DigiCert

Certification Practices Statement for *Thawte*-Branded Certificates

Version 3.7.23

June 25, 2019

DigiCert, Inc.
2801 N. Thanksgiving Way
Suite 500
Lehi, UT 84043
USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481
www.digicert.com

DigiCert Certification Practices Statement for *Thawte*-branded Certificates

Printed in the United States of America.

Revision date: June 25, 2019

Trademark Notices

TABLE OF CONTENTS

Change History Table

Version	Description of Changes
1.0	Original Draft.
2.3	Various editorial changes throughout the document. Added SSL Wildcard Certificates.Removed SGC SuperCerts. Deleted references to the Reseller Partner Program and replaced it with references to the ISP Partner Program. Added Code Signing Certificates, Medium Assurance Certificates, SSL123 Certificates, and Wildcard Certificates in section 9.2.
3.3	Various editorial changes throughout the document. Added High assurance with extended validation Premium Server Gated Cryptography SSL Certificates. Added the Thawte Primary Root CA, and Thawte Extended Validation SSL CA. Added SSL Web Server Certificates with EV. Added Appendix A1-A3 for Extended Validation Certificate procedures.
3.4	Various editorial changes throughout the document. Updated allowable validity period of from 2 to 3 years CA to end-user Subscriber Up to 3 years. Updated EV procedures in line with Version 1.0 of the EV Guidelines issued by the CA/Browser Forum.
3.5	Updated the profile information for the EV VeriSign Class 3 Primary CA to include the extendedKeyUsage field.
3.6	Various editorial changes throughout the document. Several CAs added including; Thawte Primary Root CA –G2, Thawte Primary Root CA – G3, Thawte Primary Root CA –G2, and Thawte Primary Root CA – G3. Updated to allow for verification of address of a or a Parent/Subsidiary Company. Updated Appendix A4 in line with published errata to the EV Guidelines. Added terms “Country”, “Sovereign State”, “Interational Organization”, and “Parent Company.” Updated “Subsidiary Company” to be a majority owned and not a wholly owned company.
3.7	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.
3.7.1	Updated the next update date for “for other Thawte CAs“ from 14 to 28 days. Updated maximum validity period from one year to thirteen months. Replaced all references to RFC 3280 with RFC 5280. Updates profiles and other sections within the Appendix A1 and A3.
3.7.2	Various editorial changes throughout the document. Key sizes updated to 2048 bit RSA from 1024 bit RSA. Change from Starter PKI (SPKI) to Thawte Certificate Center Enterprise (TCCE) throughout. Updates to key sizes: All ECC certificates – 256 & 384 bit. Location of Primary site changed from MV CA to Delaware. Governing Law jurisdiction changed from California to Fairfax County, Virginia. Explicitly added SAN to list of extensions for Subscriber certs. SubjectAltName: If present is populated in accordance with RFC5280 and criticality is set to FALSE.
3.7.3	Various editorial changes throughout the document. Eliminated all practices for issuance of low assurance, Personal Email, FreeMail and Web of Trust certificates. Reflected the change in ownership from VeriSign to Symantec. Corrected CA naming from S Africa to US locations. Changed from Virginia to California. Changed from VeriSign to Symantec.
3.7.4	Various editorial changes throughout the document. Throughout the document changed email address specified from VeriSign to Symantec. *Thawte* CA key pairs are at least 2048 bit RSA.
3.7.5	Identified Thawte non-EV OIDs. All updates reflecting compliance with CABF Requirements for DV and OV certificates, Effective July 1, 2012. (See PWG Approval Mapping Matrix for Thawte CPS).
3.7.6	Various editorial changes throughout the document. Throughout Converted document format from rfc2527 to rfc3647 standard. All updates completed to reflect compliance with CABF Requirements for EV Code Signing Certificates, v1.4.
3.7.7	Addition of 2048 DSA CA hierarchies.
3.7.8	Re-alignment with CABF EV v1.4 Guidelines including. Updating Appendix B1, C, D, and other updates throughout the CPS.
3.7.9	Added new Roots & Subordinate CAs and added procedure for verification of IDNs to detect cases of homographic spoofing of IDNs.
3.7.10	Identified conformity to CABF Baseline Requirements in the introduction. Added clarity regarding subscriber certificates under 2048bit will have EKU without server auth flag and designated OID. Added clarity regarding subscriber certificates under 2048bit will have EKU without server auth flag and designated OID. Authorization of certificates 2048bit and less in length to be used within a selected group or closed eco systems. Updated Extended Validation Guidelines to version 1.4.3. Updated Baseline Requirements to version 1.1.6.
3.7.11	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. Replaced ‘Thawte’s security policy’ (legacy document that no longer exists) with ‘Symantec Security and Audit Requirements guide’ throughout the document.
3.7.12	Added language to specifically include Certificate Authority Authorization (CA).
3.7.13	Added the CABF policy OIDs for DV and OV Certificate offerings.
3.7.14	Removed the fax number throughout the document. Updated the retention period for Certificate records from five to seven years.
3.7.15	Changed the CA descriptions for the Thawte Server CA and Thawte Premium Server CA. Added and removed text from Table 12 in order to remove it and create more clarity around vetting a domain name. Changed the FIPS level in the text from 140-1 and 2 to 140-2 and 3. Updated Public Key Delivery to

	Certificate Issuer in order to support TLS 1.0, 1.1, and 1.2 instead of SSL v1, v2, and v3. Removed definition for Secure Sockets Layer (SSL). Added definition for Transport Layer Security (TLS).
3.7.16	Various editorial changes throughout the document. Updated references from RFC 2459 to RFC 5280. Added acronym: CSPRNG: Cryptographically Secure Pseudo-Random Number Generator. Added definition: Cryptographically Secure Pseudo-Random Number Generator: A random number generator intended for use in a cryptographic system.
3.7.17	Various editorial changes throughout the document. Revised section 3.2.3 from "No Stipulation" to include CABF compliance language. Removed the Microsoft Code Signing OID from Enhanced Key Usage.
3.7.18	Various editorial changes throughout the document. Added CABF policy OIDS for EV Certificates (SSL/TLS and Code Signing). Removed statement that Thawte Server CA directly issues end user subscriber certificates. Added: Thawte does not delegate domain or IP address validation to external Ras or third parties. Removed aged reference to internal server name and reserved IP address deprecation. Table 8, added to common name: For internationalized domain names, the Common Name will be represented as a Unicode encoded U-label value designed for human comprehension and that Common Name will be represented in the Subject Alternative Name extension as a puny-coded A-label value designed for automated comprehension. These different encodings of the same name are treated as equal values for the purposes of Common Name to Subject Alternative Name duplication requirements. Added to State or Province: State will appear in any certificates in the scope of the CA/Browser Forum Baseline Requirements in cases where no meaningful value for locality exists for the subject. Table 9, added to common name: For internationalized domain names, the Common Name will be represented as a Unicode encoded U-label value designed for human comprehension and that Common Name will be represented in the Subject Alternative Name extension as a puny-coded A-label value designed for automated comprehension. These different encodings of the same name are treated as equal values for the purposes of Common Name to Subject Alternative Name duplication requirements. Removed list of six domain validation methods, added ten revised methods. Added CABF requirements to section 4.2.4 regarding ICANN, CAA records, CT log server checks, and recognizing any and all of the following Issuer Domain Names as permission to issue: symantec.com, Thawte.com, geotrust.com, rapidssl.com, and any FQDN terminating in the base domain name digitalcertvalidation.com. Appended data reuse qualification. Added 24 hour investigation requirement for CABF for revocation requests and Certificate Problem Reports. Added technical support exclusion: customer service personnel, with the exception of technical support analysts. Added CAA checking results. Added that SHA-1 may be used to support legacy applications and use cases other than SSL and EV Code Signing provided that such usage does not violate procedures and policies set forth by the CA/Browser Forum and related Application Software Suppliers. Added reference to Mozilla Root Policy. Added details about how Subscribers generate and protect the private key for Code Signing Certificates. Updated references to RFC 5280 and x.509. Added to the OCSP profile that responders conform to RFC 2560, RFC 5019, and RFC 6960, excluding client requested cipher support. Added detail of audit schemes that are accepted include WebTrust specific audits for CABF. Updated definition for Applicant and added the following terms: Authorization Domain Name, Authorized Port, Base Domain Name, Domain Contact, Random Value, Request Token and Test Certificate.
3.7.19	Various editorial changes throughout the document. DigiCert replaced in key references to replace Symantec.
3.7.20	Changes made throughout the document to meet the updates on the DigiCert CP/CPS v.4.16 changes including: Added sections 1.5.2.1 for Revocation Reporting Contact Person and additions/revisions to section 4.9 to meet the revocation requirements for CABF ballot SC6.
3.7.21	Minor editorial fix to some instances of "DigiCert" to match the style of the document. Added wording to sections 1.3.3 and 3.2.2 to address the CABF SC7 ballot for IP address validation to redirect to the DigiCert CP and CPS. Minor editorial changes throughout the document to correct grammar mistakes. Modification to section 4.10.2 to state an accurate SLA expectation. Modified section 5.1.1 to redirect to the DigiCert CP and CPS for updates to physical security. Revised instances of "Issuer CA" to "Issuing CA" to align with the defined term.
3.2.22	Edited sections 3.1.6, 3.2.1, and 6.1.3 to clarify naming and proof-of-possession practices.
3.2.23	Edited section 6.3.2 entries for PCA and ICAs to align with the DigiCert CP/CPS. Modified section 5.3.1 to specify background checks are repeated every five years.

1. INTRODUCTION

A Certification Practices Statement ("CPS") is defined by the Information Security Committee of the American Bar Association as "a statement of the practices which a certification authority employs in issuing certificates." This DigiCert CPS for Thawte 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 Certification Practices Statement. The ***Thawte*** PKI operates as a single, independent PKI with a single CPS. This document should not be considered subordinate to other DigiCert Certificate Policies or Certification Practices Statements.

Thawte PKI certificates under this Certification Practices Statement for ***Thawte*** are identified by the following object identifier (OID) values:

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

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

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

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

At this time, ***Thawte*** 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.

Thawte Root CAs shall not issue SSL inspection intermediate CAs. 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.

Prior to the acquisition of the Website Security business unit by DigiCert, Symantec 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 acquired by DigiCert from Symantec 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 5th, 2015 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 include the applicable CABF policy OID.

EV certificates use the applicable CABF policy OIDs:

- SSL/TLS certificates: 2.23.140.1.1
- Code Signing certificates: 2.23.140.1.3

Effective February 1, 2017 and after, ***DigiCert*** 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 1st, 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 - https://aka.ms/csbr.

1.1 Overview

Thawte 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 ***DigiCert*** 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. ***DigiCert*** 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, ***DigiCert*** 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 ***DigiCert*** 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

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

Program	Purpose and Benefit	Program Description
Thawte Certificate Center Enterprise (TCCE) Program	The ***Thawte*** Certificate Center Enterprise (TCCE 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, ***DigiCert*** 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.	***DigiCert***'s Reseller Partner Program offers Resellers (e.g. Web Hosting companies, ISPs, Registrars) the ability to enroll for SSL Web Server, SSL Wildcard, SSL123, SGC SuperCerts and Code Signing Certificates on behalf of their customers. Although the Reseller assists with the enrollment process (*See* CPS § 4.1.2), the Reseller does not perform validation functions, but instead ***DigiCert*** 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
t-refer Program	This program allows companies to refer customers to ***DigiCert***. Once a certificate is issued to the customer, the referrer is paid a referral fee. SSL Web Server, SSL123, SGC SuperCerts and Code Signing Certificates are sold through this channel.	**t-refer** allows entities to install a link on their website: via this link their customers can buy ***Thawte*** certificates. The referrer is not necessarily affiliated to the customer and will not need to be involved in the enrollment process with the customer. The channel is used to allow referrals to ***DigiCert*** 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 DigiCert Certification Practice Statement for ***Thawte*** and it expresses the ***Thawte*** 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 ***DigiCert*** 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. ***DigiCert*** 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 ***DigiCert*** which apply to ***Thawte*** PKI Participants. These agreements bind Customers, Subscribers, and Relying Parties of ***DigiCert***. Among other things, the agreements flow down ***DigiCert*** requirements to these ***Thawte*** PKI Participants and, in some cases, state specific practices for how they must meet ***DigiCert*** 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. ***DigiCert*** currently operates the following Certification Authorities within the ***Thawte*** PKI:

Thawte Root CA	CA Description	Registration Authorities
Thawte 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.	• ***DigiCert*** • ***Thawte*** TCCE Customers
Thawte Primary Root CA	High Assurance offline Root CA that issues: • Sub-CA Certificates for ***Thawte*** Issuing CAs for Extended Validation, organization validated, domain validated and Code Signing certificates	***DigiCert***
Symantec Class 3 Public Primary CA	High Assurance Root CA that issues: • Sub-CA Certificates for ***Thawte*** Issuing CAs for ***Thawte*** SGC SuperCert Certificates	***DigiCert***
Thawte Premium 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.	***DigiCert***
Thawte Time Stamping CA	Medium Assurance Root CA that issues: • Sub-CA Certificates for Symantec Issuing CA. • End entity certificate for GeoTrust time stamping services.	***DigiCert***
Thawte Primary Root CA – G2	Currently inactive	***DigiCert***
Thawte Primary Root CA – G3	Currently inactive	***DigiCert***
Thawte Primary Root CA – G4	Root CA issuing Sub CA Certificates for ***Thawte*** Issuing CAs which issue EV and Organization Validated (OV) end entity certificates.	***DigiCert***

Table 3 – CAs within the *Thawte* PKI

The ***Thawte*** Root CAs issue certificates only to subordinate CAs.

Note: Refer to the ***Thawte*** Repository at *https://www.Thawte.com/roots* for updates to the current listing of ***Thawte*** CAs.

1.3.2 Registration Authorities

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

Registration Authority	Role
DigiCert	***DigiCert*** 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

DigiCert does not delegate domain or IP address validation to external RAs or third parties.

1.3.3 Subscribers

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

Class	Issued to	Types of Subscribers
Medium Assurance	Registered Domains	Any person who has control of a domain referring to a device including, but not limited to: • Web servers, mail servers and web traffic management devices • Intranet device utilizing IP addresses 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 was eliminated by October 2016. Any reference to IP address inclusion in Certificates are for legacy purposes or exceptional circumstances that are validated and controlled by DigiCert as per the DigiCert CPS section 3.2.2.
High Assurance	Organizations	Organizations (including agencies, Educational Institutions, Government Departments, etc.) that control a device including, but not limited to: • Web servers, mail servers and web traffic management devices • Devices digitally signing code or other content.
	Sole Proprietors	Small Office Home Office ("SOHO") clients that are typically individuals who run a sole proprietor online or development business.
High Assurance with extended validation	Organizations	Incorporated Organizations (including government agencies, Educational Institutions, Government Departments, etc.) The types of Organizations that qualify for EV Certificates are more fully described in Appendix 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 ***DigiCert***, 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. ***DigiCert*** 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 cAFlag setting to false in the 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 ***DigiCert***.

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.

DigiCert 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.

DigiCert 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. ***DigiCert*** 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

This CPS and the documents referenced herein are maintained by the DigiCert Policy Authority (DCPA), which can be contacted at:

DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
Tel: 1-801-701-9600

Fax: 1-801-705-0481
www.digicert.com
support@digicert.com

1.5.2 Contact Person

Attn: Legal Counsel
DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
www.digicert.com
support@digicert.com

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

1.5.2.1 Revocation Reporting Contact Person

Attn: Support
DigiCert Technical Support
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
https://www.digicert.com/certificate-revocation.htm

To request that a Certificate be revoked, please email revoke@digicert.com.

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. DigiCert or an RA will authenticate and log each revocation request according to Section 4.9 of the DigiCert CP and this CPS. DigiCert will always revoke a Certificate if the request is authenticated as originating from the Subscriber or the Affiliated Organization listed in the Certificate. If revocation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, DigiCert or an RA will investigate the alleged basis for the revocation request prior to taking action in accordance with Section 4.9.1 and 4.9.3.

1.5.3 Person Determining CPS Suitability for the Policy

The DigiCert Policy Authority (DCPA) 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.

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

DigiCert is responsible for the repository function for the ***Thawte*** CAs. ***DigiCert*** publishes this CPS, Subscriber Agreements, and Relying Party Agreements at *https://www.websecurity.symantec.com/legal/repository#PoliciesAndAgreements* or in the repository section of the ***Thawte*** website at *https://www.Thawte.com/repository*.

DigiCert publishes Certificates in accordance with Table 6 below.

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

Table 6 – Certificate Publication Requirements

DigiCert 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 *https://www.websecurity.symantec.com/legal/repository#PoliciesAndAgreements* or https://*www.Thawte.com/repository*. The CPS is available in the ***Thawte*** Repository in Adobe Acrobat portable document format.
rAmendments 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.

DigiCert 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.

CA information is published promptly after it is made available to the CA. ***DigiCert*** offers CRLs showing the revocation of ***Thawte*** Certificates and offers status checking services through the ***Thawte***Repository and Affiliates' repositories. CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CAs that only issue CA Certificates are issued at least annually, and also whenever a CA Certificate is revoked. If a Certificate listed in a CRL expires, it may be removed from later issued CRLs after the Certificate's expiration.

2.4 Access Controls on Repositories

Information published in repositories ***DigiCert*** is publicly accessible information. Read only access to such information is unrestricted. ***DigiCert*** requires persons to agree to a Relying Party Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. ***DigiCert*** has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries. ***DigiCert*** makes its repositories publicly available in a read-only manner at the link(s) 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 ***Thawte*** 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 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. For internationalized domain names, the Common Name will be represented as a Unicode encoded U-label value designed for human comprehension and that Common Name will be represented in the Subject Alternative Name extension as a puny-coded A-label value designed for automated comprehension. These different encodings of the same name are treated as equal values for the purposes of Common Name to Subject Alternative Name duplication requirements.
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. State will appear in any certificates in the scope of the CA/Browser Forum Baseline Requirements in cases where no meaningful value for locality exists for the subject.
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 –SSL123

3.1.1.3.1 Certificate subject details – SSL123Certificates

Attribute	Value
Common Name (CN)	Registered domain name. For internationalized domain names, the Common Name will be represented as a Unicode encoded U-label value designed for human comprehension and that Common Name will be represented in the Subject Alternative Name extension as a puny-coded A-label value designed for automated comprehension. These different encodings of the same name are treated as equal values for the purposes of Common Name to Subject Alternative Name duplication requirements.
Organizational Unit (OU)	"Domain Validated"
Organizational Unit (OU)	Go to *https://www.Thawte.com/repository/index.html*
Organizational Unit (OU)	***Thawte*** SSL123 Certificate
Organization (O)	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.

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, ***DigiCert*** 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. For EV SSL Certificates, DigiCert implements a process that prevents EV Certificates from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless DigiCert has verified this information in accordance with the EV Guidelines and section 3.2 of the DigiCert CP and CPS. For all other Certificate types, ***DigiCert*** does notverify 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. ***DigiCert*** 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

DigiCert may verify 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 ***DigiCert***-approved method.

3.2.2 Authentication of Organization Identity

DigiCert 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 DigiCert CPS section 3.2.2 and generally described in the subsections below. 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

DigiCert 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 ***DigiCert*** authenticates the Organization's right to use that domain name based on the methods documented in the DigiCert CPS Section 3.2.2.

With respect to ***Thawte*** Certificate Center Enterprise (TCCE) Customers, the identity confirmation process begins with ***DigiCert***'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 an 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 listed in the DigiCert CPS section 3.2.2.

3.2.2.1.2 Mozilla Verification Requirements for Organization Applicants

For requests for internationalized domain names (IDNs) in Certificates, ***DigiCert*** performs domain name owner verification to detect cases of homographic spoofing of IDNs.

DigiCert 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, ***DigiCert*** 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, ***DigiCert*** 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, ***DigiCert*** 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.

DigiCert Administrators are entitled to request the revocation of end-user Subscriber Certificates. ***DigiCert*** 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 ***DigiCert*** in accordance with CPS § 6.1.3,
- demonstrating to ***DigiCert*** pursuant to CPS § 3.2.1 that the Certificate Applicant has possession of the private key corresponding to the public key delivered to ***DigiCert***, and
- manifesting assent to the relevant Subscriber Agreement.

Certificate Applications are submitted either to ***DigiCert*** 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	***DigiCert***	***DigiCert***
High Assurance – SSL Web Server Certificates and Code Signing	• ***DigiCert*** • TCCE Customers	***DigiCert***
Medium Assurance – SSL123 Certificates	***DigiCert***	***DigiCert***

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 ***DigiCert*** 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*.

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, ***DigiCert*** (*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.

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, ***DigiCert*** approves the Certificate Application and issues a Certificate based on the information in the Certificate Application. If authentication is unsuccessful, ***DigiCert*** 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, DigiCert will check Certificate Authority Authorization (CAA) records as part of its public SSL certificate authentication and verification processes. Prior to this date DigiCert 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.

As of September 8, 2017, CAA issue and issuewild records are checked either within 8 hours of issuance or the CAA record's Time to Live (TTL), whichever is greater, except where CAA was similarly checked prior to the creation of a Certificate Transparency pre-certificate that was logged in at least 2 public CT log servers. CAA checking may be omitted for technically-constrained subordinate CAs.

DNS access failure is treated as permission to issue when the failure is proven to be outside ***DigiCert*** infrastructure, was retried at least once, and the domain zone does not have a DNSSEC validation chain to the ICANN root.

DigiCert logs actions taken based on CAA records, and documents issuance prevented by CAA for feedback to the CA/Browser Forum.

DigiCert recognizes any and all of the following Issuer Domain Names as permission to issue: digicert.com, symantec.com, Thawte.com, geotrust.com, rapidssl.com, and any FQDN terminating in the base domain name digitalcertvalidation.com.

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. 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, ***DigiCert*** 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 ***DigiCert*** 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 ***DigiCert***'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. ***DigiCert*** 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) ***DigiCert*** permits Subscribers to request a new certificate for an existing key pair (technically defined as "renewal"). Table 15 below describes ***DigiCert***'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 ***DigiCert***'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. ***DigiCert*** will sign the previous CSR for the new validity period, where the server's key management functionality allows the installation of a new certificate for an existing key pair. Accordingly, for Server Certificates, both rekey and renewal are supported.
CA Certificates	Renewal of CA Certificates is permitted as long as the cumulative certified lifetime of the CA key pair does not exceed the applicable maximum CA key pair lifetime specified in CPS § 6.3.2. ***Thawte*** CAs may also be rekeyed in accordance with CPS § 5.6. Accordingly, for ***Thawte*** 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.

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, ***DigiCert*** may rekey, or renew the certificate. As an alternative to using a password, ***DigiCert*** 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, ***DigiCert*** will issue the Certificate if the enrollment information (including Corporate and Technical contact information) has not changed, provided that the initial validation data has not exceeded the CA/Browser Forum guideline limits for data reuse.

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

DigiCert will revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that DigiCert revoke the Certificate;
2. The Subscriber notifies DigiCert that the original Certificate request was not authorized and does not retroactively grant authorization;
3. DigiCert obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
4. DigiCert obtains evidence that the validation of domain authorization or control for any FDQN or IP address in the Certificate should not be relied upon.

DigiCert may revoke a certificate within 24 hours and will revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/B Forum Baseline Requirements;
2. DigiCert obtains evidence that the Certificate was misused;
3. The Subscriber or the cross-certified CA breached a material obligation under the CP, this CPS, or the relevant agreement;
4. DigiCert confirms any circumstance indicating that use of a FQDN or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name registrant and the Applicant has terminated, or the Domain Name registrant has failed to renew the Domain Name);
5. DigiCert confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
6. DigiCert confirms a material change in the information contained in the Certificate;
7. DigiCert confirms that the Certificate was not issued in accordance with the CA/B Forum requirements or the DigiCert CP, DigiCert CPS, or this CPS;
8. DigiCert determines or confirms that any of the information appearing in the Certificate is inaccurate;

9. DigiCert's right to issue Certificates under the CA/B Forum requirements expires or is revoked or terminated, unless DigiCert has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by the DigiCert CP, DigiCert CPS, or this CPS; or
11. DigiCert confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

DigiCert will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies DigiCert that the original Certificate request was not authorized and does not retroactively grant authorization;
3. DigiCert obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a key compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/B Forum Baseline Requirements;
4. DigiCert obtains evidence that the CA Certificate was misused;
5. DigiCert confirms that the CA Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. DigiCert determines that any of the information appearing in the CA Certificate is inaccurate or misleading;
7. DigiCert or the Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;
8. DigiCert's or the Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless DigiCert has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by DigiCert's Certificate Policy and/or Certification Practice Statement; or
10. The technical content or format of the CA Certificate presents an unacceptable risk to application software suppliers or Relying Parties.

An end-user Subscriber Certificate is revoked if:

- 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,
- 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 ***DigiCert*** indicating that the certificate was used to sign malware, 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, ***DigiCert*** 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, ***DigiCert*** 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 ***DigiCert*** of a known or suspected compromise of its private key in accordance with the procedures in CPS § 4.9.3.

DigiCert will revoke a CA Certificate if:

- ***DigiCert*** discovers or has reason to believe that there has been a compromise of the CA private key,
- ***DigiCert*** 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,
- ***DigiCert*** determines that a material prerequisite to Certificate issuance was neither satisfied nor waived, or
- Authorized ***DigiCert*** personnel request revocation of the Certificate.

DigiCert always revokes a Certificate if the binding between the subject and the subject's Public Key in the certificate is no longer valid or if an associated Private Key is compromised.

Subscribers shall state the reason(s) for requesting revocation upon submitting the request.

DigiCert will revoke a cross-Certificate if the cross-certified entity (including DigiCert) no longer meets the stipulations of the corresponding policies, as indicated by policy OIDs listed in the policy mapping extension of the cross-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 stated in the DigiCert CPS section 4.9.1.

4.9.2 Who Can Request Revocation

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

- ***DigiCert*** 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 ***DigiCert*** is entitled to request or initiate the revocation of the Certificates issued to its own CAs. ***DigiCert*** may initiate the revocation of any CA Certificate for reasons as set forth in CPS § 4.9.1.

Regarding code signing certificates, ***DigiCert*** 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. ***DigiCert*** publicly discloses the instructions on the ***Thawte*** website.

DigiCert revokes a Code Signing Certificate in any of these four circumstances: (1) the Application Software Supplier requests revocation and ***DigiCert*** 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. ***DigiCert*** 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. ***DigiCert*** 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 ***DigiCert***, who in turn will promptly initiate revocation of the Certificate. Communication of such revocation requests shall be in accordance with CPS § 3.4.

Once DigiCert receives the request, it processes a revocation request as follows:

1. DigiCert logs the identity of the entity making the request or problem report and the reason for requesting revocation based on the list in section 4.9.1. DigiCert may also include its own reasons for revocation in the log.
2. DigiCert may request confirmation of the revocation from a known administrator, where applicable, via out-of-band communication (e.g., telephone, fax, etc.).
3. If the request is authenticated as originating from the Subscriber, DigiCert revokes the Certificate based on the timeframes listed in 4.9.1 as listed for the reason for revocation.
4. For requests from third parties, DigiCert personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
    a. the nature of the alleged problem,
    b. the number of reports received about a particular Certificate or website,
    c. the identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
    d. relevant legislation.
5. If DigiCert determines that revocation is appropriate, DigiCert personnel revoke the Certificate and update the CRL.

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

If DigiCert deems appropriate, DigiCert may forward the revocation reports to law enforcement.

DigiCert maintains a continuous 24/7 ability to internally respond to any high priority revocation requests.

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 stated in the DigiCert CPS section 4.9.3.

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

Certificate problem reports are submitted by third parties and subject to investigation. Revocation requests are submitted by DigiCert, an RA, or the Subscriber.

Certificate problem reports are submitted by third parties and subject to investigation. Revocation requests are submitted by DigiCert, an RA, or the Subscriber.

Within 24 hours after receiving a Certificate problem report, DigiCert investigates the facts and circumstances related to a Certificate problem report and will provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate problem report.

After reviewing the facts and circumstances, DigiCert works with the Subscriber and any entity reporting the Certificate problem report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which DigiCert will revoke the certificate. The period from receipt of the Certificate problem report or revocation-related notice to published revocation must not exceed the time frame set forth in Section 4.9.1. The date selected by DigiCert will consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate problem reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
5. Relevant legislation.

Under normal operating circumstances, DigiCert will revoke Certificates as quickly as practical after validating the revocation request following the guidelines of this section and Section 4.9.1, generally within the following time frames:

1. Certificate revocation requests for publicly-trusted Certificates are processed within 18 hours after their receipt,
2. Revocation requests received two or more hours before CRL issuance are processed before the next CRL is published, and
3. Revocation requests received within two hours of CRL issuance are processed before the following CRL is published.

DigiCert takes commercially reasonable steps to process revocation requests without delay. Effective February 1, 2017, ***DigiCert*** 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)

DigiCert 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)	***Thawte*** Personal Freemail CA (terminated) ***Thawte*** Primary Root CA ***Thawte*** Primary Root CA –G2 ***Thawte*** Primary Root CA – G3 ***Thawte*** Primary Root CA – G4 ***Thawte*** Time Stamping CA	At least quarterly and upon Sub-CA certificate revocation
	Thawte Server CA ***Thawte*** Premium Server CA	At least daily
Subordinate Issuing CAs	***Thawte*** Personal Freemail Issuing CA (terminated) ***Thawte*** Extended Validation SSL CA ***Thawte*** Code Signing CA – G2 ***Thawte*** DV SSL CA ***Thawte*** SSL CA ***Thawte*** SGC CA – G2 ***Thawte*** 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.

4.9.7.2 Microsoft Requirements for CRL Issuance

Frequency of CRL issuance for code signing and timestamp certificates 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.

4.9.9.2 Microsoft Requirements for OCSP Availability

DigiCert 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, ***DigiCert*** uses commercially reasonable efforts to notify potential Relying Parties if ***DigiCert*** 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

DigiCert 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.

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.

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

DigiCert's Certificate and CRL signing systems are housed in secure facilities 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 ***DigiCert***'s segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes. For more details about the DigiCert physical security, see ***DigiCert***'s CPS § 5.1.2.

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 with physical security measures that include proximity badge access and video monitoring.

DigiCert also maintains disaster recovery facilities in the United States for its CA operations.

5.1.2 Physical Access

See CPS § 5.1.1.

5.1.3 Power and Air Conditioning

DigiCert'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

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

5.1.5 Fire Prevention and Protection

DigiCert has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. ***DigiCert***'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 ***DigiCert*** 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 ***DigiCert***'s normal waste disposal requirements.

5.1.8 Off-Site Backup

DigiCert 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 ***DigiCert***'s disaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all ***DigiCert*** 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, with the exception of technical support analysts in some facilities,
- cryptographic business operations personnel,
- security personnel,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

DigiCert 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

DigiCert 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 ***DigiCert*** 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.

DigiCert 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

Roles requiring separation of duties or multi-person control include (but are not limited to)

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, key recovery requests or renewal requests, or enrollment information;
- the issuance of Certificates, including personnel having access to restricted portions of the repository;
- the handling of Subscriber information or requests
- the generation, issuing or destruction of a CA certificate
- the loading of a CA to a Production environment

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, ***DigiCert*** 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), and
- check of civil judgment 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, ***DigiCert*** 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

DigiCert 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. ***DigiCert*** periodically reviews and enhances its training programs as necessary.

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

- Basic PKI concepts,
- Job responsibilities,
- ***DigiCert*** 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.

5.3.4 Retraining Frequency and Requirements

DigiCert 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 ***DigiCert*** 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 ***DigiCert*** 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 ***DigiCert***'s secure facilities only to the extent they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation Supplied to Personnel

DigiCert personnel involved in the operation of ***Thawte*** PKI services are required to read this CPS and relevant ***DigiCert*** security policies. ***DigiCert*** 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

DigiCert 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 ***DigiCert*** 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.

5.4.2 Frequency of Processing Log

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

DigiCert 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, ***DigiCert*** maintains records that include documentation of:

- ***DigiCert***'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 ***DigiCert***.

DigiCert'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,
- CAA checking results,
- 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, ***DigiCert*** may implement longer retention periods in order to comply with applicable laws.

5.5.3 Protection of Archive

DigiCert 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

DigiCert 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 ***DigiCert*** 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). ***DigiCert***'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

DigiCert 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, ***DigiCert*** has implemented disaster recovery procedures described in CPS § 5.7.4 and Key Compromise response procedures described in CPS § 5.7.3. ***DigiCert***'s compromise and disaster recovery procedures have been developed to minimize the potential impact of such an occurrence and restore ***DigiCert***'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 ***DigiCert*** Security and ***DigiCert***'s incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, ***DigiCert***'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, ***DigiCert***'s Key Compromise Response procedures are enacted by an Incident Response Team. This team assesses the situation, develops an action plan, and implements the action plan with approval from ***DigiCert*** 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 ***DigiCert*** 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
- ***DigiCert*** 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

DigiCert has implemented a disaster recovery site separate from ***DigiCert***'s principal secure facilities. ***DigiCert*** 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, ***DigiCert***'s DRP includes the CA / Browser Forum requirements as set forth in the Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively.

DigiCert's disaster recovery site has implemented the physical security protections and operational controls required by ***DigiCert***'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 ***DigiCert***'s primary facilities, ***DigiCert***'s disaster recovery process is initiated.

DigiCert 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. ***DigiCert***'s disaster recovery plan has been designed to provide full recovery within one week following disaster occurring at ***DigiCert***'s primary sites. Where possible, operations are resumed at ***DigiCert***'s primary sites as soon as possible following a major disaster.

DigiCert 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. ***DigiCert***'s disaster recovery database is synchronized regularly with the production database. ***DigiCert***'s disaster recovery equipment is protected by physical security protections comparable to the physical security tiers specified in CPS § 5.1.1.

DigiCert 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, ***DigiCert*** 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, ***DigiCert*** 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, ***DigiCert*** conforms to the CA / Browser Forum requirements for Data Security.

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 ***DigiCert*** 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).

DigiCert 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 ***DigiCert*** 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

DigiCert 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, DigiCert provides such new Certificates to the browser manufacturers for inclusion in new browser releases and updates. In addition, ***DigiCert*** 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. ***DigiCert*** recommends that RAs and end-user Subscribers generate 2048-bit RSA key pairs (or ECC key sizes of equivalent strength).
Thawte CAs, RAs and end entity certificates use SHA-2 for digital signature hash. SHA-1 may be used to support legacy applications and use cases other than SSL and EV Code Signing provided that such

usage does not violate procedures and policies set forth by the CA/Browser Forum and related Application Software Suppliers.

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.

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 and Mozilla Root Policy 2.5 or greater where applicable.

** 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.

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

6.1.6 Public Key Parameters Generation and Quality Checking

DigiCert shall generate Public Key parameters for signature algorithms (the value of this public exponent shall be an odd number equal to three or more) and perform parameter quality checking in accordance with FIPS 186.6.1.7 Key Usage Purposes (as per x509v3 field)

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

6.2 Private Key Protection & Cryptographic Module Engineering Controls

DigiCert has implemented a combination of physical, logical, and procedural controls to ensure the security of Thawte CA private keys. ***DigiCert*** 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. **DigiCert** 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, ***DigiCert*** 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

DigiCert has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. ***DigiCert*** 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.

6.2.3 Private Key Escrow

DigiCert 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

DigiCert 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.

DigiCert 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.

DigiCert does not archive copies of Subscriber private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

DigiCert generates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, ***DigiCert*** 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.

DigiCert obtains a representation from the Subscriber that the Subscriber will use one of the following options to generate and protect their Code Signing Certificate private keys:

1. A Trusted Platform Module (TPM) that generates and secures a key pair and that can document the Subscriber's private key protection through a TPM key attestation.
2. A hardware crypto module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent.
3. Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+). The Subscriber MUST also warrant that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

DigiCert recommends that the Subscriber protect Private Keys using the method described in (1) or (2) over the method described in (3) and obligates the Subscriber to protect Private Keys in accordance with Section 10.3.2(2) in the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

6.2.8.1 End-User Subscriber Private Keys

This section describes the ***DigiCert*** 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 ***DigiCert*** 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 ***DigiCert***'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 ***DigiCert***'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). ***DigiCert*** 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, ***DigiCert*** 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. ***DigiCert*** 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 ***DigiCert***'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 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 15 years
CA to end-user Subscriber	Up to 5 years
SSL/TLS Server Certificates	Up to 825 days

Table 18 – Certificate Operational Periods

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

6.3.2.1 CABF Certificate Validity Period and Validation Data Reuse Requirements

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA /Browser Forum requirements.

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.

DigiCert strongly recommends that end-user Subscribers select strong passwords to protect their private keys. ***DigiCert*** 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

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

DigiCert 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

DigiCert performs all CA and RA functions using Trustworthy Systems.

6.5.1 Specific Computer Security Technical Requirements

DigiCert ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access. In addition, ***DigiCert*** limits access to production servers to those individuals with a valid business reason for such access. ***DigiCert***'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.

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 ***DigiCert*** in accordance with ***Thawte*** systems development and change management standards.

6.6.2 Security Management Controls

DigiCert 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

DigiCert performs all its CA and RA functions using networks secured to prevent unauthorized access and other malicious activity. ***DigiCert*** protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 Time-Stamping

DigiCert ensures that the accuracy of clocks used for time-stamping are within three minutes. Electronic or manual procedures may be used to maintain system time.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

Thawte Certificates conform to ITU-T Recommendation X.509 (2005): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, August 2005 and RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008 ("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. 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.

DigiCert 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) =	"DigiCert Inc", "Thawte Consulting cc" or "Thawte Consulting" or "Thawte"
	Locality (L) =	"California" or another locality where ***Thawte*** 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 ***Thawte*** 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 2048-bit 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

DigiCert 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.

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. For internationalized domain names, the Common Name will be represented as a Unicode encoded U-label value designed for human comprehension and that Common Name will be represented in the Subject Alternative Name extension as a puny-coded A-label value designed for automated comprehension. These different encodings of the same name are treated as equal values for the purposes of Common Name to Subject Alternative Name duplication requirements.

By default, *ExtendedKeyUsage* is set as a non-critical extension. Legacy ***Thawte*** CA Certificates may include the *ExtendedKeyUsage* extension as a form of technical constraint on the usage of certificates that they issue.

To explicitly comply with Microsoft Trusted Root Program Requirements section 4(A)(11) (http://aka.ms/rootcert), ***Thawte*** CA Certificates created after June 7, 2016 contain an EKU extension that includes at least the Server Authentication EKU and omits the Secure Email, Code Signing, and Time Stamping uses.

Subordinate CA Certificates created after January 1, 2019 for publicly trusted certificates, with the exception of cross-certificates that share a private key with a corresponding root certificate: will contain an EKU extension; and cannot include the anyExtendedKeyUsage KeyPurposeId; DigiCert no longer includes both the id-kp-serverAuth and id-kp-emailProtection KeyPurposeIds in the same certificate.

DigiCert's Technically Constrained Subordinate CA Certificates include an Extended Key Usage (EKU) extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue certificates. The anyExtendedKeyUsage KeyPurposeId does not appear in the EKU extension of publicly trusted certificates.

Subscriber Certificates contain the *ExtendedKeyUsage* extension, aligning to Application Software Supplier granted trust bits and private PKI use cases. For certificates issued after February 1, 2017, all End-user Subscriber certificates contain an extended key usage for the purpose that the certificate was issued to the end user, and shall not contain the anyEKU value.

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

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	http://crl.Thawte.com/ThawtePremiumServerCA.crl or http://crl3.digicert.com	Non-Critical
Authority information Access	http://ocsp.Thawte.com or http://ocsp.digicert.com	Non-Critical

Table 22 –Thawte SSL Web Server Certificate Extensions

7.1.2.4 SSL123 Certificates

Thawte SSL123 certificates include the extensions specified in Table 23 below:

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

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

Extension	*Value or Value Constraint*	*Criticality*
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Critical
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	Non-Critical
CRL Distribution Points	http://crl.Thawte.com/ThawtePremiumServerCA.crl or http://crl3.digicert.com	Non-Critical
Authority information Access	http://ocsp.Thawte.com or http://ocsp.digicert.com	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:

Extension	*Value or Value Constraint*	*Criticality*
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	Critical
Enhanced Key Usage	Code Signing(1.3.6.1.5.5.7.3.3)	Non-Critical
NetscapeCertType	Signature(10)	Non-Critical
Key Usage Restriction	Cert Policyld=1.3.6.1.4.1.311.2.1.22 Restricted Key Usage=Digital Signature(80)	Non-Critical
Subject Alternative Name	DNS Name=domain name of Subscriber's web site	Non-Critical
CRL Distribution Points	http://crl.Thawte.com/ThawteCodeSigningCA.crl or http://crl3.digicert.com	Non-Critical

Table 26 –Thawte Code Signing Certificate Extensions

7.1.3 Algorithm Object Identifiers

Thawte Certificates are signed with sha256RSA 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 Issuing CA.

7.1.5 Name Constraints

DigiCert may include name constraints in the nameConstraints field when appropriate.

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.

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

DigiCert 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, ***DigiCert*** 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. ***DigiCert*** CRLs are signed using sha256RSA (OID: 1.2.840.113549.1.1.11) 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. ***DigiCert*** CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. The Next Update date for ***DigiCert*** CRLs is set as follows: 3 months from the Effective Date for ***Thawte*** Non-Issuing Root CAs and at most 10 days from the Effective Date for other ***Thawte*** 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)

DigiCert 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.

OCSP responders conform to RFC 2560, RFC 5019, and RFC 6960, excluding client requested cipher support

CABF Requirement for OCSP Signing

For EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates, ***DigiCert*** provides OCSP responses compliant with RFC 6960.

7.3.1 Version Number(s)

DigiCert supports version 1 OCSP requests and responses. 7.3.2 OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

WebTrust "Principles and Criteria for Certification Authorities - Version 2.0" or later, and where applicable, WebTrust "Principles and Criteria for Certification Authorities – SSL Baseline with Network Security - Version 2.2" or later, WebTrust "Principles and Criteria for Certification Authorities - Extended Validation SSL 1.4.5" or later and/or WebTrust Principles and Criteria for Certification Authorities - Extended Validation Code Signing examinations are performed for the ***Thawte*** CAs on an annual basis. In addition, ***DigiCert*** 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, ***DigiCert*** shall conduct self-audits.

8.1 Frequency or Circumstances of Assessment

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

DigiCert'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 ***DigiCert*** performs compliance audits of ***DigiCert***'s operations.

8.4 Topics Covered by Assessment

The scope of ***DigiCert***'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 ***DigiCert***'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 ***DigiCert*** management with input from the auditor. If exceptions or deficiencies are identified, ***DigiCert*** management is responsible for developing and implementing a corrective action plan. If ***DigiCert*** 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, ***DigiCert*** 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 ***DigiCert'***s operations may be released at the discretion of ***DigiCert*** 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, DigiCert 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

DigiCert 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. ***DigiCert*** does not charge a fee as a condition of making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

DigiCert 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. ***DigiCert*** 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 ***DigiCert***'s prior express written consent.

9.1.4 Fees for Other Services

DigiCert 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 ***DigiCert***.

9.1.5 Refund Policy

If you cancel a Certificate request before the Certificate has been issued, ***DigiCert*** will issue a refund as documented on the DigiCert or ***Thawte*** website.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

DigiCert 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 DigiCert, Inc.

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 ***DigiCert*** or previously by 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 ***DigiCert***,
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of ***DigiCert*** 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, ***DigiCert***'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

DigiCert secures private information from compromise and disclosure to third parties.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

DigiCert has implemented a Privacy Statement, which is located at: https://www.digicert.com/digicert-privacy-policy.

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

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

Thawte PKI Participants acknowledge that ***DigiCert*** shall be entitled to disclose Confidential/Private Information if, in good faith, ***DigiCert*** 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. ***DigiCert*** 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. ***DigiCert*** 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 ***DigiCert*** 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 ***DigiCert***. ***DigiCert*** 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, ***DigiCert*** 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 ***DigiCert***. The Subscriber Agreements and Relying Party Agreements used by ***DigiCert*** 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.

9.6.2 RA Representations and Warranties

Where the RA function is not performed by ***DigiCert*** itself, external RAs assist ***DigiCert*** 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: ***DigiCert*** 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 ***DigiCert***.

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 ***DigiCert*** 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 ***DigiCert***, 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 ***DigiCert***'s Relying Party Agreement(s).

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 ***DigiCert***, 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 ***DigiCert***, 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

DigiCert is responsible for the repository functions for its CAs. Upon revocation of an end-user Subscriber's Certificate, ***DigiCert*** 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 ***DigiCert***'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 ***DigiCert***, 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.

DigiCert 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 ***DigiCert*** (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. ***DigiCert*** adheres to such requirements in its Subscriber Agreements. ***DigiCert***'s practices concerning warranties, disclaimers, and limitations in Relying Party Agreements apply to ***DigiCert***. 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

DigiCert'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.

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

DigiCert'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 ***DigiCert*** has issued and managed the Certificate(s) at issue in compliance with its Certification Practice Statement, ***DigiCert*** 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, ***DigiCert***'s Subscriber Agreements and Relying Party Agreements include, and other Subscriber Agreements shall include, a force majeure clause protecting ***DigiCert***.

9.8.1.5 Fiduciary Relationships

To the extent permitted by applicable law, ***DigiCert***'s Subscriber Agreements and Relying Party Agreements disclaim, and other Subscriber Agreements shall disclaim, any fiduciary relationship between ***DigiCert*** or a non-***DigiCert*** 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

DigiCert'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 ***DigiCert*** 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 ***DigiCert*** 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, ***DigiCert***'s Subscriber Agreements require, and other Subscriber Agreements shall require, Subscribers to indemnify ***DigiCert*** and any non-***DigiCert*** 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, ***DigiCert***'s Subscriber Agreements and Relying Party Agreements require, and other Subscriber Agreements shall require, Relying Parties to indemnify ***DigiCert*** and any non-***DigiCert*** 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 DCPA. Amendments shall either be in the form of a document containing an amended form of the CPS or an update. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

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

9.12.1.1 Items that Can Change Without Notification

DigiCert 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 ***DigiCert*** 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, ***DigiCert*** 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

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

9.12.3 Circumstances under Which OID must be Changed

No stipulation.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among *DigiCert* and Customers

Disputes between ***DigiCert*** 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, ***DigiCert*** 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 Utah, 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 Utah, 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 Utah, 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. ***DigiCert*** 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, ***DigiCert***'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.

9.16.5 Force Majeure

DigiCert is not liable for a delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an occurrence beyond DigiCert's reasonable control. The operation of the Internet is beyond DigiCert's reasonable control.

9.17 Other Provisions

No stipulation.

APPENDIX A: Definitions and Acronyms

Definitions

Term	Definition
Administrator	A Trusted Person that performs validation and other CA or RA functions at ***DigiCert***.
Affiliate	A leading trusted third party, for example in the technology, telecommunications, or financial services industry that has entered into an agreement with DigiCert as a distribution and services channel within a specific territory. In the CAB Forum context, the term "*Affiliate*" 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.
Applicant	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. The Applicant, its parent, affiliates, and subsidiaries are all considered interchangeable as Applicant.
Applicant Representative	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.
Application Software Supplier	A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.
Attestation Letter	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.
Audit Report	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.
Authorization Domain Name	The Domain Name used to obtain authorization for certificate issuance for a given FQDN. DigiCert may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then DigiCert removes all wildcard labels from the left most portion of requested FQDN. DigiCert may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.
Authorized Port	One of the following ports: 80 (http), 443 (http), 115 (sftp), 25 (smtp), 22 (ssh).
Base Domain Name	The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix. For FQDNs where the right-most domain name node is a gTLD granted directly to one owner by ICANN specifications, the gTLD itself may be used as the Base Domain Name.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Data	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.
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.

Term	Definition
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the ***Thawte*** PKI.
Certificate Management Process	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.
Certification Practice Statement (CPS)	A statement of the practices that ***DigiCert*** 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.
Certificate Problem Report	Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates
Code Signing Certificates	Certificates which secure delivery of code and content to browsers over the Internet.
Compliance Audit	A periodic audit that the ***Thawte*** PKI or its Customer undergoes to determine its conformance with ***DigiCert*** requirements that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private.
Country	A Country shall mean a Sovereign state as defined in the Guidelines.
Cross Certificate	A certificate that is used to establish a trust relationship between two Root CAs.
Cryptographically Secure Pseudo-Random Number Generator	A random number generator intended for use in a cryptographic system.
Customer	An individual or organization that has purchased a product or service from ***DigiCert*** and/or its representatives.
Delegated Third Party	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.
Domain Authorization	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.
Domain Contact	The Domain Name Registrant, technical contact, or administrative "corporate" contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.
Domain Name	The label assigned to a node in the Domain Name System.
Domain Namespace	The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
Domain Name Registrant	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.
Domain Name Registrar	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).
Expiry Date	The "Not After" date in a Certificate that defines the end of a Certificate's validity period.
EV Certificate	A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the guidelines.
Fully-Qualified Domain Name	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
Government Entity	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.).
High Assurance	Certificates issued to organizations and sole proprietors to provide stringent 3 step authentication; message, software, and content integrity; and confidentiality encryption.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.

Term	Definition
International Organization	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.
Internal Server Name	A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.
Issuing CA	In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
Key Compromise	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.
Key Generation Ceremony	A procedure whereby a CA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Generation Script	A documented plan of procedures for the generation of a CA Key Pair.
Key Pair	The Private Key and its associated Public Key.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
Medium Assurance	Certificates that are issued to Domains to provide confidentiality encryption. ***DigiCert*** validates that the person enrolling for the certificate has control of the domain by requiring the person to respond to an e-mail hosted at that domain. No organization authentication is performed on the owner of the domain.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a ***DigiCert*** Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Nonverified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Object Identifier	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
OCSP (Online Certificate Status Protocol)	An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information.
OCSP Responder	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.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
Parent Company	**Parent Company:** 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.
PKCS #7	Public-Key Cryptography Standard #7, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Principal Individual(s)	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.

Term	Definition
Private Key	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.
Public Key	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.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The ***Thawte*** PKI consists of systems that collaborate to provide and implement the ***Thawte*** PKI.
Publicly-Trusted Certificate	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.
Qualified Auditor	A natural person or Legal Entity that meets the Auditor Qualifications.
Random Value	A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
Referee	An individual who is permitted by the ***Thawte*** PKI to validate the identity of a Web of Trust subscriber in the event that a ***Thawte*** Web of Trust Notary is not available. The referee must be a bank manager, registered lawyer, or registered CPA (accountant).
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar.
Registration Agency	A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include, but is not limited (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Comptroller of Currency (OCC) or Office of Thrift Supervision (OTC)
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Reliable Method of Communication	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.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Repository	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.
Request Token	A value derived in a method specified by the CA which binds this demonstration of control to the certificate request. The Request Token incorporates the key used in the certificate request. A Request Token may include a timestamp to indicate when it was created. A Request Token may include other information to ensure its uniqueness. A Request Token that includes a timestamp remains valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp is treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and DigiCert does not re-use it for a subsequent validation. The binding uses a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.
Reseller	An entity marketing services on behalf of ***DigiCert*** to specific markets (e.g., the country representatives).
Reseller Partner Program	A program that allows Resellers to enroll for SSL Web Server Certificates, SSL Wildcard Certificates, SSL123 Certificates and SGC SuperCerts on behalf of end-user Subscribers who are customers of the Reseller.
Reserved IP Address	An IPv4 or IPv6 address that the IANA has marked as reserved: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Root CA	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Term	Definition
Root Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations.
Sovereign State	A Sovereign state is a state, or country, that administers its own government, and is not dependent upon, or subject to, another power.
SSL123 Certificates	Medium Assurance domain validated SSL certificates capable of 256-bit encryption and issued within minutes used to support SSL sessions between web browsers and servers. Delays in issuance can be caused if the domain is not registered with an accredited online registrar.
SSL Web Server Certificates	High Assurance secure SSL certificates with stringent 3 step authentication capable of 256-bit encryption used to support SSL sessions between web browsers and servers.
Subject	The 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.
Subject Identity Information	Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the *subjectAltName* extension or the Subject *commonName* field.
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
Subsidiary Company	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.
SGC SuperCerts	High Assurance Premium Server Gated Cryptography SSL certificates with stringent 3 step authentication, automatic 128-bit step-up encryption and capable of 256-bit encryption * used to support SSL sessions between web browsers and web servers. * With browsers IE 4.X or Netscape 4.06 and later
Superior Entity	An entity above a certain entity within the ***Thawte*** PKI.
Terms of Use	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.
Test Certificate	A Certificate with a maximum validity period of 30 days and which: (i) includes a critical extension with the specified Test Certificate CABF OID, or (ii) is issued under a CA where there are no certificate paths/chains to a root certificate subject to these Requirements.
Thawte PKI Participants	An individual or organization that is one or more of the following within the ***Thawte*** PKI: ***DigiCert***, a Customer, a Reseller, a Subscriber, or a Relying Party.
Thawte Repository	***DigiCert*** a database of relevant ***Thawte*** PKI information accessible on-line.
Transport Layer Security (TLS)	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.

Term	Definition
Trusted Person	An employee, contractor, or consultant of an entity within the ***Thawte*** PKI responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices.
Trusted Position	The positions within a ***Thawte*** PKI entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
Unregistered Domain Name	A Domain Name that is not a Registered Domain Name.
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280.
Validation Specialists	Someone who performs the information verification duties specified by these Requirements.
Validity Period	The period of time measured from the date when the Certificate is issued until the Expiry Date.
Web Host	An entity hosting the web site of another, such as an Internet service provider, a systems integrator, a Reseller, a technical consultant, and application service provider, or similar entity.
Wildcard Certificates	*Secure SSL certificates with stringent 3 step authentication capable of 256-bit encryption that secure multiple hosts on a single domain on the same server.* A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

Acronyms

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

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. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST 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 ***DigiCert***.

certificatePolicies:policyIdentifier (Required)

- The ***anyPolicy*** identifier if subordinate CA is controlled by ***DigiCert***
- explicit EV policy OID(s) if subordinate CA is not controlled by ***DigiCert***

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

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 ***DigiCert*'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 ***DigiCert*'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. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST 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. ***Thawte***

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 ***DigiCert***'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, ***DigiCert*** MAY include a Latin character organization name in the EV certificate. In such a case, ***DigiCert*** 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 ***DigiCert*** cannot 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, ***DigiCert*** 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.
- ***DigiCert*** MAY verify the Romanized transliteration of Applicant's formal legal name with either a QIIS or a lawyer's opinion letter.
- ***DigiCert*** MAY use the Financial Services Agency to verify an English Name. When used, ***DigiCert*** 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. ***DigiCert*** 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/