

---

***thawte***  
**Certification Practice  
Statement**

**Version 3.7.17**

**December 19, 2016**

## **thawte Certification Practice Statement**

© 2016 *thawte, Inc.* All rights reserved.  
Printed in the United States of America.

Revision date: December 19, 2016

### **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  
Net: [practices@symantec.com](mailto:practices@symantec.com).

### **Acknowledgement**

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

## TABLE OF CONTENTS

<b>1. INTRODUCTION .....</b>	<b>1</b>	4.2.2 <i>Approval or Rejection of Certificate Applications</i> .....	17
1.1 OVERVIEW.....	2	4.2.3 <i>Time to Process Certificate Applications</i> .....	17
1.2 DOCUMENT NAME AND IDENTIFICATION .....	4	4.2.4 <i>Certificate Authority Authorization (CAA)</i> .....	17
1.3 PKI PARTICIPANTS.....	4	4.3 CERTIFICATE ISSUANCE.....	17
1.3.1 <i>Certification Authorities</i> .....	5	4.3.1 <i>CA Actions During Certificate Issuance</i> .....	17
1.3.2 <i>Registration Authorities</i> .....	5	4.3.2 <i>Notification to Subscriber by the CA of Issuance of Certificate</i> .....	17
1.3.3 <i>Subscribers</i> .....	5	4.3.3 <i>Certificate Issuance by a Root CA</i> .....	17
1.3.4 <i>Relying Parties</i> .....	6	4.4 CERTIFICATE ACCEPTANCE .....	18
1.3.5 <i>Other Participants</i> .....	6	4.4.1 <i>Conduct Constituting Certificate Acceptance</i> .....	18
1.4 CERTIFICATE USAGE.....	6	4.4.2 <i>Publication of the Certificate by the CA</i> .....	18
1.4.1 <i>Appropriate Certificate Uses</i> .....	6	4.4.3 <i>Notification of Certificate Issuance by the CA to Other Entities</i> .....	18
1.4.2 <i>Prohibited Certificate Uses</i> .....	7	4.5 KEY PAIR AND CERTIFICATE USAGE.....	18
1.5 POLICY ADMINISTRATION .....	7	4.5.1 <i>Subscriber Private Key and Certificate Usage</i> .....	18
1.5.1 <i>Organization Administering the Document</i> .....	7	4.5.2 <i>Relying Party Public Key and Certificate Usage</i> .....	18
1.5.2 <i>Contact Person</i> .....	8	4.6 CERTIFICATE RENEWAL .....	18
1.5.3 <i>Person Determining CPS Suitability for the Policy</i> .....	8	4.6.1 <i>Circumstances for Certificate Renewal</i> .....	19
1.5.4 <i>CPS Approval Procedures</i> .....	8	4.6.2 <i>Who May Request Renewal</i> .....	19
1.6 DEFINITIONS AND ACRONYMS .....	8	4.6.3 <i>Processing Certificate Renewal Requests</i> .....	19
<b>2. PUBLICATION AND REPOSITORY RESPONSIBILITIES .....</b>	<b>9</b>	4.6.4 <i>Notification of New Certificate Issuance to Subscriber</i> ..	19
2.1 REPOSITORIES.....	9	4.6.5 <i>Conduct Constituting Acceptance of a Renewal Certificate</i> .....	19
2.2 PUBLICATION OF CERTIFICATION INFORMATION .....	9	4.6.6 <i>Publication of the Renewal Certificate by the CA</i> .....	19
2.3 TIME OR FREQUENCY OF PUBLICATION .....	9	4.6.7 <i>Notification of Certificate Issuance by the CA to Other Entities</i> .....	20
2.4 ACCESS CONTROLS ON REPOSITORIES.....	9	4.7 CERTIFICATE RE-KEY.....	20
<b>3. IDENTIFICATION AND AUTHENTICATION .....</b>	<b>10</b>	4.8 CERTIFICATE MODIFICATION .....	20
3.1 NAMING .....	10	4.9 CERTIFICATE REVOCATION AND SUSPENSION.....	20
3.1.1 <i>Types of Names</i> .....	10	4.9.1 <i>Circumstances for Revocation</i> .....	20
3.1.2 <i>Need for Names to be Meaningful</i> .....	11	4.9.2 <i>Who Can Request Revocation</i> .....	21
3.1.3 <i>Anonymity or Pseudonymity of Subscribers</i> .....	12	4.9.3 <i>Procedure for Revocation Request</i> .....	22
3.1.4 <i>Rules for Interpreting Various Name Forms</i> .....	12	4.9.4 <i>Revocation Request Grace Period</i> .....	22
3.1.5 <i>Uniqueness of Names</i> .....	12	4.9.5 <i>Time within Which CA Must Process the Revocation Request</i> .....	22
3.1.6 <i>Recognition, Authentication, and Role of Trademarks</i> ..	12	4.9.6 <i>Revocation Checking Requirement for Relying Parties</i> ..	22
3.2 INITIAL IDENTITY VALIDATION .....	12	4.9.7 <i>CRL Issuance Frequency (If Applicable)</i> .....	22
3.2.1 <i>Method to Prove Possession of Private Key</i> .....	12	4.9.8 <i>Maximum Latency for CRLs</i> .....	23
3.2.2 <i>Authentication of Organization Identity</i> .....	12	4.9.9 <i>On-Line Revocation/Status Checking Availability</i> .....	23
3.2.3 <i>Authentication of Individual Identity</i> .....	13	4.9.10 <i>On-line Revocation Checking Requirements</i> .....	23
3.2.4 <i>Non-Verified Subscriber Information</i> .....	13	4.9.11 <i>Other Forms of Revocation Advertisements Available</i> ..	23
3.2.5 <i>Validation of Authority</i> .....	14	4.9.12 <i>Special Requirements Regarding Key Compromise</i> .....	24
3.2.6 <i>Criteria for Interoperation</i> .....	14	4.9.13 <i>Circumstances for Suspension</i> .....	24
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS.....	14	4.9.14 <i>Who Can Request Suspension</i> .....	24
3.3.1 <i>Identification and Authentication for Routine Re-Key</i> ..	14	4.9.15 <i>Procedure for Suspension Request</i> .....	24
3.3.2 <i>Identification and Authentication for Re-Key After Revocation</i> .....	14	4.9.16 <i>Limits on Suspension Period</i> .....	24
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST....	14	4.10 CERTIFICATE STATUS SERVICES .....	24
<b>4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS .....</b>	<b>16</b>	4.10.1 <i>Operational Characteristics</i> .....	24
4.1 CERTIFICATE APPLICATION .....	16	4.10.2 <i>Service Availability</i> .....	24
4.1.1 <i>Who Can Submit a Certificate Application</i> .....	16	4.10.3 <i>Operational Features</i> .....	24
4.1.2 <i>Enrolment Process and Responsibilities</i> .....	16	4.11 END OF SUBSCRIPTION.....	24
4.2 CERTIFICATE APPLICATION PROCESSING.....	16	4.12 KEY ESCROW AND RECOVERY .....	24
4.2.1 <i>Performing Identification and Authentication Functions</i> .....	17	4.12.1 <i>Key Escrow and Recovery Policy and Practices</i> .....	24

4.12.2 Session Key Encapsulation and Recovery Policy and Practices.....	24	5.9 DATA SECURITY.....	33
<b>5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS .....</b>	<b>25</b>	<b>6. TECHNICAL SECURITY CONTROLS .....</b>	<b>34</b>
5.1 PHYSICAL CONTROLS.....	25	6.1 KEY PAIR GENERATION AND INSTALLATION .....	34
5.1.1 Site Location and Construction .....	25	6.1.1 Key Pair Generation.....	34
5.1.2 Physical Access.....	25	6.1.2 Private Key Delivery to Subscriber .....	34
5.1.3 Power and Air Conditioning .....	25	6.1.3 Public Key Delivery to Certificate Issuer.....	34
5.1.4 Water Exposures .....	25	6.1.4 CA Public Key Delivery to Relying Parties .....	34
5.1.5 Fire Prevention and Protection .....	25	6.1.5 Key Sizes .....	34
5.1.6 Media Storage.....	25	6.1.6 Public Key Parameters Generation and Quality Checking .....	35
5.1.7 Waste Disposal .....	25	6.1.7 Key Usage Purposes (as per x509v3 field) .....	36
5.1.8 Off-Site Backup .....	26	6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS .....	36
5.2 PROCEDURAL CONTROLS .....	26	6.2.1 Cryptographic Module Standards and Controls.....	36
5.2.1 Trusted Roles.....	26	6.2.2 Private Key (n out of m) Multi-Person Control.....	36
5.2.2 Number of Persons Required Per Task .....	26	6.2.3 Private Key Escrow.....	36
5.2.3 Identification and Authentication for Each Role .....	26	6.2.4 Private Key Backup .....	36
5.2.4 Roles Requiring Separation of Duties.....	27	6.2.5 Private Key Archival.....	36
5.3 PERSONNEL CONTROLS .....	27	6.2.6 Private Key Transfer Into or From a Cryptographic Module .....	37
5.3.1 Qualifications, Experience and Clearance Requirements .....	27	6.2.7 Private Key Storage on Cryptographic Module.....	37
5.3.2 Background Check Procedures.....	27	6.2.8 Method of Activating Private Key.....	37
5.3.3 Training Requirements.....	28	6.2.9 Method of Deactivating Private Key.....	38
5.3.4 Retraining Frequency and Requirements.....	28	6.2.10 Method of Destroying Private Key.....	38
5.3.5 Job Rotation Frequency and Sequence .....	28	6.2.11 Cryptographic Module Rating .....	38
5.3.6 Sanctions for Unauthorized Actions.....	28	6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT.....	38
5.3.7 Independent Contractor Requirements.....	28	6.3.1 Public Key Archival.....	38
5.3.8 Documentation Supplied to Personnel.....	28	6.3.2 Certificate Operational Periods and Key Pair Usage Periods.....	38
5.4 AUDIT LOGGING PROCEDURES.....	28	6.4 ACTIVATION DATA .....	39
5.4.1 Types of Events Recorded .....	28	6.4.1 Activation Data Generation and Installation.....	39
5.4.2 Frequency of Processing Log .....	29	6.4.2 Activation Data Protection .....	39
5.4.3 Retention Period for Audit Log.....	29	6.4.3 Other Aspects of Activation Data .....	39
5.4.4 Protection of Audit Log .....	29	6.5 COMPUTER SECURITY CONTROLS .....	39
5.4.5 Audit Log Backup Procedures.....	29	6.5.1 Specific Computer Security Technical Requirements .....	39
5.4.6 Audit Collection System (Internal vs. External) .....	30	6.5.2 Computer Security Rating.....	39
5.4.7 Notification to Event-Causing Subject.....	30	6.6 LIFE CYCLE TECHNICAL CONTROLS .....	40
5.4.8 Vulnerability Assessments.....	30	6.6.1 System Development Controls.....	40
5.5 RECORDS ARCHIVAL.....	30	6.6.2 Security Management Controls.....	40
5.5.1 Types of Records Archived .....	30	6.6.3 Life Cycle Security Controls.....	40
5.5.2 Retention Period for Archive .....	30	6.7 NETWORK SECURITY CONTROLS .....	40
5.5.3 Protection of Archive.....	30	6.8 TIME-STAMPING .....	40
5.5.4 Archive Backup Procedures.....	31	<b>7. CERTIFICATE, CRL AND OCSP PROFILES .....</b>	<b>41</b>
5.5.5 Requirements for Time-Stamping of Records .....	31	7.1 CERTIFICATE PROFILE.....	41
5.5.6 Archive Collection System (Internal vs. External).....	31	7.1.1 Version Number(s).....	41
5.5.7 Procedures to Obtain and Verify Archive Information ..	31	7.1.2 Certificate Extensions .....	42
5.6 KEY CHANGEOVER .....	31	7.1.3 Algorithm Object Identifiers .....	44
5.6.1 Routine Rekey and Renewal of CA Certificate.....	31	7.1.4 Name Forms .....	44
5.6.2 Key Changeover Procedures.....	31	7.1.5 Name Constraints .....	44
5.7 COMPROMISE AND DISASTER RECOVERY.....	32	7.1.6 Certificate Policy Object Identifier .....	44
5.7.1 Incident and Compromise Handling Procedures.....	32	7.1.7 Usage of Policy Constraints Extension.....	44
5.7.2 Computing Resources, Software and/or Data are Corrupted.....	32	7.1.8 Policy Qualifiers Syntax and Semantics .....	44
5.7.3 Entity Private Key Compromise Procedures .....	32		
5.7.4 Business Continuity Capabilities After a Disaster.....	32		
5.8 CA OR RA TERMINATION .....	33		

7.1.9 Processing Semantics for the Critical Certificate Policies Extension.....	44	9.6.4 Relying Party Representations and Warranties.....	52
7.2 CRL PROFILE.....	44	9.6.5 Representations and Warranties of Other Participants	53
7.2.1 Version Number(s).....	45	9.7 DISCLAIMERS OF WARRANTIES.....	53
7.2.2 CRL and CRL Entry Extensions.....	45	9.8 LIMITATIONS OF LIABILITY.....	53
7.3 OCSP PROFILE.....	45	9.8.1 Certification Authority Liability.....	53
7.3.1 Version Number(s).....	45	9.8.2 Registration Authority Liability.....	54
7.3.2 OCSP Extensions.....	45	9.8.3 Subscriber Liability.....	54
<b>8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....</b>	<b>46</b>	9.8.4 Relying Party Liability.....	55
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT.....	46	9.9 INDEMNITIES.....	55
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR.....	46	9.9.1 Indemnification by Subscribers.....	55
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY.....	46	9.9.2 Indemnification by Relying Parties.....	55
8.4 TOPICS COVERED BY ASSESSMENT.....	46	9.9.3 Indemnification of Application Software Suppliers.....	55
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY.....	46	9.10 TERM AND TERMINATION.....	56
8.6 COMMUNICATION OF RESULTS.....	46	9.10.1 Term.....	56
<b>9. OTHER BUSINESS AND LEGAL MATTERS.....</b>	<b>48</b>	9.10.2 Termination.....	56
9.1 FEES.....	48	9.10.3 Effect of Termination and Survival.....	56
9.1.1 Certificate Issuance or Renewal Fees.....	48	9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS... 56	
9.1.2 Certificate Access Fees.....	48	9.12 AMENDMENTS.....	56
9.1.3 Revocation or Status Information Access Fees.....	48	9.12.1 Procedure for Amendment.....	56
9.1.4 Fees for Other Services.....	48	9.12.2 Notification Mechanism and Period.....	57
9.1.5 Refund Policy.....	48	9.12.3 Circumstances under Which OID must be Changed.....	57
9.2 FINANCIAL RESPONSIBILITY.....	49	9.13 DISPUTE RESOLUTION PROVISIONS.....	57
9.2.1 Insurance Coverage.....	49	9.13.1 Disputes among thawte and Customers.....	57
9.2.2 Other Assets.....	49	9.13.2 Disputes with End-User Subscribers or Relying Parties.....	57
9.2.3 Insurance or Warranty Coverage for End-Entities.....	49	9.14 GOVERNING LAW.....	57
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION.....	49	9.15 COMPLIANCE WITH APPLICABLE LAW.....	58
9.3.1 Scope of Confidential Information.....	49	9.16 MISCELLANEOUS PROVISIONS.....	58
9.3.2 Information Not Within the Scope of Confidential Information.....	49	9.16.1 Entire Agreement.....	58
9.3.3 Responsibility to Protect Confidential Information.....	50	9.16.2 Assignment.....	58
9.4 PRIVACY OF PERSONAL INFORMATION.....	50	9.16.3 Severability.....	58
9.4.1 Privacy Plan.....	50	9.16.4 Enforcement (Attorney Fees and Waiver of Rights).....	58
9.4.2 Information Treated as Private.....	50	9.17 OTHER PROVISIONS.....	58
9.4.3 Information Not Deemed Private.....	50	<b>APPENDIX A: DEFINITIONS AND ACRONYMS.....</b>	<b>59</b>
9.4.4 Responsibility to Protect Private Information.....	50	<b>APPENDIX B1: SUPPLEMENTAL VALIDATION PROCEDURES FOR EXTENDED VALIDATION (EV) SSL CERTIFICATES.....</b>	<b>65</b>
9.4.5 Notice and Consent to Use Private Information.....	50	<b>APPENDIX B2: MINIMUM CRYPTOGRAPHIC ALGORITHM AND KEY SIZES FOR EV CERTIFICATES.....</b>	<b>66</b>
9.4.6 Disclosure Pursuant to Judicial or Administrative Process.....	50	<b>APPENDIX B3: EV CERTIFICATES REQUIRING CERTIFICATE EXTENSIONS.....</b>	<b>67</b>
9.4.7 Other Information Disclosure Circumstances.....	50	<b>APPENDIX B4: FOREIGN ORGANIZATION GUIDELINES.....</b>	<b>69</b>
9.5 INTELLECTUAL PROPERTY RIGHTS.....	50	<b>APPENDIX C: SUPPLEMENTAL VALIDATION PROCEDURES FOR EXTENDED VALIDATION (EV) CODE-SIGNING CERTIFICATES.....</b>	<b>70</b>
9.5.1 Property Rights in Certificates and Revocation Information.....	50	<b>APPENDIX D: SUPPLEMENTAL BASELINE REQUIREMENTS FOR ISSUANCE AND MANAGEMENT OF PUBLICLY-TRUSTED CERTIFICATES.....</b>	<b>71</b>
9.5.2 Property Rights in the CPS.....	51	<b>APPENDIX E: CHANGE HISTORY.....</b>	<b>72</b>
9.5.3 Property Rights in Names.....	51		
9.5.4 Property Rights in Keys and Key Material.....	51		
9.6 REPRESENTATIONS AND WARRANTIES.....	51		
9.6.1 CA Representations and Warranties.....	51		
9.6.2 RA Representations and Warranties.....	51		
9.6.3 Subscriber Representations and Warranties.....	51		

# 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”). This document contains both the requirements of a Certificate Policy and a Certificate Practice Statement. The **thawte** PKI operates as a single, independent PKI with a single CPS. This document should not be considered subordinate to the Symantec Trust Network Certificate Policy.

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](http://www.cabforum.org). In the event of any inconsistency between this document and those Requirements, 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), Individual-Validated (IV) and Organization-Validated (OV) SSL Certificates issued by **thawte** CAs under this CPS conform with the CABF Baseline Requirements. Such DV, IV and OV certificates are issued containing the corresponding policy identifier(s) indicating adherence to and conformance with these requirements. **thawte** CAs assert that all Certificates issued containing these policy identifier(s) are issued and managed in conformance with the CABF Requirements.

Management may make exceptions to this policy on a case by case basis to mitigate material, imminent impacts to customers, partners, relying parties, and/or others within the certificate ecosystem where practical workarounds do not exist. Any such management exceptions are documented, tracked, and reported as part of the audit process.

The **thawte** CA is managed within a dedicated business unit within Symantec and operates separately from the business units responsible for the Company's other security offerings. The STN shall not issue SSL inspection intermediate CAs from roots that are part of the Network. Only roots with no current or previous trust in Application Software Supplier products (private roots) may be used to create intermediate CAs used for SSL inspection.

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

All DV and OV certificates issued on or after March 5<sup>th</sup>, 2015 will include the applicable CABF policy OIDs:

- CABF OID for DV certificates: 2.23.140.1.2.1
- CABF OID for OV certificates: 2.23.140.1.2.2
- CABF OID for IV certificates: 2.23.140.1.2.3

All individual validated certificates issued after December 1, 2016 will include the applicable CABF policy OID.

Effective February 1, 2017 and after, **thawte** adopts the current version of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at <https://aka.ms/csbr>. If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

Code signing certificates issued on or after February 1<sup>st</sup>, 2017 and intended for use in Microsoft Authenticode and subsequent technologies will include the applicable certificate policy identifier, 2.23.140.1.4.1, to indicate compliance with the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.

## 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.

**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:

Certificate Type	Assurance Level	Issued to	Description and Benefit
SSL Web Server Certificates with EV	High with extended validation	Organizations	High Assurance with extended validation secure SSL certificates issued by <b>thawte</b> in conformance with the Guidelines for Extended Validation Certificates. Capable of 256-bit encryption used to support SSL sessions between web browsers and servers.

Certificate Type	Assurance Level	Issued to	Description and Benefit
SSL Web Server Certificates	High	Organizations (including sole proprietors) and individuals in the USA and Germany	High Assurance secure SSL certificates with stringent 3 step authentication capable of 256-bit encryption used to support SSL sessions between web browsers and servers.
Wildcard Certificates	High	Organizations (including sole proprietors) and individuals in the USA and Germany	Secure SSL certificates with stringent 3 step authentication capable of 256-bit encryption that secure multiple hosts on a single domain on the same server.
SGC SuperCerts	High	Organizations (including sole proprietors) and individuals in the USA and Germany	High Assurance Premium Server Gated Cryptography SSL certificates with stringent 3 step authentication, automatic 128-bit step-up encryption and capable of 256-bit encryption * used to support SSL sessions between web browsers and web servers. * Compatible with browsers IE 4.X or Netscape 4.06 and later
Code Signing Certificates	High	Organizations (including sole proprietors and individuals in the USA and Germany le proprietors)	Certificates which secure delivery of code and content to browsers over the Internet.
SSL123 Certificates	Medium	Registered Domain	Medium Assurance domain validated SSL certificates capable of 256-bit encryption used to support SSL sessions between web browsers and servers.

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

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

Program	Purpose and Benefit	Program Description
<i>thawte</i> Certificate Center Enterprise (TCCE) Program	The <i>thawte</i> 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.	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, <i>thawte</i> performs the back-end certificate issuance. Customers only issue certificates for SSL Web Server, SGC SuperCerts and Code Signing Certificates within their own organizations.
Reseller Partner Program	This program provides a one-stop base that allows Resellers to purchase, manage and resell SSL Web Server, SSL Wildcard, SSL123, SGC SuperCerts and Code Signing Certificates.	<i>thawte's</i> Reseller Partner Program offers Resellers (e.g. Web Hosting companies, ISPs, Registrars) the ability to enroll for SSL Web Server, SSL Wildcard, SSL123, SGC SuperCerts and Code Signing Certificates on behalf of their customers. Although the Reseller assists with the enrollment process ( <i>See</i> CPS § 4.1.2), the Reseller does not perform validation functions, but instead <i>thawte</i> 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.



Program	Purpose and Benefit	Program Description
<b>t-refer</b> Program	This program allows companies to refer customers to <b>thawte</b> . 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.	<b>t-refer</b> allows entities to install a link on their website: via this link their customers can buy <b>thawte</b> 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 <b>thawte</b> for compensation without having to pre-pay. The discounts offered in the referral channel are lower than those in the Reseller Partner Program. The customer is responsible for both the enrollment and payment of their certificate.

Table 2 – **thawte** PKI Programs

## 1.2 Document Name and Identification

This document is the **thawte** Certification Practice Statement and it expresses **thawte's** Certificate Policy.

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:

<b>thawte Root CA</b>	<b>CA Description</b>	<b>Registration Authorities</b>
<b>thawte</b> Server CA	As of March 2015, this root is excluded from the scope of the WebTrust for Certification Authorities – SSL Baseline Requirements (WebTrust for CA – BR) Audit.	<ul style="list-style-type: none"> <li>• <input type="checkbox"/> <b>thawte</b></li> <li>• <b>thawte</b> TCCE Customers</li> </ul>
<b>thawte</b> Primary Root CA	High Assurance offline Root CA that issues: <ul style="list-style-type: none"> <li>• Sub-CA Certificates for <b>thawte</b> Issuing CAs for Extended Validation, organization validated, domain validated and Code Signing certificates</li> </ul>	<b>thawte</b>
Symantec Class 3 Public Primary CA	High Assurance Root CA that issues: <ul style="list-style-type: none"> <li>• Sub-CA Certificates for <b>thawte</b> Issuing CAs for <b>thawte</b> SGC SuperCert Certificates</li> </ul>	Symantec
<b>thawte</b> Premium Server CA	<ul style="list-style-type: none"> <li>• As of March 2015, this root is excluded from the scope of the WebTrust for Certification Authorities – SSL Baseline Requirements (WebTrust for CA – BR) Audit.</li> </ul>	<b>thawte</b>
<b>thawte</b> Time Stamping CA	Medium Assurance Root CA that issues: <ul style="list-style-type: none"> <li>• Sub-CA Certificates for Symantec Issuing CA.</li> <li>• End entity certificate for GeoTrust time stamping services.</li> </ul>	<b>thawte</b>
<b>thawte</b> Primary Root CA – G2	Currently inactive	<b>thawte</b>
<b>thawte</b> Primary Root CA – G3	Currently inactive	<b>thawte</b>
<b>thawte</b> Primary Root CA – G4	Root CA issuing Sub CA Certificates for <b>thawte</b> Issuing CAs which issue EV and Organization Validated (OV) end entity certificates.	<b>thawte</b>

**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](http://www.thawte.com/repository) for updates to the current listing of **thawte** CAs.

### 1.3.2 Registration Authorities

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

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

**Table 4 – RAs within the **thawte** PKI**

### 1.3.3 Subscribers

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

Class	Issued to	Types of Subscribers
<b>Medium Assurance</b>	Registered Domains	Any person who has control of a domain referring to a device including, but not limited to: <ul style="list-style-type: none"> <li>• Web servers, mail servers and web traffic management devices</li> <li>• Intranet device utilizing IP addresses</li> </ul> Note that the use of Certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name has been deprecated by the CA / Browser Forum and will be eliminated by October 2016. Any such certificate issued prior to October 2016 must have an expiry date of 1 November 2015 or earlier. Previously issued certificates with expiry dates after 1 November 2015 will be revoked effective 1 October 2016.
<b>High Assurance</b>	Organizations	Organizations (including agencies, Educational Institutions, Government Departments, etc.) that control a device including, but not limited to: <ul style="list-style-type: none"> <li>• Web servers, mail servers and web traffic management devices</li> <li>• Devices digitally signing code or other content.</li> </ul>
	Sole Proprietors	Small Office Home Office (“SOHO”) clients that are typically individuals who run a sole proprietor online or development business.
<b>High Assurance with extended validation</b>	Organizations	Incorporated Organizations (including government agencies, Educational Institutions, Government Departments, etc.) The types of Organizations that qualify for EV Certificates are more fully described in Appendix B1 of this CPS.

**Table 5 – Subscribers within the *thawte* PKI**

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

### 1.3.4 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.

**thawte** does not issue any certificate that can be used for man-in-the-middle (MITM) or traffic management of domain names or IP addresses that the certificate holder does not legitimately own or control. Such certificate usage is expressly prohibited.

**thawte** periodically rekeys Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. **thawte** therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates.

### ***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)  
[practices@symantec.com](mailto:practices@symantec.com)

### **1.5.2 Contact Person**

Address inquiries about the CPS to [practices@symantec.com](mailto: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)  
[practices@symantec.com](mailto:practices@symantec.com)

Contact information for the CA/Browser Forum is available here: <https://cabforum.org/leadership/>

### **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](http://www.thawte.com/repository).

**thawte** publishes Certificates in accordance with Table 6 below.

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

**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](http://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](mailto: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.

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

### 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. **thawte** makes their repositories publicly available in a read-only manner at the link stated in section 2.3.

### 3. IDENTIFICATION AND AUTHENTICATION

#### 3.1 Naming

##### 3.1.1 Types of Names

###### 3.1.1.1 CA Certificates

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

Attribute	Value
Common Name (CN)	CA Name
Organizational Unit (OU)	Optional
Organization (O)	"Thawte Consulting cc" or "Thawte Consulting" or "Thawte" or "Thawte Inc."
Locality (L)	"California" or another locality where <b>thawte</b> legally conducts business, or not used.
State or Province (P)	"California" or another locality where <b>thawte</b> legally conducts business, or not used.
Country (C)	"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.
E-Mail (E)	May be used for Root CAs to include a contact e-mail address for the CA.

**Table 7 – Distinguished Name Attributes in CA Certificates**

###### 3.1.1.2 Server Certificates

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

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

**Table 8 – Distinguished Name Attributes in Server Certificates**

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

###### 3.1.1.3 Certificate Subject details –SSL 123

###### 3.1.1.3.1 Certificate subject details – SSL123Certificates

Attribute	Value
Common Name (CN)	Registered domain name
Organizational Unit (OU)	"Domain Validated"
Organizational Unit (OU)	Go to <a href="https://www.thawte.com/repository/index.html">https://www.thawte.com/repository/index.html</a>
Organizational Unit (OU)	<b>thawte</b> SSL123 Certificate

Attribute	Value
Organization (O)	Not used
Locality (L)	Not used
State or Province (P)	Not used
Country (C)	Not used
E-Mail (E)	Not used

**Table 9 – Distinguished Name Attributes in SSL123 Certificates**

### **3.1.1.3.2 Code Signing Certificates**

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

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

**Table 11 – Distinguished Name Attributes in Code Signing Certificates**

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).

### **3.1.1.3.3 SSL Web Server Certificates with EV**

“SSL Web Server Certificates with EV distinguished name attributes are discussed in Section 3 of Appendix B3 to this CPS.”

### **3.1.1.3.4 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, 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***

**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.

Where a domain name or e-mail address is included in the certificate **thawte** authenticates the Organization's right to use that domain name. **thawte** uses the following methods of vetting a domain name, with option 1 being the primary method:

1. Confirm the Applicant as the Domain Name Registrant directly with the Domain Name Registrar by performing a whois look up.
2. Communicate directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar;
3. Rely upon a Domain Authorization Document;
4. Communicate directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field;
5. Communicate with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN;
6. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN.

With respect to **thawte** Certificate Center Enterprise (TCCE), formerly SPKI, Customers, the identity confirmation process begins with **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 **thawte** Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively..

#### **3.2.2.1.2 Mozilla Verification Requirements for Organization Applicants**

For requests for internationalized domain names (IDNs) in Certificates, **thawte** performs domain name owner verification to detect cases of homographic spoofing of IDNs. **thawte** employs an automated process that searches various 'whois' services to find the owner of a particular domain. A search failure result is flagged for manual review and the RA manually rejects the Certificate Request. Additionally, the RA rejects any domain name that visually appears to be made up of multiple scripts within one hostname label.

**thawte** actively participates in the CA/Browser Forum providing input to the standards for IDN Certificates and fully commits to complying with standards drafted by that body.

### **3.2.3 Authentication of Individual Identity**

Where applicable to the information available about an Applicant that is not registered under any authority, **thawte** performs Individual Validation as described in section 3.2.3 of the CABF Baseline Requirements.

### **3.2.4 Non-Verified Subscriber Information**

No stipulation.

### 3.2.5 Validation of Authority

Whenever an individual's name is associated with an Organization name in a certificate in such a way to indicate the individual's affiliation or authorization to act on behalf of the Organization the CA or RA:

- determines that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or recognized authority that confirms the existence of the organization, and
- Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.

### 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.

Timing	Requirement
Prior to Certificate expiration	For replacement of a Certificate following revocation of the Certificate, <b>thawte</b> 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.
After Certificate expiration	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.

**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.

## 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.

Certificate Type	Entity Processing Certificate Applications	Entity Issuing Certificate
High Assurance with extended validation – SSL Web Server Certificates with EV	<b>thawte</b>	<b>thawte</b>
High Assurance – SSL Web Server Certificates and Code Signing	<ul style="list-style-type: none"><li>• <b>thawte</b></li><li>• TCCE Customers</li></ul>	<b>thawte</b>
Medium Assurance – SSL123 Certificates	<b>thawte</b>	<b>thawte</b>

**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.

##### 4.1.2.2 CABF Certificate Application Requirements

Practices for Certificate enrollment for EV SSL Certificates, Domain-Validated and Organization-Validated SSL Certificates are documented in this CPS and comply with section 3 of the applicable governing CA/Browser Forum Guidelines published at [www.cabforum.org](http://www.cabforum.org).

### 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, 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.

## **4.2.4 Certificate Authority Authorization (CAA)**

As of October 1, 2015, Thawte will check Certificate Authority Authorization (CAA) records as part of its public SSL certificate authentication and verification processes. Prior to this date Thawte may not check CAA records for all public SSL certificate orders. 'Public SSL Certificates' are those that chain up to our publicly available root certificates and which meet CA/Browser Forum Baseline or Extended Validation Requirements.

## ***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.

**thawte** CA certificate requests are created and approved by authorized **thawte** personnel through a controlled process that requires the participation of multiple trusted individuals.

## ***4.4 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.

Certificate Type	Routine Rekey and Renewal Requirements
Code Signing Certificates (excluding Java Code Signing Certificates)	For these types of Certificates, Subscriber key pairs are browser generated as part of the online enrollment process. The Subscriber does not have the option to submit an existing key pair for "renewal." Accordingly, for these types of Certificates, rekey is supported and Certificate renewal is not.
Server Certificates and Java Code Signing Certificates	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. <b>thawte</b> will sign the previous CSR for the new validity period, where the server's key management functionality allows the installation of a new certificate for an existing key pair. Accordingly, for Server Certificates, both rekey and renewal are supported.
CA Certificates	Renewal of CA Certificates is permitted as long as the cumulative certified lifetime of the CA key pair does not exceed the applicable maximum CA key pair lifetime specified in CPS § 6.3.2. <b>thawte</b> CAs may also be rekeyed in accordance with CPS § 5.6. Accordingly, for <b>thawte</b> CA Certificates both rekey and certificate renewal are supported.

**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,
- In the case of code signing certificates,
  - An Application Software Supplier requests the CA revoke and an investigation indicates that the certificate is being used to sign malware or other unwanted software,
  - A report is submitted to **thawte** indicating that the certificate was used to sign malware,
- 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.

When considering whether certificate usage is harmful to the **thawte** trust infrastructure, **thawte** considers, among other things, the following:

- The nature and number of complaints received
- The identity of the complainant(s)
- Relevant legislation in force
- Responses to the alleged harmful use from the Subscriber

When considering whether the use of a Code Signing Certificate is harmful to the **thawte** trust infrastructure, **thawte** additionally considers, among other things, the following:

- The name of the code being signed
- The behavior of the code
- Methods of distributing the code
- Disclosures made to recipients of the code
- Any additional allegations made about the code
- Effective February 1, 2017, whether the Code Signing Certificate satisfies any of the Reasons for Revoking a Subscriber Certificate in section 13.1.5 of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates as adopted by Microsoft

**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, 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.

Regarding code signing certificates, **thawte** provides Anti-Malware Organizations, Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions on how they can report suspected Private Key Compromise, Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. **thawte** publicly discloses the instructions on its website.

**thawte** revokes a Code Signing Certificate in any of these four circumstances: (1) the Application Software Supplier requests revocation and **thawte** does not intend to pursue an alternative course of action, (2) the authenticated subscriber requests revocation, (3) a third party provides information that leads the CA to believe that the certificate is compromised or is being used for Suspect Code, or (4) the CA otherwise decides that the certificate should be revoked. **thawte** follows the process for handling

revocation requests detailed at section 13.1.5 of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.

Any person claiming to have witnessed certificate misuse, inappropriate conduct related to certificates, fraud or key compromise may submit a Certificate Problem Report using the online form available at the **thawte** website. **thawte** will investigate all Certificate Problem Reports and take action within the prescribed timing stated in the CABF Baseline Requirements.

### 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, Appendix B1, Appendix C and 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. Effective February 1, 2017, **thawte** complies with the revocation timeframes specified for malware in the Minimum Requirements for Issuance and Management of Publicly-Trusted Code Signing Certificates in section 13.1.5.3 for code signing certificates.

### 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:

CA Type	CA Name	CRL Issuance Frequency
Root CAs (Non-Issuing)	<b>thawte</b> Personal Freemail CA (terminated) <b>thawte</b> Primary Root CA <b>thawte</b> Primary Root CA –G2 <b>thawte</b> Primary Root CA – G3 <b>thawte</b> Primary Root CA – G4 <b>thawte</b> Time Stamping CA	At least quarterly and upon Sub-CA certificate revocation
	<b>thawte</b> Server CA <b>thawte</b> Premium Server CA	At least daily

CA Type	CA Name	CRL Issuance Frequency
Subordinate Issuing CAs	<b>thawte</b> Personal Freemail Issuing CA (terminated) <b>thawte</b> Extended Validation SSL CA <b>thawte</b> Code Signing CA – G2 <b>thawte</b> DV SSL CA <b>thawte</b> SSL CA <b>thawte</b> SGC CA – G2 <b>thawte</b> DSA SSL CA	At least daily

**Table 16 – CRL Issuance Frequency**

Expired Certificates are removed from the CRL after the Certificates' expiration with the exception of code signing certificates, effective February 1, 2017 in compliance with the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at <https://aka.ms/csbr>

#### ***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, Appendix B1, Appendix C, and Appendix D, respectively.

#### ***4.9.7.2 Microsoft Requirements for CRL Issuance***

Frequency of CRL issuance for code signing and timestamp certificates is documented in the **thawte** CPS and complies with section 13,2,2 of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at <https://aka.ms/csbr>.

### **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 Appendix B1, Appendix C, and Appendix D, respectively.

#### ***4.9.9.2 Microsoft Requirements for OCSP Availability***

**thawte** provides OCSP responses for Code Signing Certificates and Timestamp Certificates for the time period specified in this CPS, which is 10 years after the expiration of the certificate. Revoked certificates remain on the CRL for at least 10 years after the expiration of the certificate.

#### **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, Appendix B1, Appendix C and 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, 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** employees in a comparable position.

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

### **5.3.8 Documentation Supplied to Personnel**

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

## ***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 driver's 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 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 10 years and six months 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, PKI 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, Appendix B1, Appendix C and 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, 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 140-2 level 3.

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 Transport Layer Security (TLS). Currently, TLS 1.0, 1.1, 1.2 are supported on our consoles. SSL v1, v2 and v3 are not supported.

#### 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, DSA and within a selected group or those in a closed ecosystem.

### 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, Appendix B1, Appendix C and Appendix D, respectively.

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

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

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

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

	Validity period beginning on or before 31 Dec 2010 and ending on or before 31 Dec 2013	Validity period beginning after 31 Dec 2010 or ending after 31 Dec 2013
Digest algorithm	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
Minimum DSA modulus size (bits)	N/A	2048
ECC curve	NIST P-256, P-384 or P-521	NIST P-256, P-384 or P-521

**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.

	Validity period ending on or before 31 Dec 2013	Validity period ending after 31 Dec 2013
Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
Minimum DSA modulus size (bits)	2048	2048
ECC curve	NIST P-256, P-384 or P-521	NIST P-256, P-384 or P-521

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

\* SHA-1 MAY be used with RSA keys in accordance with the criteria defined in Section 7.1.3 of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

\*\* 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 not 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 140-2 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.

Certificate Issued By:	Operational Period
Root CAs	Up to 25 years
Root CA to Sub-CA	Up to 10 years
CA to end-user Subscriber	Up to 5 years <sup>1</sup>

**Table 18 – Certificate Operational Periods**

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

---

<sup>1</sup> 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.

### ***6.3.2.1 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, Appendix B1, Appendix C and Appendix D, respectively.

## **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 the Symantec Security and Audit Requirements guide.

### **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, 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 the Symantec Security and Audit Requirements guide 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** Certificates conform to ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 5280"). As applicable to the Certificate type, **thawte** Certificates conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

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

Field	Value or Value constraint	
Version	Version 3	
Serial Number	Unique value per Issuer DN that contains at least 64 bits of entropy output from a CSPRNG	
Signature Algorithm	sha256RSA: Certificate signatures produced using these algorithms shall comply with RFC 3279. Use of sha256WithRSAEncryption shall be used over sha-1WithRSAEncryption except in support of legacy applications and in full compliance of CA/Browser Forum and Application Software Supplier procedures and policies for support of legacy applications with SHA-1	
Issuer Distinguished Name	Common Name (CN) =	CA Name
	Organizational Unit (OU) =	Optional
	Organization (O) =	"Thawte Consulting cc" or "Thawte Consulting" or "Thawte"
	Locality (L) =	"California" or another locality where <b>thawte</b> legally conducts business or not used.
	State or Province (P) =	"California" or another locality where Thawte legally conducts business, or not used.
	Country (C) =	"US" (except for <b>thawte</b> Code Signing CA which omits 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.
	E-Mail (E) =	May be used for Root CAs to include a contact e-mail address for the CA.
Valid From	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 5280.	
Valid To	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 5280. The validity period will be set in accordance with the constraints specified in CPS § 6.3.2.	
Subject Distinguished Name	Populated in accordance with CPS §3.1.1.	
Subject Public Key	Encoded in accordance with RFC 5280 using the RSA algorithm and key lengths in accordance with CPS § 6.1.5 .	
Signature	Generated and encoded in accordance with RFC 5280.	

**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.

Note: Thawte certificates that do not conform to the current version of the CA/Browser Forum Baseline Requirements that have a key pair and key length size less than 2048bit may have server auth removed and/or a designated OID of 2.16.840.1.113733.1.8.54.1.

#### 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, Appendix B1, Appendix C, and Appendix D, respectively.

For all web server certificates, the SubjectAltName extension is populated with the authenticated value in the Common Name field of the subject DN (domain name or public IPAddress). The SubjectAltName extension may contain additional authenticated domain names or public IPAddresses.

### 7.1.2.1 Root CA Certificates

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

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

**Table 20 – Root CA Certificate Extensions**

Note: Thawte certificates that have a non-standard key pair and key length size of less than 2048bit are authorized to be used within a selected group or closed eco system.

### 7.1.2.2 Subordinate CA Certificates

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

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

**Table 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:

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

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

### 7.1.2.4 SSL 123 Certificates

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

Extension	Value or Value Constraint	Criticality
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Critical

<b>Extension</b>	<b>Value or Value Constraint</b>	<b>Criticality</b>
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	Non-Critical
Authority information Access	<a href="http://ocsp.thawte.com">http://ocsp.thawte.com</a>	Non-Critical

**Table 23 – thawte SSL123 Certificate Extensions**

### **7.1.2.5 SGC SuperCerts**

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

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

**Table 24 –thawte SGC SuperCert Certificate Extensions**

### **7.1.2.6 SSL Wildcard Certificates**

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

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

**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 3 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:

<b>Extension</b>	<b>Value or Value Constraint</b>	<b>Criticality</b>
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Critical
Enhanced Key Usage	Code Signing(1.3.6.1.5.5.7.3.3)	Non-Critical
NetscapeCertType	Signature(10)	Non-Critical
Key Usage Restriction	Cert PolicyId=1.3.6.1.4.1.311.2.1.22 Restricted Key Usage=Digital Signature(80)	Non-Critical
Subject Alternative Name	DNS Name=domain name of Subscriber's web site	Non-Critical



CRL Distribution Points	<a href="http://crl.thawte.com/ThawteCodeSigningCA.crl">http://crl.thawte.com/ThawteCodeSigningCA.crl</a>	Non-Critical
-------------------------	---	--------------

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, 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:

Field	Value or Value constraint
Version	See CPS §7.2.1.
Signature Algorithm	Algorithm used to sign the CRL. <b>thawte</b> CRLs are signed using sha1RSA (OID: 1.2.840.113549.1.1.4) in accordance with RFC 5280.
Issuer	Entity who has signed and issued the CRL. The CRL Issuer Name is in accordance with the Issuer Distinguished Name requirements specified in CPS § 3.1.1.
Effective Date	Issue date of the CRL. <b>thawte</b> CRLs are effective upon issuance.

<b>Field</b>	<b>Value or Value constraint</b>
Next Update	Date by which the next CRL will be issued. The Next Update date for <b>thawte</b> CRLs is set as follows: 3 months from the Effective Date for <b>thawte</b> Non-Issuing Root CAs and 28 days from the Effective Date for other <b>thawte</b> CAs. CRL issuance frequency is in accordance with the requirements of CPS § 4.9.7.
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

**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-validated and organization-validated SSL Certificates, **thawte** provides OCSP responses compliant with RFC 6960 and as further set forth in the **thawte** Supplemental Procedures, Appendix B1, Appendix C, 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, Appendix B1, Appendix C, and 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](mailto: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-irhome>

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

## **9.6 Representations and Warranties**

### **9.6.1 CA Representations and Warranties**

CAs perform the specific obligations appearing throughout this CPS. In addition, **thawte** uses commercially reasonable efforts to ensure that Subscriber Agreements and Relying Party Agreements bind Subscribers and Relying Parties within the **thawte** PKI. Examples of such efforts include, but are not limited to, requiring assent to a Subscriber Agreement as a condition of enrollment or requiring assent to a Relying Party Agreement as a condition of receiving Certificate status information. Similarly, Resellers (where required by contract) must use Subscriber Agreements and Relying Party Agreements in accordance with the requirements imposed by **thawte**. The Subscriber Agreements and Relying Party Agreements used by **thawte** and Resellers must include the provisions required by CPS §§ 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, Appendix B1, Appendix C, and 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](http://www.thawte.com/repository).



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

Subscriber Agreements apply the specific obligations appearing in the CPS to Subscribers within the **thawte** PKI. Subscriber Agreements require Subscribers to use their Certificates in accordance with CPS § 1.4. 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](http://www.thawte.com/repository).

Relying Party Agreements within the **thawte** PKI state that, before any act of reliance Relying Parties must independently assess the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose. They state that **thawte**, CAs, and RAs are not responsible for assessing the appropriateness of the use of a Certificate. Relying Party Agreements specifically state that Relying Parties must not use Certificates beyond the limitations in CPS § 1.4.1.2 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 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](http://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](http://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 Dispute Resolution Provisions***

### **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

<b>Term</b>	<b>Definition</b>
<b>Administrator</b>	A Trusted Person that performs validation and other CA or RA functions at <b>thawte</b> .
<b>Affiliate</b>	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 " <i>Affiliate</i> " 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.
<b>Applicant</b>	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.
<b>Applicant Representative</b>	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.
<b>Application Software Supplier</b>	A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.
<b>Attestation Letter</b>	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.
<b>Audit Report</b>	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.
<b>Certificate</b>	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.
<b>Certificate Applicant</b>	An individual or organization that requests the issuance of a Certificate by a CA.
<b>Certificate Application</b>	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
<b>Certificate Chain</b>	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
<b>Certificate Data</b>	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.
<b>Certificate Revocation List (CRL)</b>	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.
<b>Certificate Signing Request</b>	A message conveying a request to have a Certificate issued.
<b>Certification Authority (CA)</b>	An entity authorized to issue, manage, revoke, and renew Certificates in the <b>thawte</b> PKI.
<b>Certificate Management Process</b>	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.
<b>Certification Practice Statement (CPS)</b>	A statement of the practices that <b>thawte</b> 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.
<b>Certificate Problem Report</b>	Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates
<b>Code Signing Certificates</b>	Certificates which secure delivery of code and content to browsers over the Internet.
<b>Compliance Audit</b>	A periodic audit that the <b>thawte</b> PKI or its Customer undergoes to determine its conformance with <b>thawte</b> requirements that apply to it.



<b>Term</b>	<b>Definition</b>
<b>Compromise</b>	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.
<b>Confidential/Private Information</b>	Information required to be kept confidential and private.
<b>Country</b>	A Country shall mean a Sovereign state as defined in the Guidelines.
<b>Cross Certificate</b>	A certificate that is used to establish a trust relationship between two Root CAs.
<b>Cryptographically Secure Pseudo-Random Number Generator</b>	A random number generator intended for use in a cryptographic system.
<b>Customer</b>	An individual or organization that has purchased a product or service from <b>thawte</b> and/or its representatives.
<b>Delegated Third Party</b>	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.
<b>Domain Authorization</b>	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.
<b>Domain Name</b>	The label assigned to a node in the Domain Name System.
<b>Domain Namespace</b>	The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
<b>Domain Name Registrant</b>	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.
<b>Domain Name Registrar</b>	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).
<b>Expiry Date</b>	The "Not After" date in a Certificate that defines the end of a Certificate's validity period.
<b>EV Certificate</b>	A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the guidelines.
<b>Fully-Qualified Domain Name</b>	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
<b>Government Entity</b>	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.).
<b>High Assurance</b>	Certificates issued to organizations and sole proprietors to provide stringent 3 step authentication; message, software, and content integrity; and confidentiality encryption.
<b>Intellectual Property Rights</b>	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
<b>International Organization</b>	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.
<b>Internal Server Name</b>	A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.
<b>Issuing CA</b>	In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
<b>Key Compromise</b>	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.
<b>Key Generation Ceremony</b>	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.
<b>Key Generation Script</b>	A documented plan of procedures for the generation of a CA Key Pair.
<b>Key Pair</b>	The Private Key and its associated Public Key.
<b>Legal Entity</b>	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

<b>Term</b>	<b>Definition</b>
<b>Medium Assurance</b>	Certificates that are issued to Domains to provide confidentiality encryption. <b>thawte</b> 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.
<b>Non-repudiation</b>	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 <b>thawte</b> Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
<b>Nonverified Subscriber Information</b>	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.
<b>Object Identifier</b>	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
<b>OCSP (Online Certificate Status Protocol)</b>	An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information.
<b>OCSP Responder</b>	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.
<b>Operational Period</b>	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.
<b>Parent Company</b>	<b>Parent Company:</b> 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.
<b>PKCS #7</b>	Public-Key Cryptography Standard #7, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
<b>PKCS #10</b>	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
<b>PKCS #12</b>	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
<b>Principal Individual(s)</b>	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.
<b>Private Key</b>	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.
<b>Public Key</b>	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.
<b>Public Key Infrastructure (PKI)</b>	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The <b>thawte</b> PKI consists of systems that collaborate to provide and implement the <b>thawte</b> PKI.
<b>Publicly-Trusted Certificate</b>	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.
<b>Qualified Auditor</b>	A natural person or Legal Entity that meets the Auditor Qualifications.
<b>Referee</b>	An individual who is permitted by the <b>thawte</b> PKI to validate the identity of a Web of Trust subscriber in the event that a <b>thawte</b> Web of Trust Notary is not available. The referee must be a bank manager, registered lawyer, or registered CPA (accountant).

<b>Term</b>	<b>Definition</b>
<b>Registered Domain Name</b>	A Domain Name that has been registered with a Domain Name Registrar.
<b>Registration Agency</b>	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 to (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)
<b>Registration Authority (RA)</b>	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.
<b>Reliable Method of Communication</b>	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.
<b>Relying Party</b>	An individual or organization that acts in reliance on a certificate and/or a digital signature.
<b>Relying Party Agreement</b>	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
<b>Repository</b>	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.
<b>Reseller</b>	An entity marketing services on behalf of <b>thawte</b> to specific markets (e.g., the country representatives).
<b>Reseller Partner Program</b>	A program that allows Resellers to enroll for SSL Web Server Certificates, SSL Wildcard Certificates, SSL123 Certificates and SGC SuperCerts on behalf of end-user Subscribers who are customers of the Reseller.
<b>Reserved IP Address</b>	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>
<b>Root CA</b>	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
<b>Root Certificate</b>	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
<b>RSA</b>	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
<b>Secret Share</b>	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.
<b>Secret Sharing</b>	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.
<b>Sovereign State</b>	A Sovereign state is a state, or country, that administers its own government, and is not dependent upon, or subject to, another power.
<b>SSL123 Certificates</b>	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.
<b>SSL Web Server Certificates</b>	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.
<b>Subject</b>	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.
<b>Subject Identity Information</b>	Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the <i>subjectAltName</i> extension or the Subject <i>commonName</i> field.
<b>Subordinate CA</b>	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

<b>Term</b>	<b>Definition</b>
<b>Subscriber</b>	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.
<b>Subscriber Agreement</b>	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
<b>Subsidiary Company</b>	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.
<b>SGC SuperCerts</b>	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
<b>Superior Entity</b>	An entity above a certain entity within the <b>thawte</b> PKI.
<b>Terms of Use</b>	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.
<b>thawte PKI Participants</b>	An individual or organization that is one or more of the following within the <b>thawte</b> PKI: <b>thawte</b> , a Customer, a Reseller, a Subscriber, or a Relying Party.
<b>thawte Repository</b>	<b>thawte's</b> database of relevant <b>thawte</b> PKI information accessible on-line.
<b>thawte Security Policy</b>	The highest-level document describing <b>thawte's</b> security policies.
<b>Transport Layer Security (TLS)</b>	The proposed IETF standard, TLS, is the successor of Secure Sockets Layer (SSL). The protocol secures server-client communication by providing many different methods for exchanging keys, encrypting data and authenticating message integrity, including symmetric cryptography, public key cryptography, message authentication code, forward secrecy and others.
<b>Trusted Person</b>	An employee, contractor, or consultant of an entity within the <b>thawte</b> PKI responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices.
<b>Trusted Position</b>	The positions within a <b>thawte</b> PKI entity that must be held by a Trusted Person.
<b>Trustworthy System</b>	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.
<b>Unregistered Domain Name</b>	A Domain Name that is not a Registered Domain Name.
<b>Valid Certificate</b>	A Certificate that passes the validation procedure specified in RFC 5280.
<b>Validation Specialists</b>	Someone who performs the information verification duties specified by these Requirements.
<b>Validity Period</b>	The period of time measured from the date when the Certificate is issued until the Expiry Date.
<b>Web Host</b>	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.
<b>Wildcard Certificates</b>	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.

## Acronyms

<b>Acronym</b>	<b>Term</b>
<b>AICPA</b>	American Institute of Certified Public Accountants.
<b>ANSI</b>	The American National Standards Institute.
<b>BIS</b>	The United States Bureau of Industry and Science of the United States Department of Commerce.
<b>BXA</b>	The United States Bureau of Export Administration of the United States Department of Commerce.
<b>CA</b>	Certification Authority.
<b>ccTLD</b>	Country Code Top-Level Domain
<b>CICA</b>	Canadian Instituted of Chartered Accountants
<b>CPS</b>	Certification Practice Statement.
<b>CRL</b>	Certificate Revocation List.
<b>CSPRNG</b>	Cryptographically Secure Pseudo-Random Number Generator
<b>DBA</b>	Doing Business As
<b>DNS</b>	Domain Name System
<b>EV</b>	Extended Validation
<b>FIPS</b>	United States Federal Information Processing Standards.
<b>FQDN</b>	Fully Qualified Domain Name
<b>ICC</b>	International Chamber of Commerce.
<b>IM</b>	Instant Messaging
<b>IANA</b>	Internet Assigned Numbers Authority
<b>ICANN</b>	Internet Corporation for Assigned Names and Numbers
<b>ISO</b>	International Organization for Standardization
<b>NIST</b>	(US Government) National Institute of Standards and Technology
<b>OCSP</b>	Online Certificate Status Protocol.
<b>OID</b>	Object Identifier
<b>OFAC</b>	Office of Foreign Assets Control
<b>PIN</b>	Personal identification number.
<b>PKCS</b>	Public-Key Cryptography Standard.
<b>PKI</b>	Public Key Infrastructure.
<b>RA</b>	Registration Authority.
<b>RFC</b>	Request for comment.
<b>S/MIME</b>	Secure multipurpose Internet mail extensions.
<b>SSL</b>	Secure Sockets Layer.
<b>TLD</b>	Top-Level Domain
<b>TLS</b>	Transport Layer Security
<b>VOID</b>	Voice Over Internet Protocol

## **APPENDIX B1: Supplemental Validation Procedures for Extended Validation (EV) SSL Certificates**

The current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) SSL Certificates can be accessed at <https://cabforum.org/extended-validation/>

---

## APPENDIX B2: Minimum Cryptographic Algorithm and Key Sizes for EV Certificates

### 1. Root CA Certificates

	Key sizes
Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	2048 bit
ECC	256 or 384 v

### 2. Subordinate CA Certificates

	Key sizes
Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	2048 bit
ECC	256 or 384 bits

### 3. Subscriber Certificates

	Key sizes
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA-512
RSA	2048 bit
ECC	256 or 384 bits

\* SHA-1 MAY be used with RSA keys in accordance with the criteria defined in Section 7.1.3 of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

## 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)

- The *anyPolicy* identifier if subordinate CA is controlled by *thawte*
- 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

- id-qt 2 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier

- 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'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**

The current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) Code Signing Certificates can be accessed at <https://cabforum.org/ev-code-signing-certificate-guidelines/>

## **APPENDIX D: Supplemental Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates**

The current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates can be accessed at <https://cabforum.org/baseline-requirements-documents/>

## APPENDIX E: Change History

### History of changes: version 3.7.17 (effective Dec 2016)

Section	Changes made
Various	Miscellaneous clerical and administrative changes
1. INTRODUCTION	<p>Added: This document contains both the requirements of a Certificate Policy and a Certificate Practice Statement. The <b>thawte</b> PKI operates as a single, independent PKI with a single CPS. This document should not be considered subordinate to the Symantec Trust Network Certificate Policy.</p> <p>Management may make exceptions to this policy on a case by case basis to mitigate material, imminent impacts to customers, partners, relying parties, and/or others within the certificate ecosystem where practical workarounds do not exist. Any such management exceptions are documented, tracked, and reported as part of the audit process.</p> <p>The <b>thawte</b> CA is managed within a dedicated business unit within Symantec and operates separately from the business units responsible for the Company's other security offerings. The STN shall not issue SSL inspection intermediate CAs from roots that are part of the Network. Only roots with no current or previous trust in Application Software Supplier products (private roots) may be used to create intermediate CAs used for SSL inspection.</p> <p>Added to CABF conformity statement: Individual-Validated (IV)</p> <p>Added to CABF OID list:</p> <ul style="list-style-type: none"> <li>CABF OID for IV certificates: 2.23.140.1.2.3</li> </ul> <p>All individual validated certificates issued after December 1, 2016 will include the applicable CABF policy OID.</p>
1.2 Document Name and Identification	<p>Added clause at end: This document is the <b>thawte</b> Certification Practice Statement and it expresses <b>thawte's</b> Certificate Policy.</p>
1.4.2 Prohibited Certificate Uses	<p>Added: <b>thawte</b> does not issue any certificate that can be used for man-in-the-middle (MITM) or traffic management of domain names or IP addresses that the certificate holder does not legitimately own or control. Such certificate usage is expressly prohibited.</p>
3.2.3 Authentication of Individual Identity	<p>Removed: No stipulation.</p> <p>Added: Where applicable to the information available about an Applicant that is not registered under any authority, <b>thawte</b> performs Individual Validation as described in section 3.2.3 of the CABF Baseline Requirements.</p>
4.9.1 Circumstances for Revocation	<p>Added: When considering whether certificate usage is harmful to the <b>thawte</b> trust infrastructure, <b>thawte</b> considers, among other things, the following:</p> <ul style="list-style-type: none"> <li>The nature and number of complaints received</li> <li>The identity of the complainant(s)</li> <li>Relevant legislation in force</li> <li>Responses to the alleged harmful use from the Subscriber</li> </ul> <p>When considering whether the use of a Code Signing Certificate is harmful to the <b>thawte</b> trust infrastructure, <b>thawte</b> additionally considers, among other things, the following:</p> <ul style="list-style-type: none"> <li>The name of the code being signed</li> <li>The behavior of the code</li> <li>Methods of distributing the code</li> </ul>

Section	Changes made
	<ul style="list-style-type: none"> <li>Disclosures made to recipients of the code</li> <li>Any additional allegations made about the code</li> <li>Effective February 1, 2017, whether the Code Signing Certificate satisfies any of the Reasons for Revoking a Subscriber Certificate in section 13.1.5 of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates as adopted by Microsoft</li> </ul>
4.9.2 Who Can Request Revocation	Added: Any person claiming to have witnessed certificate misuse, inappropriate conduct related to certificates, fraud or key compromise may submit a Certificate Problem Report using the online form available at the <b>thawte</b> website. <b>thawte</b> will investigate all Certificate Problem Reports and take action within the prescribed timing stated in the CABF Baseline Requirements.
7.1.2.8 Code Signing Certificates	Removed from Enhanced Key Usage: In addition, Certificates issued for Microsoft code signing include: Microsoft Code Signing (1.3.6.1.4.1.311.2.1.22)

---

### History of changes: version 3.7.16 (effective Sep 2016)

Section	Changes made
Various	Miscellaneous clerical and administrative changes throughout document
1. INTRODUCTION	Added: Effective February 1, 2017 and after, <b>thawte</b> adopts the current version of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at <a href="https://aka.ms/csbr">https://aka.ms/csbr</a> . If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document.  Code signing certificates issued on or after February 1 <sup>st</sup> , 2017 and intended for use in Microsoft Authenticode and subsequent technologies will include the applicable certificate policy identifier, 2.23.140.1.4.1, to indicate compliance with the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.
1.4.2 Prohibited Certificate Uses	Added:  <b>thawte</b> periodically rekeys Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. <b>thawte</b> therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates.
1.5.2 Contact Person	Added: Contact information for the CA/Browser Forum is available here: <a href="https://cabforum.org/leadership/">https://cabforum.org/leadership/</a>
2.3 Time or Frequency of Publication	Added: <b>thawte</b> develops, implements, enforces, and annually updates a Certification Practices Statement that describes in detail how the CA implements the latest version of the CA/Browser Forum Baseline Requirements.
2.4 Access Controls on Repositories	Added: <b>thawte</b> makes their repositories publicly available in a read-only manner at the link stated in section 2.3.
3.2.5 Validation of Authority	Added: Whenever an individual's name is associated with an Organization name in a certificate in such a way to indicate the individual's affiliation or authorization to act on behalf of the Organization the CA or RA: <ul style="list-style-type: none"> <li>determines that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or recognized authority that confirms the existence of the organization, and</li> <li>Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of</li> </ul>

Section	Changes made
	the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.
4.1.2.2 CABF Certificate Application Requirements	Added: Practices for Certificate enrollment for EV SSL Certificates, Domain-Validated and Organization-Validated SSL Certificates are documented in this CPS and comply with section 3 of the applicable governing CA/Browser Forum Guidelines published at <a href="http://www.cabforum.org">www.cabforum.org</a> .
4.3.3 Certificate Issuance by a Root CA	Removed exception: The thawte Root CAs issue certificates only to subordinate CAs, <b>with the exception of the thawte Server CA which issues end-user Subscriber certificates.</b>
4.3.3.1 CABF Requirements for Certificate Issuance by a Root CA	Removed section.
4.9.1 Circumstances for Revocation	Added: <ul style="list-style-type: none"> <li>• In the case of code signing certificates, <ul style="list-style-type: none"> <li>○ An Application Software Supplier requests the CA revoke and an investigation indicates that the certificate is being used to sign malware or other unwanted software,</li> <li>○ A report is submitted to <b>thawte</b> indicating that the certificate was used to sign malware</li> </ul> </li> </ul>
4.9.2 Who Can Request Revocation	Added: Regarding code signing certificates, <b>thawte</b> provides Anti-Malware Organizations, Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions on how they can report suspected Private Key Compromise, Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. <b>thawte</b> publicly discloses the instructions on its website.  <b>thawte</b> revokes a Code Signing Certificate in any of these four circumstances: (1) the Application Software Supplier requests revocation and <b>thawte</b> does not intend to pursue an alternative course of action, (2) the authenticated subscriber requests revocation, (3) a third party provides information that leads the CA to believe that the certificate is compromised or is being used for Suspect Code, or (4) the CA otherwise decides that the certificate should be revoked. <b>thawte</b> follows the process for handling revocation requests detailed at section 13.1.5 of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.
4.9.5 Time within Which CA Must Process the Revocation Request	Added: Effective February 1, 2017, <b>thawte</b> complies with the revocation timeframes specified for malware in the Minimum Requirements for Issuance and Management of Publicly-Trusted Code Signing Certificates in section 13.1.5.3 for code signing certificates.
4.9.7 CRL Issuance Frequency (If Applicable)	Added second clause: Expired Certificates are removed from the CRL after the Certificates' expiration with the exception of code signing certificates, effective February 1, 2017 in compliance with the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at <a href="https://aka.ms/csbr">https://aka.ms/csbr</a>
4.9.7.2 Microsoft Requirements for CRL Issuance	Added: Frequency of CRL issuance for code signing and timestamp certificates is documented in the <b>thawte</b> CPS and complies with section 13.2.2 of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at <a href="https://aka.ms/csbr">https://aka.ms/csbr</a> .
4.9.9.2 Microsoft Requirements for OCSP Availability	Added: <b>thawte</b> provides OCSP responses for Code Signing Certificates and Timestamp Certificates for the time period specified in this CPS, which is 10 years after the expiration of the certificate. Revoked certificates remain on the CRL for at least 10 years after the expiration of the certificate.
5.5.2 Retention Period for Archive	Corrected duration: Records associated with Certificates are retained for at least 10 years and six months following the date the Certificate expires or is revoked.
6.1.5.1 CABF Requirements for Key Sizes	Added: * SHA-1 MAY be used with RSA keys in accordance with the criteria defined in Section 7.1.3 of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates  Removed: where applicable. SHA-1 may be used until SHA-256 is supported widely by browsers used by a substantial portion of relying parties worldwide.
7.1 Certificate Profile	Modified text specifying serial number in table 6: Unique value per Issuer DN that contains at least 64 bits of entropy output from a CSPRNG

Section	Changes made
	<p>Modified text specifying Signature Algorithm in table 6:            sha256RSA: Certificate signatures produced using these algorithms shall comply with RFC 3279. Use of sha256WithRSAEncryption shall be used over sha-1WithRSAEncryption except in support of legacy applications and in full compliance of CA/Browser Forum and Application Software Supplier procedures and policies for support of legacy applications with SHA-1</p> <p>Updated references from RFC 2459 to RFC 5280.</p>
7.1.2 Certificate Extensions	<p>Added:            For all web server certificates, the SubjectAltName extension is populated with the authenticated value in the Common Name field of the subject DN (domain name or public iAddress). The SubjectAltName extension may contain additional authenticated domain names or public iAddresses.</p>
7.3 OCSP Profile	<p>Modified to reference RFC 6960:            For EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates, <b>thawte</b> provides OCSP responses compliant with RFC 6960 and as further set forth in the <b>thawte</b> Supplemental Procedures, Appendix B1, Appendix C, and Appendix D, respectively.</p>
Appendix A. Table of Acronyms and Definitions	<p>Added acronym:            CSPRNG: Cryptographically Secure Pseudo-Random Number Generator</p> <p>Added definition:            Cryptographically Secure Pseudo-Random Number Generator: A random number generator intended for use in a cryptographic system.</p>

Section	Section & Changes made
Table 9 – Distinguished Name Attributes in SSL 123 Certificates	<p>Changed the text for the Organization (O) Value:  <a href="#">Registered-Domain-Name Not used</a></p>

**History of changes: version 3.7.15 (effective Mar 2016)**



Section	Section & Changes made
<p>Table 3 – CAs within the <b>76hawte</b> PKI</p>	<p>Changed the CA Description for the following two CAs:</p> <p><b>76hawte</b> Server CA:  <del>Root CA that issues medium assurance domain validated SSL Certificates until June 26, 2010</del>  As of March 2015, this root is excluded from the scope of the WebTrust for Certification Authorities – SSL Baseline Requirements (WebTrust for CA – BR) Audit.</p> <p><b>76hawte</b> Premium Server CA:  <del>High Assurance Root CA that until June 26, 2010 issued:</del></p> <ul style="list-style-type: none"> <li><del>• Server Certificates</del></li> <li><del>• Sub CA Certificates for 76hawte Issuing CAs</del></li> </ul> <p>As of March 2015, this root is excluded from the scope of the WebTrust for Certification Authorities – SSL Baseline Requirements (WebTrust for CA – BR) Audit.</p>
<p>3.2.2.1 Authentication of the Identity of Organizational End-User Subscribers</p>	<p>Added and removed text as indicated below &amp; removed Table 12 “Specific Authentication Procedures”.</p> <p>Where a domain name or e-mail address is included in the certificate <b>76hawte</b> authenticates the Organization’s right to use that domain name. <b>76hawte</b> uses the following methods of vetting a domain name, with option 1 being the primary method:</p> <ol style="list-style-type: none"> <li>1. Confirm the Applicant as the Domain Name Registrant directly with the Domain Name Registrar by performing a whois look up.</li> <li>2. Communicate directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar;</li> <li>3. Rely upon a Domain Authorization Document;</li> <li>4. Communicate directly with the Domain Name Registrant using the contact information listed in the WHOIS record’s “registrant”, “technical”, or “administrative” field;</li> <li>5. Communicate with the Domain’s administrator using an email address created by pre-pending ‘admin’, ‘administrator’, ‘webmaster’, ‘hostmaster’, or ‘postmaster’ in the local part, followed by the at-sign (“@”), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN;</li> <li>6. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN.</li> </ol> <p><del>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.</del></p>
<p>6.1.1 Key Pair Generation</p>	<p>Changed the FIPS level:</p> <p>For <b>thawte</b> Root CAs and Issuing CAs, the cryptographic modules used for key generation meet the requirements of at least FIPS 140-<del>1</del>2 level 23.</p>
<p>6.1.3 Public Key Delivery to Certificate Issuer</p>	<p>Changed text as indicated below.</p> <p>End-user Subscribers submit their public keys to <b>thawte</b> 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 <del>Secure Sockets Layer (SSL)</del> Transport Layer Security (TLS). Currently, TLS 1.0, 1.1, 1.2 are supported on our consoles. SSL v1, v2 and v3 are not supported.</p>
<p>6.2.1 Key Pair Generation</p>	<p>Changed the FIPS level:</p> <p>For <b>thawte</b> CA key pair generation and CA private key storage, <b>thawte</b> uses hardware cryptographic modules that meet the requirements of at least FIPS 140-<del>1</del>2 level 3.</p>

Appendix A – Definitions and Acronyms	Removed definition for Secure Sockets Layer (SSL). Added definition for Transport Layer Security (TLS).
---------------------------------------	--

#### History of changes: version 3.7.14 (effective Sep 2015)

Section	Section & Changes made
Trademark Notices	Removed fax number
1.5.1 Organization Administering the Document	Removed fax number
1.5.2 Contact Person	Removed fax number
5.5.2 Retention Period for Archive	Records associated with Certificates are retained for at least <b>57</b> 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.

#### History of changes: version 3.7.13 (effective Feb 2015)

Section	Section & Changes made
1. Introduction	Added the following text at the end of the section:  All DV and OV certificates issued on or after March 5th, 2015 will include the applicable CABF policy OIDs: <ul style="list-style-type: none"> <li>• CABF OID for DV certificates: 2.23.140.1.2.1</li> <li>• CABF OID for OV certificates: 2.23.140.1.2.2</li> </ul>

#### History of changes: version 3.7.12 (effective Jan 2015)

Description	Section & Changes made
Added language to specifically include Certificate Authority Authorization (CAA)	4.2.4 Certificate Authority Authorization (CAA) As of October 1, 2015, Thawte will check Certificate Authority Authorization (CAA) records as part of its public SSL certificate authentication and verification processes. Prior to this date Thawte may not check CAA records for all public SSL certificate orders. 'Public SSL Certificates' are those that chain up to our publicly available root certificates and which meet CA/Browser Forum Baseline or Extended Validation Requirements.

#### History of changes: version 3.7.11 (effective November 2014)

Section	Section & Changes made
1.3.3 Subscribers	Added footnote that the use of Certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name has been deprecated by the CA / Browser Forum including dates.
Table 10 - Distinguished Name Attributes in SSL123 Certificates for Intranet Use	Removed Table 10
Table 12 – Specific Authentication Procedures	Removed entry for 'SSL 123 for Intranet Certificate'
6.5 Computer Security Controls	Replaced 'thawte's security policy' (legacy document that no longer exists) with 'Symantec Security and Audit Requirements guide'.
6.7 Network Security Controls	Replaced 'thawte's security policy' (legacy document that no longer exists) with 'Symantec Security and Audit Requirements guide'.
Appendix B1	Appendix B1 Replaced text with reference to URL on external website "The current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) Certificates can be accessed at <a href="https://cabforum.org/extended-validation/">https://cabforum.org/extended-validation/</a> "
Appendix C	Appendix C Replaced text with reference to URL on external website "The current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) Code Signing Certificates can be accessed at <a href="https://cabforum.org/ev-code-signing-certificate-guidelines/">https://cabforum.org/ev-code-signing-certificate-guidelines/</a> "

Section	Section & Changes made
Appendix D	Appendix D Replaced text with reference to URL on external website “The current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates can be accessed at <a href="https://cabforum.org/baseline-requirements-documents/">https://cabforum.org/baseline-requirements-documents/</a> ”

#### History of changes: version 3.8.10 (effective November 2013)

Section	Section & Changes made
Section 1 Introduction	Identified conformity to CABF Baseline Requirements
6.1.5 Key sizes	Added clarity regarding subscriber certificates under 2048bit will have EKU without server auth flag and designated OID
7.1 Certificate Profile	Added clarity regarding subscriber certificates under 2048bit will have EKU without server auth flag and designated OID
7.1.2.1 Key Usage	Authorization of certificates 2048bit and less in length to be used within a selected group or closed eco systems
Appendix B1	Updated Extended Validation Guidelines to version 1.4.3
Appendix D	Updated Baseline Requirements to version 1.1.6

#### History of changes: version 3.7.9 (Feb 2013)

Description	Section & Changes made
Addition of new Roots	Section 4.9.7 – added new Roots & Subordinate CAs
Addition of Mozilla IDN Verification requirements	Section 3.2.2.1.2 – Added procedure for verification of IDNs to detect cases of homographic spoofing of IDNs.

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

Description	Section & Changes made
Re-alignment with CABF EV v1.4 Guidelines	<ul style="list-style-type: none"> <li>• Updated Appendix B1 all sections to match re-structured CABF Guidelines.</li> <li>• Updated Appendix C (EV CodeSigning) for cross-references to &amp; from Appendix B1.</li> <li>• Created Appendix D (Baseline for OV &amp; DV Certs) for cross-references to &amp; from Appendix B1.</li> <li>• CPS updated throughout with references to Appx B1, C &amp; D as required for CABF procedures.</li> </ul>

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

Section	Description
6.1.5 Key Sizes	Addition of 2048 DSA CA hierarchies

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

Section	Description
Throughout document	Converted document format from rfc2527 to rfc3647 standard.
All updates reflecting compliance with CABF Requirements for EV Code Signing Certificates, v1.4.	Appendix C.
Routine maintenance	Changed to affirmative language: “ <i>thawte</i> 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,

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

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

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

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

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

Section	Description
Throughout document	Eliminated all practices for issuance of low assurance, Personal Email, FreeMail and Web of Trust certificates.

Throughout document	Reflected the change in ownership from VeriSign to Symantec.
3.1.1 & 7.1	Corrected CA naming from S Africa to US locations
2.4.1 (Governing Law) & 2.4.3 (Dispute Resolution)	Changed from Virginia to California
2.3.3 Assets	Changed from VeriSign to Symantec.

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

Section	Description
Sections 1.1, 1.3.1, 1.3.2, 2.1.2, 2.7, 3.1.8, 4.1.1, 4.4.2.1	Change from Starter PKI (SPKI) to <u>Thawte Certificate Center Enterprise (TCCE)</u> throughout.
Section 1.3.1 and 4.4.9  Thawte Timestamping Root CA now active.	Section 1.3.1: <u>Medium Assurance Root CA that issues:</u> <ul style="list-style-type: none"> <li><u>Sub-CA Certificates for VeriSign Issuing CA.</u></li> <li><u>End entity certificate for GeoTrust time stamping services.</u></li> </ul> Section 4.4.9: <u>Root CA (Non-Issuing) – thawte Time Stamping CA</u>
Section 6.1.5 Key Sizes	Thawte CA key pairs are at least 1024 bit RSA <u>and shall be transitioned to 2048 bit RSA no later than December 31, 2010.</u> <u>thawte</u> recommends that <u>RAs and</u> end-user Subscribers generate <u>10242048</u> bit RSA key pairs. <u>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</u> permits 512 bit RSA key pairs to support certain legacy applications and web servers. <u>Key sizes for thawte EV certificates are identified in Appendix A2.</u>
Section 7.1.1 Certificate Profile	Subject Public Key – Encoded in accordance with RFC 2459 using the RSA algorithm and key lengths <u>of at least 512 bits</u> in accordance with CPS § 6.1.5 <u>(except for SGC SuperCerts which require a key length of at least 1024 bits).</u>
Appendix A2	Updates to key sizes: <ul style="list-style-type: none"> <li>All ECC certificates – 256 &amp; 384 bit</li> </ul>
Section 5.1.1 Site Location	Location of Primary site changed from MV CA to Delaware.
Sections 2.4.1 and 2.4.3.2	Governing Law jurisdiction changed from California to Fairfax County, Virginia.
Appendix A3	Explicitly added SAN to list of extensions for Subscriber certs. <u>SubjectAltName: If present is populated in accordance with RFC5280 and criticality is set to FALSE</u>

#### History of changes: version 3.7.1

Section	Description
Section 7.2	Updated the next update date for “for other Thawte CAs “ from 14 to 28 days
Appendix A1 Section 8	Updated maximum validity period from one year to thirteen months
Appendix A1 Section 22(d)(3)	Created section 22(d)(3)
Appendix A1 Section 25	Deleted: “Before renewing an EV Certificate, thawte performs all authentication and verification tasks required by the Guidelines and this procedure to ensure that the renewal request is properly authorized by the Applicant and that the information displayed in the EV Certificate is still accurate and valid.” Replaced this paragraph with content consistent with published errata to the EV Guidelines. Also included a definition of renewal consistent with the Guidelines.
Appendix A3 Section 3	Added: “(f) extKeyUsage”
Appendix A1-A4 & throughout document	Replaced all references to RFC 3280 with RFC 5280

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

Section	Description
6..3..2	Updated validity period of CA to end user subscriber certificate from 3 to 5 years. Added a footnote to the effect that “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

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

Section	Description
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
Appendix A1 Section 5	Added <u>Non-Commercial Entity Subjects</u>
Appendix A1 Section 6(a)3	Added: Non-Commercial Entities: V1.0, Clause 5.(3)
Appendix A1 Section 14	Added: Government Entities and Non-Commercial Entities
Appendix A1 Section 19	Added Prior Equivalent Authority

Appendix A4 Definitions	Updated Appendix A4 in line with published errata to the EV Guidelines Added: "Country": "Sovereign State": "International Organization": "Parent Company" Updated "Subsidiary Company" to be a majority owned and not a wholly owned company.
----------------------------	--

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

Section	Description
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)

Section	Description
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"
1.3.1-Table 3	Added note to Thawte SSL Domain CA: that, "this CA is no longer in use. Medium assurance domain validated certificates are issued by the thawte Server CA"
3.2.1	Added: "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."
5.1.1	Deleted "thawte's RA operations are conducted within thawte facilities in the United States and in South Africa that are protected by multiple tiers of physical security including proximity badge access." Added "thawte's RA operations are conducted within thawte facilities that are protected by multiple tiers of physical security including proximity badge access."
6.3.2 - table 22	Updated allowable validity period of from 2 to 3 years CA to end-user Subscriber Up to 3 years.
Definitions	Added: "Principal Individual", "Subsidiary Company", "Registration Agency"
Appendix A1-A4	Updated EV procedures in line with Version 1.0 of the EV Guidelines issued by the CA/Browser Forum.

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

Section 1.1	Deleted: " <b>thawte's</b> 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: " <b>thawte's</b> 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)." <b>thawte</b> High Assurance with extended validation Certificates are certificates issued by <b>thawte</b> in conformance with the Guidelines for Extended Validation Certificates published by the a forum consisting of major certification authorities and browser vendors."
Section 1.1. Table 1	Added: new Product, "High Assurance with extended validation secure SSL certificates issued by thawte in conformance with the Guidelines for Extended Validation Certificates. Capable of 256-bit encryption used to support SSL sessions between web browsers and servers."
Section 1.1. Table 1	Added New product: "High Assurance with extended validation Premium Server Gated Cryptography SSL certificates issued by thawte in conformance with the Guidelines for Extended Validation"
Section 1.3.1 Table 3	Added: thawte Primary Root CA Added: thawte Extended Validation SSL CA
Section 1.3.3 table 5	Added "High assurance with extended validation...Incorporated Organizations (including Government agencies, Educational Institutions, Government Departments.). The types of Organizations that qualify for EV Certificates are more fully described in Appendix A1 of this CPS."
Section 1.3.4	Added: "High Assurance with extended validation"
Section 2.2.1.3	Added: "thawte's limitation of liability for EV certificates is further described in Section 37 of Appendix A1 to this CPS"
Section 3.1.1.1	Added:" EV SSL certificate content and profile requirements are discussed in Section 6 of Appendix A3 to this CPS"

Section 3.1.1.7	<b>Added:</b> <i>“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.”</i>
Section 3.1.8.1 - Table 14	<i>“SSL Web Server Certificates with EV... <b>thawte</b>'s procedures for issuing Extended Validation SSL Certificates are described in Appendix A1 to this CPS.”</i>
Section 4.1.1 – Table 19	Added: <i>“High Assurance with extended validation – SSL Web Server Certificates with EV”</i>
Section 4.4.9 – Table 20	Added <i>“thawte Primary Root CA”; “thawte Extended Validation SSL CA”</i>
Section 6.2.2 –	Deleted <i>“Table 21 below shows the threshold number of shares required for the different types of <b>thawte</b> 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</i> Added: <i>“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.”</i>
Section 6.2.7.1.2	<b>Added</b> <i>“and High Assurance with extended validation Certificates”</i>
Section 7.1.1	Added: <i>“SSL Web Server Certificates with EV standard certificate profiles are discussed in Section 6 of Appendix A3 to this CPS.””</i>
Section 7.1.2.7	Added new Section
Section 9	Added Definitions for Extended Validation
APPENDIX A	Added Appendix A1-A3 for Extended Validation Certificate procedures

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

Section 1.1	Deleted: <b>thawte</b> Medium Assurance SSL123 Certificates are issued to Domains to provide confidentiality encryption. <b>thawte</b> 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. <b>thawte</b> Medium Assurance. SSL123 provide confidentiality encryption for internal Intranets. <b>thawte</b> validates that the Server, Intranet name or IP are not publicly accessible via the World Wide Web. Added: <b>thawte</b> Medium Assurance SSL123 Certificates are issued to Domains to provide confidentiality encryption. <b>thawte</b> 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 <b>thawte</b> '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 <b>thawte</b> 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 <b>thawte</b> SSL123 Certificate provides validation of a registered domain and <b>thawte</b> 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: <b>thawte</b> 's Reseller Partner Program permits entities acting as a host (“Web Host”) to the web sites of their clients to manage lifecycle processes for server and code signing Certificates on behalf of their clients. The ISP Program offers Resellers (e.g. Web Hosting companies, ISPs, Registrars) the ability to enroll for SSL Web Server, SSL Wildcard, SSL123, SGC SuperCerts and Code Signing Certificates on behalf of their customers . Although the Reseller assists with the enrollment process (See CPS § 4.1.1), the Reseller does not perform validation functions, but instead <b>thawte</b> 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.

	<p>Added: <b>thawte's</b> Reseller Partner Program offers Resellers (e.g. Web Hosting companies, ISPs, Registrars) the ability to enroll for SSL Web Server, SSL Wildcard, SSL123, SGC SuperCerts and Code Signing Certificates on behalf of their customers . Although the Reseller assists with the enrollment process (See CPS § 4.1.1), the Reseller does not perform validation functions, but instead <b>thawte</b> 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.</p>
Section 1.1	<p>Deleted: <b>thawte</b> performs the RA function for all high assurance certificates, and for low assurance "Freemail" certificates, which do not include the subscriber's name.</p> <p>Added: <b>thawte</b> 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.</p>
Section 1.3.4.	<p>Deleted: This CPS applies to all <b>thawte</b> PKI Participants, including <b>thawte</b>, Customers, Resellers, Subscribers, and Relying Parties. This CPS describes the practices governing the use of High Assurance, and Low Assurance Certificates within the <b>thawte</b> 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).</p> <p>Added: This CPS applies to all <b>thawte</b> PKI Participants, including <b>thawte</b>, 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 <b>thawte</b> 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).</p>
Section 2.3.3	<p>Deleted: <b>thawte</b>, Inc. is a wholly owned subsidiary of VeriSign, Inc. VeriSign's financial resources are set forth in disclosures appearing at: <a href="http://corporate.verisign.com/investor/sec-filings.html">http://corporate.verisign.com/investor/sec-filings.html</a>. 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.</p> <p>Added: <b>thawte</b>, Inc. is a wholly owned subsidiary of VeriSign, Inc. VeriSign's financial resources are set forth in disclosures appearing at: <a href="http://www.verisign.com/verisign-inc/vrsn-investors/sec-filings/index.html">http://www.verisign.com/verisign-inc/vrsn-investors/sec-filings/index.html</a>. 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.</p>
Section 2.5.6	<p>Deleted: A Subscriber may make changes to the name included in a certificate within 30 days of issue. <b>thawte</b> authenticates the new domain in terms of Section 3.1.8.1.</p> <p>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. <b>thawte</b> authenticates the new domain in terms of Section 3.1.8.1.</p>
Section 3.1.1.2	<p>Deleted: Server Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in Table 8 below.</p> <p>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.</p>
Section 3.1.8.1	<p>Deleted: Organization authentication is not for SSL123. Specified that confirmation with an appropriate Organizational contact is not done for SSL123 Certificates</p> <p>Added: Organization authentication is not performed for SSL123 Certificates. These certificates are authenticated as described in Table 14 below.</p> <p>Where a domain name or e-mail address is included in the certificate <b>thawte</b> 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.</p>
Section 3.1.9.2.3	<p>Added: US Notary public (limited to Notary Publics in States where the licensing status information is provided online by the appropriate licensing authority)</p>
Section: 3.2.1	<p>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.</p> <p>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.</p>
Section 3.4:	<p>Deleted: Prior to the revocation of a Certificate, <b>thawte</b> verifies that the revocation has been requested by the Certificate's Subscriber or the entity that approved the Certificate Application. The subscriber must contact <b>thawte</b> 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.</p> <p>Added: Prior to the revocation of a Certificate, <b>thawte</b> 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:</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked,</li> <li>• 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</li> <li>• However, only the Authorizing Contact can sign a revocation form for SSL123 Certificates.</li> </ul>

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: <a href="http://crl.thawte.com/ThawteServerCA.crl">http://crl.thawte.com/ThawteServerCA.crl</a> Added: <a href="http://crl.thawte.com/ThawtePremiumServerCA.crl">http://crl.thawte.com/ThawtePremiumServerCA.crl</a>																	
Section 7.1.2.5.	Deleted: <a href="http://crl.thawte.com/ThawteServerCA.crl">http://crl.thawte.com/ThawteServerCA.crl</a> Added: <a href="http://crl.thawte.com/ThawteSGCCA.crl">http://crl.thawte.com/ThawteSGCCA.crl</a>																	
	Authority information Access	<a href="http://ocsp.thawte.com">http://ocsp.thawte.com</a>	Non-Critical															
Section 7.1.2.6	<p><b>Added: SSL Wildcard Certificates</b>  <b>thawte</b> SSL Wildcard Certificates include the extensions specified in Table 26 below:</p> <table border="1"> <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>CRL Distribution Points</td> <td><a href="http://crl.thawte.com/ThawtePremiumServerCA.crl">http://crl.thawte.com/ThawtePremiumServerCA.crl</a></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> <p><b>Table 26 –thawte SSL Web Server Certificate Extensions</b></p>			Extension	Value or Value Constraint	Criticality	Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Critical	Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	Non-Critical	CRL Distribution Points	<a href="http://crl.thawte.com/ThawtePremiumServerCA.crl">http://crl.thawte.com/ThawtePremiumServerCA.crl</a>	Non-Critical	Authority information Access	<a href="http://ocsp.thawte.com">http://ocsp.thawte.com</a>	Non-Critical
Extension	Value or Value Constraint	Criticality																
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Critical																
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	Non-Critical																
CRL Distribution Points	<a href="http://crl.thawte.com/ThawtePremiumServerCA.crl">http://crl.thawte.com/ThawtePremiumServerCA.crl</a>	Non-Critical																
Authority information Access	<a href="http://ocsp.thawte.com">http://ocsp.thawte.com</a>	Non-Critical																
Section: 7.1.3	Deleted: <b>thawte</b> Certificates are signed with md5RSA. Added: <b>thawte</b> 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: 7.2	Deleted: Algorithm used to sign the CRL. Thawte CRLs are signed using md5RSA (OID: 1.2.840.113549.1.1.4) in accordance with RFC 2459. Added: Algorithm used to sign the CRL. Thawte CRLs are signed using md5RSA or sha1RSA (OID: 1.2.840.113549.1.1.4) in accordance with RFC 2459.																	
Section 9.2.	<p>Deleted:</p> <table border="1"> <tr> <td><b>SGC SuperCerts</b></td> <td>High Assurance Certificate used to support SSL sessions between web browsers and web servers that are encrypted using strong cryptographic protection consistent with applicable export laws.</td> </tr> </table> <p>Added:</p> <table border="1"> <tr> <td><b>SGC SuperCerts</b></td> <td>High Assurance Premium Server Gated Cryptography SSL certificates with stringent 3 step authentication, automatic 128-bit step-up encryption and capable of 256-bit encryption * used to support SSL sessions between web browsers and web servers. * With browsers IE 4.X or Netscape 4.06 and later</td> </tr> </table>			<b>SGC SuperCerts</b>	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.	<b>SGC SuperCerts</b>	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											
<b>SGC SuperCerts</b>	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.																	
<b>SGC SuperCerts</b>	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																	
Section 9.2.	<p>Deleted:</p> <table border="1"> <tr> <td><b>SSL Web Server Certificates</b></td> <td>An organizational Certificate used to support SSL sessions between web browsers and servers.</td> </tr> </table> <p>Added:</p> <table border="1"> <tr> <td><b>SSL Web Server Certificates</b></td> <td>High Assurance secure SSL certificates with stringent 3 step authentication capable of 256-bit encryption used to support SSL sessions between web browsers and servers.</td> </tr> </table>			<b>SSL Web Server Certificates</b>	An organizational Certificate used to support SSL sessions between web browsers and servers.	<b>SSL Web Server Certificates</b>	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.											
<b>SSL Web Server Certificates</b>	An organizational Certificate used to support SSL sessions between web browsers and servers.																	
<b>SSL Web Server Certificates</b>	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 9.2.	<p>Deleted:</p> <table border="1"> <tr> <td><b>High Assurance</b></td> <td>Certificates issued to organizations and sole proprietors to provide authentication; message, software, and content integrity; and confidentiality encryption.</td> </tr> </table> <p>Added:</p> <table border="1"> <tr> <td><b>High Assurance</b></td> <td>Certificates issued to organizations and sole proprietors to provide stringent 3 step authentication; message, software, and content integrity; and confidentiality encryption.</td> </tr> </table>			<b>High Assurance</b>	Certificates issued to organizations and sole proprietors to provide authentication; message, software, and content integrity; and confidentiality encryption.	<b>High Assurance</b>	Certificates issued to organizations and sole proprietors to provide stringent 3 step authentication; message, software, and content integrity; and confidentiality encryption.											
<b>High Assurance</b>	Certificates issued to organizations and sole proprietors to provide authentication; message, software, and content integrity; and confidentiality encryption.																	
<b>High Assurance</b>	Certificates issued to organizations and sole proprietors to provide stringent 3 step authentication; message, software, and content integrity; and confidentiality encryption.																	
Section 9.2.	<p>Deleted:</p> <table border="1"> <tr> <td><b>Reseller Partner Program</b></td> <td>A program that allows to enroll for SSL Web Server Certificates, and SGC SuperCerts on behalf of end-user Subscribers who are customers of the Web Host.</td> </tr> </table> <p>Added:</p> <table border="1"> <tr> <td><b>ISP Partner Program</b></td> <td>A program that allows Web Hosts to enroll for SSL Web Server Certificates, SSL Wildcard Certificates, SSL123 Certificates and SGC SuperCerts on behalf of end-user Subscribers who are customers of the Reseller.</td> </tr> </table>			<b>Reseller Partner Program</b>	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.	<b>ISP Partner Program</b>	A program that allows Web Hosts to enroll for SSL Web Server Certificates, SSL Wildcard Certificates, SSL123 Certificates and SGC SuperCerts on behalf of end-user Subscribers who are customers of the Reseller.											
<b>Reseller Partner Program</b>	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.																	
<b>ISP Partner Program</b>	A program that allows Web Hosts to enroll for SSL Web Server Certificates, SSL Wildcard Certificates, SSL123 Certificates and SGC SuperCerts on behalf of end-user Subscribers who are customers of the Reseller.																	
Section 9.2.	Added:																	



	<b>Code Signing Certificates</b>	Certificates which secure delivery of code and content to browsers over the Internet.
Section 9.2.	Added: <b>Medium Assurance</b>	Certificates that are issued to Domains to provide confidentiality encryption. <b>thawte</b> 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 9.2.	Added: <b>SSL123 Certificates</b>	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.
Section 9.2.	Added: <b>Wildcard Certificates</b>	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.