is not always practical, for instance, when signed code has to be loaded earlier in the boot sequence than the network communication stack.

   In the timestamp model, the platform should deviate from the RFC 5280 certification path validation algorithm and check the revocation status, not only of the timestamp certificate, but also of the Subscriber's EV Code Signing Certificate at the time of reliance rather than at the time the time-stamp was applied.

   In addition to checking revocation status, where practical, platforms should consult blacklists of suspect software.

(D) **Revocation Consequences**: A certificate may have a one-to-one relationship with the software object that it verifies. In such cases, revocation of the certificate only invalidates the signature on the code that is suspect. If, on the other hand, a certificate has a one-to-many relationship with the software objects that it verifies, then revocation of the certificate invalidates the signatures on all those software objects, some of which may be perfectly sound.

(E) **Responsiveness**. thawte responds to all plausible notices of Suspect Code in a signed software object that verifies with a certificate that thawte has issued, by setting the revocation status of that certificate to ‘revoked’.

14. EMPLOYEE AND THIRD PARTY ISSUES

14.1 Trustworthiness and Competence
As specified in Section 14.1 of Appendix B1, EV SSL Certificates.
14.2 Delegation of Functions to Registration Authorities and Subcontractors

thawte shall not delegate the RA functions for EV Code Signing Certificates.

15. DATA RECORDS

thawte records events in accordance with section 15, Appendix D, Supplemental Baseline Requirements.

16. DATA SECURITY

thawte implements a comprehensive security program in accordance with section 16, Appendix D, Supplemental Baseline Requirements. In addition, thawte requires actions by at least two trusted persons before creating an EV Code Signing Certificate.

In addition:
(1) not applicable.
(2) not applicable.
(3) thawte CAs protect private keys in a FIPS 140-2 level 3 (or equivalent) crypto module as set forth in section 6.2.1 of this CPS.
(4) thawte ensures that the Subscriber’s private key is generated, stored and used in a crypto module that meets or exceeds the requirements of FIPS 140-2 level 2. thawte ships the FIPS 140-2 level 2 crypto module along with necessary drivers to the Subscriber. The Subscriber installs the driver and visits the thawte web page that generates keys only on a FIPS 140-2 level 2 device.

17. AUDIT

17.1 Eligible Audit Schemes

thawte undergoes a WebTrust for Certification Authorities v2.0, or later, audit as set forth in section 8 of this CPS.

Such audits will cover all CA obligations under the CA/Browser Forum Guidelines regardless of whether they are performed directly by thawte or delegated to an RA or subcontractor.

17.2 Audit Period

See Section 17.1.

17.3 Audit Record

See Section 17.1.

17.4 Pre-Issuance Readiness Audit

Not applicable.

17.5 Regular Self-Audits

thawte and Affiliates undergo self-audits to monitor adherence to its Certificate Policy and CPS requirements and strictly control its service quality on at least a quarterly basis against a randomly selected sample of the greater of one Certificate or at least 3% of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

For all EV Code Signing Certificates where the Final Cross-Correlation and Due Diligence requirements of Section 11.12 of this Appendix is performed by an RA, thawte strictly controls its service quality by performing ongoing self audits against a randomly selected sample of at least 6% of the EV Code Signing Certificates it has issued in the period beginning immediately after the last sample was taken.
17.6 Auditor Qualification
A Qualified Auditor (as defined in Section 8.2 of this CPS) performs thawte’s annual audit.

17.7 Root CA Key Pair Generation
As specified in Section 17.7 of Appendix B1, EV SSL Certificates.

18. LIABILITY AND INDEMNIFICATION
thawte is subject to the liability and indemnification obligations as set forth in Section 18 of Appendix B1, EV SSL Certificates.
APPENDIX D
Supplemental Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates


Table of Contents

1. Introduction
2. Purpose
3. References
4. Definitions
5. Abbreviations and Acronyms
6. Conventions
7. Certificate Warranties and Representations
   7.1 By the CA
      7.1.1 Certificate Beneficiaries
      7.1.2 Certificate Warranties
   7.2 By the Applicant
8. Community and Applicability
   8.1 Compliance
   8.2 Certificate Policies
   8.3 Commitment to Comply
   8.4 Trust Model
9. Certificate Content and Profile
   9.1 Issuer Information
      9.1.1 Issuer Common Name Field
      9.1.2 Issuer Domain Component Field
   9.2 Subject Information
      9.2.1 Subject Alternate Name Extension (Required)
      9.2.2 Subject Common Name Field (Optional)
      9.2.3 Subject Domain Component Field (Optional)
      9.2.4 Subject Organization Name Field (Optional)
      9.2.5 Subject Country Name Field (Optional)
      9.2.6 Other Subject Attributes
   9.3 Certificate Policy Identification
      9.3.1 Reserved Certificate Policy Identifiers
      9.3.2 Root CA Certificates
      9.3.3 Subordinate CA Certificate
      9.3.4 Subscriber Certificate
   9.4 Validity Period
   9.5 Subscriber Public Key
   9.6 Certificate Serial Number
   9.7 Additional Technical Requirements
10. Certificate Application
    10.1 Documentation Requirements
    10.2 Certificate Request
        10.2.1 General
        10.2.2 Request and Certification
        10.2.3 Information Requirements
        10.2.4 Subscriber Private Key
    10.3 Subscriber and Terms of Use Agreement
        10.3.1 General
        10.3.2 Agreement Requirements
11. Verification Practices
    11.1 Authorization by Domain Name Registrant
    11.2 Verification of Subject Identity Information
        11.2.1 Identity
11.2.2 DBA/Tradename
11.2.3 Authenticity of Certificate Request
11.2.4 Verification of Individual Applicant
11.2.5 Verification of Country
11.3 Age of Certificate Data
11.4 Denied List
11.5 High Risk Status
11.6 Data Source Accuracy

12. Certificate Issuance by a Root CA

13. Certificate Revocation and Status Checking
   13.1 Revocation
      13.1.1 Revocation Request
      13.1.2 Certificate Problem Reporting
      13.1.3 Investigation
      13.1.4 Response
      13.1.5 Reasons for Revocation
   13.2 Certificate Status Checking
      13.2.1 Mechanisms
      13.2.2 Repository
      13.2.3 Response Time
      13.2.4 Deletion of Entries
      13.2.5 OCSP Signing

14. Employees and Third Parties
   14.1 Trustworthiness and Competence
      14.1.1 Identity and Background Verification
      14.1.2 Training and Skill Level
   14.2 Delegation of Functions
      14.2.1 General
      14.2.2 Compliance Obligation
      14.2.3 Allocation of Liability
      14.2.4 Enterprise RAs

15. Data Records
   15.1 Documentation and Event Logging
   15.2 Events and Actions
   15.3 Document Retention
      15.3.1 Audit Log Retention
      15.3.2 Retention of Documentation

16. Data Security
   16.1 Objectives
   16.2 Risk Assessment
   16.3 Security Plan
   16.4 Business Continuity
   16.5 System Security
   16.6 Private Key Protection

17. Audit
   17.1 Eligible Audit Schemes
   17.2 Audit Period
   17.3 Audit Report
   17.4 Pre-Issuance Readiness Audit
   17.5 Audit of Delegated Functions
   17.6 Auditor Qualifications
   17.7 Key Generation Ceremony
   17.8 Regular Quality Assessment Self Audits

18. Liability and Indemnification
   18.1 Liability to Subscribers and Relying parties
   18.2 Indemnification of Application Software Suppliers
   18.3 Root CA Obligations
1. INTRODUCTION

This Appendix articulates supplemental procedures to thawte’s CPS for issuing Organization Validated (OV) Certificates and Domain Validated (DV) Certificates in conformance with the Baseline Requirement for Publicly Trusted Certificates (“Baseline Requirements”). Additionally, certain sections in this Appendix are referenced from thawte’s Supplemental Procedures for the issuance of EV SSL Certificates (Appendix B1) and EV Code-Signing Certificates (Appendix C). Baseline Requirements are published by the CA Browser Forum at www.cabforum.org, to describe certain of the minimum requirements that a Certificate Authority (CA) must meet in order to issue Publicly Trusted Certificates.

thawte’s OV and DV Certificates issued under the Supplemental Procedures in this Appendix are used for authenticating servers accessible through the Internet.

2. PURPOSE

As specified in section 2 of the CA/Browser Forum Baseline Requirements.

3. REFERENCES

As specified in section 3 of the CA/Browser Forum Baseline Requirements.

4. DEFINITIONS

As specified in section 4 of the CA/Browser Forum Baseline Requirements.

5. ABBREVIATIONS AND ACRONYMS

As specified in section 5 of the CA/Browser Forum Baseline Requirements.

6. CONVENTIONS

As specified in section 6 of the CA/Browser Forum Baseline Requirements.

7. CERTIFICATE WARRANTIES AND REPRESENTATION

7.1 By the CA

By issuing a Certificate, thawte makes Certificate Warranties (as listed in section 7.1.2) to the Certificate Beneficiaries (as described in 7.1.1).

7.1.1 Certificate Beneficiaries

Certificate Beneficiaries of thawte CAs include, but are not limited to:

- The Subscriber that is a party to the Subscriber Agreement for the Certificate;
- All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
- All Relying Parties who reasonably rely on a Valid Certificate.

7.1.2 Certificate Warranties

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with these Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate. The Certificate Warranties specifically include, but are not limited to, the following:

1. **Right to Use Domain Name or IP Address**: That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate’s subject field and subjectAltName...
extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA’s Certificate Policy and/or Certification Practice Statement;

2. **Authorization for Certificate**: That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA’s Certificate Policy and/or Certification Practice Statement;

3. **Accuracy of Information**: That, at the time of issuance, the CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the `subject:organizationalUnitName` attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA’s Certificate Policy and/or Certification Practice Statement;

4. **No Misleading Information**: That, at the time of issuance, the CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate’s `subject:organizationalUnitName` attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA’s Certificate Policy and/or Certification Practice Statement;

5. **Identity of Applicant**: That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.1.1.1 and 3.2.2.1; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA’s Certificate Policy and/or Certification Practice Statement;

6. **Subscriber Agreement**: That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are Affiliated, the Applicant Representative acknowledged and accepted the Terms of Use;

7. **Status**: That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and

8. **Revocation**: That the CA will revoke the Certificate for any of the reasons specified in these Requirements.

### 7.2 By the Applicant

**thawte** requires that the Applicant makes the commitments and warranties set forth in section 10.3.2 of this Appendix for the benefit of the CA and the Certificate Beneficiaries.

### 8. COMMUNITY AND APPLICABILITY

#### 8.1 Compliance

The **thawte** CA complies with the requirements set forth in this Appendix. **thawte** issues Certificates and operates its PKI in accordance with applicable law as set forth in section 9.15 of this CPS.

If a court of government body with jurisdiction over the activities covered by these Baseline Requirements determines that the performance of any mandatory requirement is illegal, then such requirement is considered reformed to the minimum extent necessary to make the requirement valid and legal. This applies only to operations or certificate issuances that are subject to the laws of that jurisdiction. The parties involved **SHALL** notify the CA / Browser Forum of the facts, circumstances and law(s) involved so that the CA/Browser Forum may revise the Baseline Requirements accordingly.
8.2 Certificate Policies

8.2.1 Implementation

thawte develops, implements, enforces and annually updates a Certificate Policy and Certificate Practice Statement that describes in detail how thawte implements the latest version of the CA/Browser Forum Baseline Requirements.

8.2.2 Disclosure

thawte publicly discloses Certificate Information via an online repository as set forth in section 2.2 that is readily available on a 24x7 basis. Such CA business practices are provided in accordance with RFC 3647 and the WebTrust for CAs Audit Scheme.

8.3 Commitment to Comply

CAs within the thawte Trust Network hierarchy conform to the current version of the CA/Browser Forum (CABF) Baseline Requirements for the Issuance and Management of Publicly- Trusted Certificates published at www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

8.4 Trust Model

thawte discloses all Cross-Certificates that identify a thawte CA as the Subject. Such disclosures are provided in section 1 (Cross-Certification) of this CPS.

9. CERTIFICATE CONTENT AND PROFILE

9.1 Issuer Information

The following naming attributes shall be used to populate the Issuer Name in Certificates issued under this CPS:

9.1.1 Issuer Common Name Field (optional)

If the Issuer commonName (CN=) field is present, it must contain a name that accurately identifies the Issuing CA.

9.1.2 Issuer Domain Component Field

No stipulation.

9.1.3 Issuer Organization Name Field (required)

The organizationName (O=) field is required and contains the Issuer organization name (or abbreviation thereof), trademark, or other meaningful identifier for thawte, that accurately identifies thawte. The field must not contain a generic designation such as “Root” or “CA1”.

9.1.4 Issuer Country Name Field (required)

The countryName (C=) component is required and contains the two-letter ISO 3166-1 country code for the country in which the issuer’s place of business is located.

9.2 Subject Information

The following naming attributes shall be used to populate the Subject in Certificates issued under this CPS:
9.2.1 Subject Alternative Name Extensions (required)

The subjectAlternativeName extension is required and contains at least one entry. Each entry is either a dNSName containing the Fully Qualified Domain Name or an IPAddress containing the IP address of a server. The thawte CA confirms that the Applicant controls the Fully Qualified Domain Name (FQDN) or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate. Wildcard FQDNs are permitted.

Prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name, the thawte CA notifies the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. Also, as of July 1 2012, the thawte CA shall not issue a certificate with an Expiry Date later than 1 November 2015 with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name. Effective 1 October 2016, thawte CAs shall revoke all unexpired Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Server Name.

9.2.2 Subject Common Name Field (optional)

The commonName (CN=) component is deprecated (discouraged, but not prohibited). If present, commonName contains a single IP address or Fully Qualified Domain Name that is also one of the values contained in the Certificate’s subjectAlternativeName extension.

9.2.3 Subject Domain Component Field (optional)

The domainComponent (dc=) component is optional. If present, domainComponent contains all components of the subject’s Registered Domain Name in ordered sequence, with the most significant component, closest to the root of the namespace, written last.

9.2.4 Subject Organization Name Field (optional)

If the organizationName (O=) field is present, the field contains the Subject’s name or DBA and the required address fields contain a location of the Subject as verified in accordance with section 11.2.

If the Subject is a natural person, because Subject name attributes for individuals (e.g. givenName and surname) are not broadly supported by application software, the CA may use the organizationName field to convey the Subject’s name or DBA (see 11.2 Verification of Subject Identity Information).

If the fields include discrepancies that the CA considers minor, such as common variations and abbreviations, then the CA shall document the discrepancy and shall use locally accepted abbreviations when abbreviating the organization name (e.g., if the official record shows “Company Name Incorporated”, the CA may include “Company Name, Inc.”). The organizationName field may include a verified DBA or tradename of the Subject.

If organizationName is present, then localityName, stateOrProvinceName (where applicable), and countryName shall also be required and countryName shall also be required and streetAddress and postalCode are optional. If organizationName is absent, then the Certificate shall not contain a streetAddress, localityName, stateOrProvinceName, or postalCode attribute. The CA may include the Subject’s countryName field without including other Subject Identity Information pursuant to countryName requirements above.

9.2.5 Subject Country Name Field (optional)

If present, the countryName (C=) component shall be the two-letter ISO 3166-1 country code. If present, thawte CAs shall verify the country associated with the Subject in accordance with section 11.2.5.
9.2.6 Other Subject Attributes

Optional attributes, when present in the subject field, must contain information that has been verified by the CA. Metadata such as `.`, `,`, and ` ` (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable, shall not be used.

`thawte` shall not include Fully-Qualified Domain Names in Subject attributes except as specified for `subjectAlternativeName` and `CommonName` above.

**OrganizationalUnitName (optional)**

The `OrganizationalUnitName` (OU=) component, when present, may contain information that has not been verified by the CA. Metadata such as `.`, `,`, and ` ` (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable, shall not be used.

`thawte` implements a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless `thawte` has verified this information in accordance with section 11.2 and the Certificate also contains `subject:organizationName`, `subject:localityName`, and `subject:countryName` attributes, also verified in accordance with section 11.2.5.

When an OU value is submitted in a Request, the value is subjected to a search of various high risk lists as per section 11.5, *High Risk Requests*. If a match is found, the value is reviewed by the RA to ensure that the value is accurate and not misleading. If the OU value identifies the name of a legal entity, the value is verified in accordance with section 11.2.

9.3 Certificate Policy Identification

9.3.1 Reserved Certificate Policy Identifiers

No stipulation.

9.3.2 Root CA Certificates

`thawte` Root CA certificates shall not contain the `certificatePolicies` extension.

9.3.3 Subordinate CA Certificates

`thawte` Certificates contain the corresponding policy identifier specified in section 1.2 of the `thawte` CPS that indicates the Certificate is issued and managed in compliance with the CA/Browser Forum Requirements.

The effective date (“Effective Date”) of the CA/Browser Forum Baseline requirements is July 1, 2012.

After the Effective Date, a Certificate issued to a Subordinate CA that is not an Affiliate of the Issuing CA:

- must include the corresponding policy identifier identified in section 1.2 of the `thawte` CPS that indicates the Subordinate CA’s adherence to and compliance with these CABF Requirements, and
- must not contain the “anyPolicy” identifier (2.5.29.32.0).

After the Effective Date, a Certificate issued to a Subordinate CA that is an Affiliate of the Issuing CA:

- may include the corresponding policy identifier identified in section 1.2 of the `thawte` CPS that indicates the Subordinate CA’s adherence to and compliance with these CABF Requirements, and
- may contain the “anyPolicy” identifier (2.5.29.32.0) in place of the explicit policy identifier.
9.3.4 Subscriber Certificates

\textit{thawte} has assigned a reserved OID value, in section 1.2 of the \textit{thawte} CPS, for asserting conformance with the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Truste Certificates. This OID value is reserved for use by any brand of \textit{thawte} CA as a means of asserting compliance with these CABF Requirements and as such does not distinguish a particular brand or class of Certificate.

\textit{thawte}'s domain validated and organization validated SSL Certificates contain the corresponding OID value in section 1.2 of the \textit{thawte} CPS that indicates adherence to and compliance with the CA / Browser Forum Baseline Requirements.

9.4 Validity Period

\textit{thawte}'s domain validated and organization validated SSL Certificates issued after the Effective Date\(^3\) must have a Validity Period no greater than 48 months (4 years).

Except as provided for below, Certificates issued after 1 April 2015 must have a Validity Period no greater than 36 months (3 years). Beyond 1 April 2015, CAs may continue to issue Certificates with a Validity Period greater than 36 months but not greater than 48 months provided that the CA documents that the Certificate is for a system or software that:

a) was in use prior to the Effective Date;
b) is currently in use by either the Applicant or a substantial number of Relying Parties;
c) fails to operate if the Validity Period is shorter than 48 months;
d) does not contain known security risks to Relying Parties; and
e) is difficult to patch or replace without substantial economic outlay.

9.5 Subscriber Public Key

\textit{thawte} Certificates meet the requirements for algorithm type and key size as set forth in section 6.1.5 of this CPS. See Appendix B2 for minimum cryptographic algorithm and key sizes.

9.6 Certificate Serial Number

\textit{thawte} generates a unique serial number value per Issuer DN that exhibits at least 20 bits of entropy.

9.7 Additional Technical Information

See Appendix B2 for minimum cryptographic algorithm and key sizes. See Appendix B3 for required certificate extensions for EV Certificates.

10. CERTIFICATE APPLICATION

10.1 Documentation Requirements

Prior to the issuance of a Certificate, \textit{thawte} obtains the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An executed Subscriber Agreement, which may be electronic.

\textit{thawte} obtains any additional documentation necessary to meet these Requirements.

\(^3\) The Effective Date of the CA Browser Forum requirements for OV and DV certificates is July 1, 2012.
10.2 Certificate Request

10.2.1 General

Prior to the issuance of a Certificate, thawte obtains from the Applicant a certificate request in a form prescribed by thawte that complies with these Requirements. One certificate request may suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in Section 11.3, Age of Certificate Data, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request may be made, submitted and/or signed electronically.

10.2.2 Request and Certification

The certificate request must contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

10.2.3 Information Requirements

The certificate request may include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for thawte to obtain from the Applicant in order to comply with these Requirements and thawte's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, thawte obtains the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant.

Applicant information must include, but not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the Certificate’s SubjectAltName extension.

10.2.4 Subscriber Private Key

Parties other than the Subscriber shall not archive the Subscriber Private Key.

If thawte or any of its designated RAs become aware that a Subscriber’s Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then thawte shall revoke all certificates that include the Public Key corresponding to the communicated Private Key.

10.3 Subscriber Agreement

10.3.1 General

Prior to the issuance of a 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 for a Certificate to be issued pursuant to a Certificate Request.

thawte implements a process to ensure that each Subscriber Agreement is legally enforceable against the Applicant. In either case, the Agreement must apply to the Certificate to be issued pursuant to the certificate request.

thawte uses an electronic or “click-through” Agreement; such agreements are legally enforceable. A separate Agreement may be used for each certificate request, or a single Agreement may be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that thawte issues to the Applicant is clearly covered by that Subscriber Agreement.

10.3.2 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 Certificate Request and as otherwise requested by thawte in connection with the issuance of the 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 Certificate(s) (and any associated access information or device – e.g., password or token);

- **Acceptance of 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 Certificate;

- **Use of Certificate**: An obligation and warranty to install the Certificate only on the server accessible at the domain name listed on the Certificate, and to use the 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 a Certificate and its associated Private Key, and promptly request thawte to revoke the 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 Certificate;

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

- **Responsiveness**: An obligation to respond to thawte’s instructions concerning Key Compromise or Certificate misuse within a specified time period.

- **Acknowledgment and Acceptance**: An acknowledgment and acceptance that thawte is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if thawte discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

### 11. VERIFICATION PRACTICES

#### 11.1 Authorization of Domain Name Registrant

thawte confirms that, as of the date the Certificate was issued, the Applicant either had the right to use, or had control of, the Fully-Qualified Domain Name(s) and IP address(es) listed in the Certificate, or was authorized by a person having such right or control (e.g. under a Principal-Agent or Licensor-Licensee relationship) to obtain a Certificate containing the Fully-Qualified Domain Name(s) and IP address(es).

When relying on a confirmation of the right to use or control the Registered Domain Name(s) from a Domain Name Registrar, and the top-level Domain is a two-letter country code (ccTLD), thawte obtains the confirmation directly from the Domain Name Registrar for the Domain Name level to which the rules of the ccTLD apply. For example, if the requested FQDN is www.mysite.users.example.co.uk, then thawte obtains confirmation from the Domain Name Registrar of the Domain Name example.co.uk, because applications for Domain Names immediately subordinate to .co.uk are governed by the rules of the .uk registry.

When using the Internet mail system to confirm that the Applicant has authorization from the Domain Name Registrant to obtain a Certificate for the requested Fully-Qualified Domain Name, thawte uses a mail system address formed in one of the following ways:
1. Supplied by the Domain Name Registrar;
2. Taken from the Domain Name Registrant’s “registrant”, “technical”, or “administrative” contact information, as it appears in the Domain’s WHOIS record; or;
3. By pre-pending a local part to a Domain Name as follows:
   a. Local part - One of the following: ‘admin’, ‘administrator’, ‘webmaster’, ‘hostmaster’, or ‘postmaster’; and
   b. Domain Name – Formed by pruning zero or more components from the Registered Domain Name or the requested Fully-Qualified Domain Name.

If the Domain Name Registrant has used a private, anonymous, or proxy registration service, and thawte relies upon a Domain Authorization as an alternative to the foregoing, the Domain Authorization must be received directly from the private, anonymous, or proxy registration service identified in the WHOIS record for the Registered Domain Name. The document must contain the letterhead of the private, anonymous, or proxy registration service, the signature of the General Manager, or equivalent, or an authorized representative of such officer, dated on or after the certificate request date, and the Fully-Qualified Domain Name(s) to be included in the Certificate.

If the WHOIS record identifies the private, anonymous, or proxy registration service as the Domain Name Registrant, then the Domain Authorization must contain a statement granting the Applicant the right to use the Fully-Qualified Domain Name in a Certificate. thawte contacts the private, anonymous, or proxy registration service directly, using contact information obtained from a reliable, independent, third-party data source, and obtain confirmation from the Domain Name Registrant that the Domain Authorization is authentic.

11.2 Verification of Subject Identity Information

If the Applicant requests a Certificate that will contain Subject identity Information comprised only of the countryName field, then thawte will verify the country associated with the Subject in accordance with section 11.2.5.

If the Applicant requests a Certificate that will contain the countryName field and other Subject Identity Information, then thawte verifies the identity of the Applicant, and the authenticity of the Applicant Representative’s certificate request using a verification process meeting the following sets of requirements. thawte inspects any document relied upon under this Section for alteration or falsification.

11.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, thawte verifies the identity and address of the organization and that the address is the Applicant’s address of existence or operation. thawte verifies the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1) A government agency (e.g. Secretary of State) in the jurisdiction of the Applicant’s legal creation, existence, or recognition;
2) An external third party database (e.g. Dun and Bradstreet database) that is periodically updated, which thawte has evaluated in accordance with Data Source Accuracy (below);
3) A site visit by the thawte CA or a third party who is acting as an agent for the CA; or
4) An Attestation Letter.

thawte may use the same documentation or communication described in 1 through 4 above to verify both the Applicant’s identity and address.

Alternatively, thawte may verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that meets the requirements of Data Source Accuracy in section 11.6.
11.2.2 DBA/Tradename

If the Subject Identity Information includes a DBA or tradename, thawte verifies the Applicant’s right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant’s legal creation, existence, or recognition;
2. Documentation or communication provided by a third party source that meets the requirements of Data Source Accuracy in section 11.6;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;
4. An Attestation Letter accompanied by documentary support that meets the requirements of Data Source Accuracy (below); or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that meets the requirements of Data Source Accuracy in section 11.6.

11.2.3 Authenticity of Certificate Request (Reliable Method of Communication)

If the Applicant for a Certificate containing Subject Identity Information is an organization, thawte uses a Reliable Method of Communication to verify the authenticity of the Applicant Representative’s certificate request including: email, postal services and telephone.

thawte uses the sources listed in section 11.2.1 to verify the Reliable Method of Communication. Using a Reliable Method of Communication, thawte establishes the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant’s organization, such as the Applicant’s main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

In addition, thawte has a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then thawte shall not accept any certificate requests that are outside this specification. Upon the Applicant’s verified written request thawte will provide a list of the Applicant’s authorized certificate requesters.

11.2.4 Verification of Individual Applicant

If an Applicant is a natural person then thawte verifies the Applicant’s name, Applicant’s address, and the authenticity of the certificate request (also see 9.2.4 OrganizationName).

thawte verifies the Applicant’s name using a legible copy, which discernibly shows the Applicant’s face, of at least one currently valid government-issued photo ID (passport, driver’s license, military ID, national ID, or equivalent document type). thawte inspects the copy for any indication of alteration or falsification.

thawte verifies the Applicant’s address using a form of identification that meets “Data Source Accuracy” requirements, such as a government ID, utility bill, or bank or credit card statement. thawte may rely on the same government-issued ID that was used to verify the Applicant’s name.

thawte verifies the certificate request with the Applicant using a Reliable Method of Communication.

11.2.5 Verification of Country (Subject Identity comprised of only country Name)

If the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the countryName field, then thawte verifies the country associated with the Subject using one of the following:

a) the IP Address range assignment by country for either
   (i) the web site’s IP address, as indicated by the DNS record for the web site or
   (ii) the Applicant’s IP address;

b) the two-letter country code (ccTLD) of the requested Domain Name;

c) information provided by the Domain Name Registrar; or
11.3 **Age of Certificate Data**

*thawte* shall not use any data or document to validate a certificate request if the data or document was obtained more than thirty-nine (39) months prior to the Certificates' issuance.

11.4 **Denied List**

*thawte* maintains an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns, for at least seven (7) years in accordance with documentation retention requirements (section 5.5.2 of this CPS).

*thawte* uses this information to identify subsequent suspicious certificate requests.

11.5 **High Risk Status**

*thawte* takes reasonable steps to identify Applicants 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 Certificates, including Certificates and previously rejected Certificate Requests, due to suspected phishing or other fraudulent usage. This information is used to flag suspicious new Certificate Requests for future scrutiny before issuance.

*thawte* uses information identified by *thawte*’s high-risk criteria to flag suspicious certificate requests. *thawte* follows a documented procedure for performing additional verification of any certificate request flagged as suspicious or high risk. 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.

11.6 **Data Source Accuracy**

Before relying on a data source to verify Subject Identity Information, *thawte* evaluates the data source’s accuracy and reliability. To verify Subject Identity Information, *thawte* uses only those data sources that *thawte* has evaluated to be reasonably accurate or reliable.

12. **CERTIFICATE ISSUANCE BY A ROOT CA**

*thawte*’s Root CA Private Keys shall not be used to sign Subscriber Certificates. *thawte*’s Root CA Private Keys shall be used to sign Certificates under only the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates, and OCSP Response verification Certificates).

Certificate issuance by the Root CA requires an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation. Additional controls for Certificate issuance by the Root CA are described in section 5.6, Key Changeover and section 6.1, Key Pair Generation.
13. CERTIFICATE REVOCATION AND STATUS CHECKING

13.1 Revocation.

13.1.1 Revocation Request

*thawte* provides Subscribers with an online form to request revocation of their own certificates as set forth in section 4.9 of this CPS. *thawte* maintains a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.

13.1.2 Certificate Problem Reporting

*thawte* provides Subscribers, Relying Parties, Application Software Vendors, and other third parties with an online form to report complaints or suspected Private Key compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates ("Certificate Problem Reports") at: [EV-abuse@thawte.com](mailto:EV-abuse@thawte.com).

13.1.3 Investigation

*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:

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

13.1.4 Response

*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 Certificate that is the subject of such a complaint.

13.1.5 Reasons for Revocation

In addition to any revocation circumstances listed in section 4.9.1 of this CPS, *thawte* will revoke an Certificate within 24 hours if one or more of the following events occurs:

1. The Subscriber requests in writing that the CA revoke its Certificate;
2. The Subscriber notifies *thawte* that the original 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 Certificate) has been compromised, or that the Certificate has otherwise been misused (eg, Private key has been archived);
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 the Fully-Qualified Domain Name or IP address listed in the Certificate is no longer permitted (e.g, a court or arbitrator has revoked a Registrant’s right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or that the Domain Name Registrant has failed to renew its Domain Name);
6. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
7. *thawte* receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
8. A determination, in thawte's sole discretion, that the Certificate was not issued in accordance with the terms and conditions of thawte's CPS;

9. thawte determines that any of the information appearing in the Certificate is inaccurate or misleading.

10. thawte ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;

11. thawte's right to issue Certificates under this CPS expires or is revoked or terminated, unless thawte makes arrangements to continue maintaining the CRL/OCSP Repository;

12. thawte's Private Key for its 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.

14. Revocation is otherwise required by the thawte CPS, or

15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. as determined by the CA/Browser Forum).

### 13.2 Certificate Status Checking

#### 13.2.1 Mechanisms

thawte makes revocation information available as stipulated in Appendix B3, Required Certificate Extensions.

#### 13.2.2 Repository

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

For Subscriber Certificates:

1. **CRLs.** are be updated and reissued at least every seven (7) days, and the nextUpdate field value SHALL NOT be more than ten (10) days beyond the value of the thisUpdate field; or

2. **OCSP.** 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.

For thawte's Subordinate CA Certificate:

1. **CRLs.** Are updated and reissued at least (i) every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate, with the value of the nextUpdate field not more than twelve (12) months beyond the value of the thisUpdate field; or

2. **OCSP.** If used, thawte's OCSP for CA Certificates will be updated at least (i) every twelve (12) months, and (ii) within 24 hours after revoking a Subordinate CA Certificate.

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 Certificates issued by it.

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

Effective 1 January 2013, the CA shall support an OCSP capability using the GET method for Certificates issued in accordance with these Requirements.

#### 13.2.3 Response Time

thawte's CRL and OCSP capability shall provide a response time of ten (10) seconds or less under normal operating conditions.
13.2.4 Deletion of Entries
See section 4.9.7 of this CPS.

13.2.5 OCSP Signing
OCSP Responses shall conform to RFC5019 and either be:
- Signed by the CA that issued the Certificates whose revocation status is being checked, or
- Signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate
  whose revocation status is being checked. Such OCSP Responder signing Certificate shall
  contain the extension id-pkix-ocsp-nocheck as defined by RFC2560.

14 EMPLOYEES AND THIRD PARTIES

14.1 Trustworthiness and Competence

14.1.1 Identity and Background Verification
As specified in section 5.3.2 of this CPS.

14.1.2 Training and Skill Level
thawte provides all personnel performing information verification duties with skills-training that covers
basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including
this CPS), common threats to the information verification process (including phishing and other social
engineering tactics), and the pertinent CABF Requirements.

thawte maintains records of such training and ensures that personnel entrusted with Validation Specialist
duties maintain a skill level that enables them to perform such duties satisfactorily. Validation Specialists
engaged in Certificate Issuance shall maintain skill levels consistent with the CA’s training and
performance programs.

thawte documents that each Validation Specialist possesses the skills required by a task before allowing
the Validation Specialist to perform that task. thawte requires all Validation Specialists to pass an
examination provided by the CA on the information verification requirements outlined in the CABF
Requirements.

14.2 Delegation of Functions

14.2.1 General
Should thawte delegate the performance of all or part of Section 11 of this Appendix to a Delegated Third
Party, thawte shall enforce the requirements as set forth in section 14.2.1 of the CA/Browser Forum
Baseline Requirements.

14.2.2 Compliance Obligation
Should thawte delegate the performance of all or part of Section 11 of this Appendix to a Delegated Third
Party, thawte shall enforce the requirements as set forth in section 14.2.2 of the CA/Browser Forum
Baseline Requirements.

14.2.3 Allocation of Liability
Should thawte delegate the performance of all or part of Section 11 of this Appendix to a Delegated Third
Party, thawte shall remain fully responsible as if the tasks had not been delegated as set forth in section
14.2.3 of the CA/Browser Forum Baseline Requirements.
14.2.4 Enterprise RAs
Should thawte delegate the performance of all or part of Section 11 of this Appendix to a Delegated Third Party, thawte shall enforce the requirements as set forth in section 14.2.4 of the CA/Browser Forum Baseline Requirements.

15 DATA RECORDS

15.1 Documentation and Event Logging
thawte and each Delegated Third Party (if any) 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 delegated third parties, including registration agents (RAs) and subcontractors as well.

15.2 Events and Actions
The foregoing record requirements include, but are not limited to, an obligation to record the following events:

1. CA key lifecycle management events, including:
   a. Key generation, backup, storage, recovery, archival, and destruction; and
   b. Cryptographic device lifecycle management events

2. 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

3. 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

4. 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
   c. Description of entry

15.3 Document Retention

15.3.1 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.

15.3.2 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.

16. DATA SECURITY

16.1 Objectives

thawte develops, implements, and maintains a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability (CIA) of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to the CA by law.

16.2 Risk Assessment

thawte performs an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

16.3 Security Plan

Based on results of the annual Risk Assessment, thawte develops, implements, and maintains a Security Plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

The Security Plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The Security Plan takes into account then-available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

16.4 Business Continuity

thawte maintains a Disaster Recovery Plan (DRP) to maintain or restore thawte’s business operations in a timely manner following the interruption to or failure of critical business processes.

thawte’s DRP defines the procedures for the teams to reconstitute thawte CA operations using backup data and backup copies of the thawte keys. The DRP defines emergency procedures, fallback procedures and resumption procedures, the conditions for activating the plan and what constitutes an acceptable system outage and recovery time objective (RTO).

thawte’s DRP identifies administrative requirements including:

- maintenance schedule for the plan;
- Awareness and education requirements;
- Responsibilities of the individuals; and
- Regular testing of contingency plans.

Additionally, **thawte**'s DRP includes:
- Requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location,
- Frequency for taking backup copies of essential business information and software,
- Separation distance of the Disaster recovery site to the CA's main site,
- Procedures for securing the Disaster facility during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site,

### 16.5 System Security

**thawte** includes system security controls for the Certificate Management Process as follows:

1. Physical security and environmental controls (see section 5.1 of this CPS),
2. System integrity controls including configuration management, integrity maintenance of trusted code and malware detection/prevention (see section 6.6.2 of this CPS),
3. Network security and firewall management, including port restrictions and IP address filtering (see section 6.7 of this CPS),
4. User management, separate trusted-role assignments, education, awareness and training (see section 5.2 of this CPS), and,
5. Logical access controls, activity logging and inactivity time-outs to provide individual accountability (see sections 5.2.3 and 5.4.1 of this CPS).

**thawte** enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.

### 16.6 Private Key Protection

**thawte**'s private key protection is described in sections 5.1.2 (Physical Access), 5.2.3 (Identification and Authentication for Each Role), 6.2.9 (Method of Deactivating Private Key) and 6.6.1 (System Development Controls) of this CPS.

### 17. AUDIT

#### 17.1 Eligible Audit Schemes

**thawte** undergoes a WebTrust for Certification Authorities v2.0 or later audit as set forth in section 8 of this CPS.

Such audits will cover all CA obligations under the CA/Browser Forum Guidelines regardless of whether they are performed directly by **thawte** or delegated to an RA or subcontractor.

#### 17.2 Audit Period

**thawte** conducts annual compliance audits as set forth in section 8.1 of this CPS.

#### 17.3 Audit Report

**thawte** makes its annual Audit Report publicly available as set forth in section 8.6 of this CPS.

#### 17.4 Pre-Issuance Readiness Audit

No stipulation.

#### 17.5 Audit of Delegated Functions

No stipulation.
17.6 Auditor Qualifications

*thawte* engages a qualified auditor as set forth in section 8.2 of this CPS.

17.7 Key Generation Ceremony

*thawte* conducts key generation ceremonies as set forth in section 6.1.1 of this CPS and additionally in *thawte*’s confidential security policies.

17.8 Regular Quality Assessment Self Audits

*thawte* and Affiliates shall undergo self-audits to monitor adherence to its Certificate Policy and CPS requirements and strictly control its service quality on at least a quarterly basis against a randomly selected sample of the greater of one Certificate or at least 3% of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

18. LIABILITY AND INDEMNIFICATION

18.1 Liability to Subscribers and Relying Parties

To the extent *thawte* has issued and managed the Certificate(s) at issue in compliance with CA/Browser Forum requirements and its CPS, *thawte* shall have no liability to the Subscriber, any Relying Parties or any other third parties for any damages or losses suffered as a result of use or reliance on such Certificate.

In cases where *thawte* has not issued or managed the Certificate(s) in complete compliance with CA/Browser Forum requirements and its 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 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 Certificate shall not exceed $2,000.

18.2 Indemnification of Application Software Suppliers

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 the *thawte* Root CA 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 Certificates or reliance thereon by Relying Parties or others.

*thawte* shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a 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 Supplier related to a Certificate issued by *thawte* where such claim, damage, or loss was directly caused by such Application Software Supplier’s software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from *thawte* online, and the browser/application software either failed to check such status or ignored an indication of revoked status).

18.3 Root CA Obligations

The Root CA shall be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA’s compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under these Requirements, as if the Root CA were the Subordinate CA issuing the Certificates.
# APPENDIX E: Change History

## History of changes: version 3.7.8 (Jan 15, 2013)

<table>
<thead>
<tr>
<th>Description</th>
<th>Section &amp; Changes made</th>
</tr>
</thead>
</table>
| Re-alignment with CABF EV v1.4 Guidelines |  • Updated Appendix B1 all sections to match re-structured CABF Guidelines.  
• Updated Appendix C (EV CodeSigning) for cross-references to & from Appendix B1.  
• Created Appendix D (Baseline for OV & DV Certs) for cross-references to & from Appendix B1.  
• CPS updated throughout with references to Appx B1, C & D as required for CABF procedures. |

## History of changes: version 3.7.7 (Effective date October 2012)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.5 Key Sizes</td>
<td>Addition of 2048 DSA CA hierarchies</td>
</tr>
</tbody>
</table>

## History of changes: version 3.7.6 (Effective date August 2012)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughout document</td>
<td>Converted document format from rfc2527 to rfc3647 standard.</td>
</tr>
<tr>
<td>All updates reflecting compliance with CABF Requirements for EV Code Signing Certificates, v1.4.</td>
<td>Appendix C.</td>
</tr>
<tr>
<td>Routine maintenance</td>
<td>Changed to affirmative language: “thawte confirms” instead of “CA shall confirm” – in sections 3.2.2.1, 4.1.2.2, 4.9.3.2, 4.9.7.1, 4.9.9.1, 6.1.5.1, 6.3.2.1, 6.5.1.1, 7.1.2.2.1,</td>
</tr>
</tbody>
</table>

## History of changes: version 3.7.5 (Effective date June 2012)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 1.0</td>
<td>Identified thawte non-EV OIDs</td>
</tr>
<tr>
<td>Throughout document</td>
<td>All updates reflecting compliance with CABF Requirements for DV and OV certificates, Effective July 1, 2012. (See PWG Approval Mapping Matrix for thawte CPS).</td>
</tr>
</tbody>
</table>

## History of changes: version 3.7.4 (Effective date September 20, 2011)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughout document</td>
<td>Change email address from VeriSign to Symantec.</td>
</tr>
<tr>
<td>6.1.5 Key Sizes and Appendix A2</td>
<td>thawte CA key pairs are at least 2048 bit RSA.</td>
</tr>
</tbody>
</table>

## History of changes: version 3.7.3 (Effective date September 17, 2010)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughout document</td>
<td>Eliminated all practices for issuance of low assurance, Personal Email, FreeMail and Web of Trust certificates.</td>
</tr>
<tr>
<td>Throughout document</td>
<td>Reflected the change in ownership from VeriSign to Symantec.</td>
</tr>
<tr>
<td>3.1.1 &amp; 7.1</td>
<td>Corrected CA naming from S Africa to US locations</td>
</tr>
<tr>
<td>2.4.1 (Governing Law) &amp; 2.4.3 (Dispute Resolution)</td>
<td>Changed from Virginia to California</td>
</tr>
<tr>
<td>2.3.3 Assets</td>
<td>Changed from VeriSign to Symantec.</td>
</tr>
</tbody>
</table>

## History of changes: version 3.7.2 (Effective date March 30, 2010)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sections 1.1, 1.3.1, 1.3.2, 2.1.2, 2.7, 3.1.8, 4.1.1, 4.4.2.1</td>
<td>Change from Starter PKI (SPKI) to Thawte Certificate Center Enterprise (TCCE) throughout.</td>
</tr>
<tr>
<td>Section 1.3.1 and 4.4.9</td>
<td>Thawte Timestamping Root CA now active.</td>
</tr>
</tbody>
</table>
| Section 1.3.1 | Medium Assurance Root CA that issues:  
• Sub-CA Certificates for VeriSign Issuing CA  
• End entity certificate for GeoTrust time stamping services. |
| Section 4.4.9 | Root CA (Non-Issuing) – thawte Time Stamping CA |
| Section 6.1.5 Key Sizes | Thawte CA key pairs are at least 1024 bit RSA and shall be transitioned to 2048 bit RSA no later than December 31, 2010. thawte recommends that RAs and end-user Subscribers generate 1024/2048 bit RSA key pairs. thawte will continue to approve end entity certificates generated with a key pair size of less than 2048 bit RSA but will phase out all 1024-bit RSA by December 31, 2013, but currently in rare circumstances thawte permits 512 bit RSA key pairs to support certain legacy applications and web servers. Key sizes for thawte EV certificates are identified in Appendix A2. |
| Section 7.1.1 Certificate Profile | 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 |
### Appendix A2

SuperCerts which require a key length of at least 1024 bits.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1 Site Location</td>
<td>Location of Primary site changed from MV CA to Delaware.</td>
</tr>
<tr>
<td>2.4.1 and 2.4.3.2</td>
<td>Governing Law jurisdiction changed from California to Fairfax County, Virginia.</td>
</tr>
</tbody>
</table>

### Appendix A3

Explicitly added SAN to list of extensions for Subscriber certs.

- `SubjectAltName: If present is populated in accordance with RFC5280 and criticality is set to FALSE`

---

### History of changes: version 3.7.1

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| Appendix A2 | Updates to key sizes:  
- All ECC certificates – 256 & 384 bit |
| Appendix A3 | Location of Primary site changed from MV CA to Delaware.  
Governing Law jurisdiction changed from California to Fairfax County, Virginia.  
Explicitly added SAN to list of extensions for Subscriber certs.  
`SubjectAltName: If present is populated in accordance with RFC5280 and criticality is set to FALSE` |

### History of changes: Version 3.7 (Effective date May 01, 2008)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6..3..2</td>
<td>Updated validity period of CA to end user subscriber certificate from 3 to 5 years. Added a footnote to the effect that &quot;At a minimum, the Distinguished Name of 4 and 5 year validity SSL certificates is reverified after three years from date of issuance. There is no requirement to reverify the Distinguished Name of 4 and 5 year SSL123 certificates during the validity period of the certificate&quot;</td>
</tr>
</tbody>
</table>

### History of changes: Version 3.6 (Effective date April 03, 2008)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.3.1 – table 3 | Added: "thawte Primary Root CA – G2"  
Added: "thawte Primary Root CA – G3" |
| 4.4.9 – table 20 | Added: "thawte Primary Root CA – G2"  
Added: "thawte Primary Root CA – G3" |
| Appendix A1 Section 16(a) | Updated to allow for verification of address of a or a Parent/Subsidiary Company  
Added **Non-Commercial Entity Subjects**  
Added: **Non-Commercial Entities:** V1.0, Clause 5.(3)  
Added: Government Entities and Non-Commercial Entities  
Added Prior Equivalent Authority  
Updated Appendix A4 in line with published errata to the EV Guidelines  
**Definitions**  
Updated "Subsidiary Company" to be a majority owned and not a wholly owned company. |
| Appendix A1 Section 5 | Added: "Country":  
"Sovereign State":  
"International Organization":  
"Parent Company" |
| Appendix A1 Section 6(a)3 | Added: "thawte’s Root CA Certificate for EV Certificates is the thawte Primary Root CA. This Root CA does not contain the certificatePolicies or extendedKeyUsage fields"  
To  
"thawte’s Root CA Certificate for EV Certificates is the thawte Primary Root CA. This Root CA does not contain the certificatePolicies but does contain the extendedKeyUsage field." |

### History of changes: Version 3.5 (Effective date January, 2008)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| Appendix A1: Section 7(c) | Updated "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"  
To  
"thawte’s Root CA Certificate for EV Certificates is the thawte Primary Root CA. This Root CA does not contain the certificatePolicies but does contain the extendedKeyUsage field." |

### History of changes: Version 3.4 (Effective date July, 2007)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.3.1-Table 3 | Updated description of thawte Server CA  
Deleted: "High Assurance Root CA that issues  
Server Certificates  
Sub-CA Certificates for thawte Issuing CAs"  
Added: "Root CA that issues medium assurance domain validated SSL Certificates" |
<table>
<thead>
<tr>
<th>Section</th>
<th>Added/Deleted</th>
</tr>
</thead>
</table>
| 1.1     | Added: "thawte’s Certification Authorities (CAs) offer three distinct classes of end user subscriber certificates – High 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)."
|         | Added: "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 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."
| 1.3.3   | Added: "High assurance with extended validation…Incorporated Organizations (including Government agencies, Educational Institutions, Government Departments.). The types of Organizations that qualify for EV Certificates are more fully described in Appendix A1 of this CPS."
| 1.3.4   | Added: "High Assurance with extended validation”
| 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”
| 3.1.1.1 | Added: “EV SSL certificate content and profile requirements are discussed in Section 6 of Appendix A3 to this CPS”
| 3.1.1.7 | 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.”
| 3.1.8.1 | "SSL Web Server Certificates with EV…thawte’s procedures for issuing Extended Validation SSL Certificates are described in Appendix A1 to this CPS.”
| 4.1.1   | Added: “High Assurance with extended validation – SSL Web Server Certificates with EV”
| 4.4.9   | Added “thawte Primary Root CA”; “thawte Extended Validation SSL CA”
| 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 of shares distributed for disaster recovery tokens is 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 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.”
| 6.2.7.1.2 | Added "and High Assurance with extended validation Certificates”
| 7.1.1   | Added: “SSL Web Server Certificates with EV standard certificate profiles are discussed in Section 6 of Appendix A3 to this CPS."
| 7.1.2.7 | Added new 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,SQC 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,SQC 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 1.3.4.4
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 1
Deleted: A Subscriber may make changes to the name included in a certificate within 30 days of issue. thawte
2.5.6

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.

Section 7.1.2.3

Deleted: http://crl.thawte.com/ThawteServerCA.crl

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

Section 7.1.2.5

Deleted: http://crl.thawte.com/ThawteServerCA.crl

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

Authority information Access http://ocsp.thawte.com Non-Critical

Section 7.1.2.6

Added: SSL Wildcard Certificates

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

<table>
<thead>
<tr>
<th>Extension</th>
<th>Value Constraint</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Constraints</td>
<td>Subject Type=End Entity</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>Path Length Constraint=None</td>
<td></td>
</tr>
<tr>
<td>Enhanced Key Usage</td>
<td>Server Authentication (1.3.6.1.5.5.7.3.1)</td>
<td>Non-Critical</td>
</tr>
<tr>
<td></td>
<td>Client Authentication (1.3.6.1.5.5.7.3.2)</td>
<td></td>
</tr>
<tr>
<td>Authority information Access</td>
<td><a href="http://ocsp.thawte.com">http://ocsp.thawte.com</a></td>
<td>Non-Critical</td>
</tr>
</tbody>
</table>

Table 26 – thawte SSL Web Server Certificate Extensions

Section 7.1.3

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.

Section 7.1.3

Deleted: Algorithm used to sign the CRL. Thawte CRLs are signed using md5RSA (OID: 1.2.840.113549.1.1.4) in
<table>
<thead>
<tr>
<th>Section 9.2.</th>
<th>Deleted:</th>
<th>Added:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SGC SuperCerts</strong></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>
<td><strong>SGC SuperCerts</strong></td>
</tr>
<tr>
<td><strong>SSL Web Server Certificates</strong></td>
<td>An organizational Certificate used to support SSL sessions between web browsers and servers.</td>
<td><strong>SSL Web Server Certificates</strong></td>
</tr>
<tr>
<td><strong>High Assurance</strong></td>
<td>Certificates issued to organizations and sole proprietors to provide authentication; message, software, and content integrity; and confidentiality encryption.</td>
<td><strong>High Assurance</strong></td>
</tr>
<tr>
<td><strong>Reseller Partner Program</strong></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>
<td><strong>ISP Partner Program</strong></td>
</tr>
<tr>
<td><strong>Code Signing Certificates</strong></td>
<td>Certificates which secure delivery of code and content to browsers over the Internet.</td>
<td><strong>Medium Assurance</strong></td>
</tr>
<tr>
<td><strong>SSL123 Certificates</strong></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>
<td><strong>Wildcard Certificates</strong></td>
</tr>
</tbody>
</table>