Sectigo Code Signing Certificates Certificate Policy and Certification Practice Statement

Sectigo Limited
Version: 1.0.5
Effective: November 11, 2025
Unit 7, Campus Road, Listerhills Science Park,
Bradford, BD7 1HR, United Kingdom
Tel: +44 (0) 161 874 7070
www.sectigo.com
Sectigo Limited

Latest Revision: November 11, 2025

Table of Contents

1. INTRODUCTION

Sectigo is a Certification Authority (CA) that issues high quality and highly trusted Code Signing Certificates to entities including private and public companies and individuals in accordance with this document. In its role as a CA, Sectigo performs functions associated with public key operations that include receiving requests, issuing, revoking and renewing a digital Certificate and the maintenance, issuance and publication of Certificate Revocation Lists (CRLs) for users within the Sectigo Public Key Infrastructure (PKI).

1.1. Overview

For the issuance of Code Signing Certificates Sectigo conforms to the latest published version of the Code Signing Baseline Requirements (CS BRs) published at https://www.cabforum.org. In the event of any inconsistency between this document and the CS BRs, the CS BRs take precedence over this document.

Sectigo MAY extend, under agreement, membership of its PKI to approved third parties known as Registration Authorities (RAs). The international network of Sectigo RAs share Sectigo's policies, practices, and CA Infrastructure to issue Sectigo digital Certificates.

This document states the Policy and Practice Statement applied to the Code Signing Certificates of Sectigo, referred as the Certification Practice Statement (CPS).

This document is only one of a set of documents relevant to the provision of Certification Services by Sectigo and that the list of documents contained in this clause are other documents that this docuemnt will from time to time mention, although this is not an exhaustive list. The document name, location of and status, whether public or private, are detailed below.

Document	Status	Location
Sectigo Relying Party Agreement	Public	Sectigo Repository
Certificate Subscriber Agreement	Public	Sectigo Repository
Enterprise Certificate Agreement	Public	Sectigo Repository

This document and related agreements are available online at sectigo.com/legal.

1.2. Document Name and Identification

This document is the Sectigo Certificate Policy and Certification Practice Statement for Code Signing Certificates. It outlines the legal, commercial and technical principles and practices that Sectigo employ in providing certification services that include, but are not limited to, approving, issuing, using and managing of Digital Certificates and in maintaining a X.509 Certificate based public key infrastructure (PKI) in accordance with the Certificate Policies determined by Sectigo. It also defines the underlying certification processes for Subscribers and describes Sectigo's repository operations. This document is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the Sectigo PKI.

This document is a public statement of the policies and practices of Sectigo and the conditions of issuance, revocation and renewal of a Certificate issued under Sectigo's own hierarchy.

This document is structured in accordance with the Internet Engineering Task Force (IETF) standard RFC 3647.

OIDs found in Certificates reliant upon CAB Forum requirements and guidelines include the designated reserved policy identifiers in the Certificate Policy extension as specified in the CAB Forum Code Signing Baseline Requirements.

1.2.1. Revisions

See Appendix B.

1.3. PKI Participants

This section identifies and describes some of the entities that participate within the Sectigo PKI. Sectigo conforms to this CPS and other obligations it undertakes through adjacent contracts when it provides its services.

1.3.1. Certification Authorities

In its role as a CA, Sectigo provides Certificate services within the Sectigo PKI. Sectigo will:

- Conform its operations to this CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the Repository,
- Issue and publish Certificates in a timely manner in accordance with the issuance times set out in this CPS,
- Upon receipt of a valid request to revoke the Certificate from a person authorized to request revocation using the revocation methods detailed in this CPS, revoke a Certificate issued for use within the Sectigo PKI,
- Publish CRLs on a regular basis, in accordance with the applicable Policy and with provisions described in this CPS,
- Distribute issued Certificates in accordance with the methods detailed in this CPS,
- Update CRLs in a timely manner as detailed in this CPS,
- Notify Subscribers via email of the imminent expiry of their Sectigo issued Certificate (for a period disclosed in this CPS).

1.3.2. Registration Authorities

The registration authorities (RAs) collect and verify each Subscriber's identity and information that is to be entered into the Subscriber's Public Key Certificate. The RA performs its function in accordance with this document approved by the Policy Authority Sectigo has established the necessary secure infrastructure to fully manage the lifecycle of digital Certificates within its PKI. Through a network of RAs, Sectigo also makes its certification authority services available to its Subscribers. Sectigo RAs:

- Accept, evaluate, approve or reject the registration of Certificate applications.
- Verify the accuracy and authenticity of the information provided by the Subscriber at the time of application as specified in this CPS and the CS BRs.
- Use official, notarized or otherwise indicated document to evaluate a Subscriber application.
- Verify the accuracy and authenticity of the information provided by the Subscriber at the time of reissue or renewal as specified in this CPS and the CS BRs.

RAs act locally within their own context of geographical or business partnerships on approval and authorization by Sectigo in accordance with Sectigo practices and procedures.

Sectigo MAY extend the use of RAs for its Enterprise Public Key Infrastructure (EPKI) Manager. Upon successful approval to join the program, EPKI Manager Subscriber MAY be permitted to act as an RA on behalf of Sectigo. RAs are required to conform to this CPS and the CS BR.

RAs MAY only undertake their validation duties from pre-approved systems which are identified to the CA by various means that always include but are not limited to the white-listing of the IP address from which the RA operates.

Sectigo operates several intermediate CAs from which it issues certificates for which some part of the validation has been performed by a Registration Authority. Some of the intermediate CAs are dedicated to the work of a single RA, whilst others are dedicated to the work of multiple related RAs.

1.3.2.1. Internal Registration Authority

Sectigo operates its own internal RA that allows retail customers as well as all customers of Reseller Partners along with some of Sectigo's Resellers to manage their Certificate lifecycle, including application, issuance, renewal and revocation. Sectigo's RA adheres to this Sectigo's CPS.

Sectigo's internal RA, together with its staff and systems, all fall within the scope of Sectigo's WebTrust certifications.

1.3.2.2. External Registration Authority

Some resellers, Partners or enterprise customers may be authorized by Sectigo to act as external RAs. As such they MAY be granted RA functionality which MAY include the validation of some or all of the subject identity information. The external RA is obliged to conduct validation in accordance with this CPS and the CS BRs prior to issuing a Certificate and acknowledges that they have sufficiently validated the Applicant's identity. This acknowledgement may be via an online process (for example by checking the "I have sufficiently validated this application" checkbox when applying for a Certificate), or via API parameters that sufficient validation has taken place prior to Sectigo issuing a Certificate.

Some of these external RAs have their own practice statement for RAs and are duly audited and certified.

1.3.3. Subscribers (End Entities)

Subscribers of Sectigo services are individuals or companies that use PKI in relation with Sectigo supported transactions and communications. Subscribers are parties that are identified in a Certificate and hold the Private Key corresponding to the Public Key listed in the Certificate. Prior to verification of identity and issuance of a Certificate, a Subscriber is an Applicant for the services of Sectigo.

1.3.4. Relying Parties

A Relying Party is an entity that relies on the validity of the binding of the Subscriber's name to a Public Key. The Relying Party uses a Subscriber's Certificate to verify or establish the identity and status of the Subscriber. A Relying Party is responsible for deciding whether or how to check the validity of the Certificate by checking the appropriate Certificate status information. A Relying Party MAY use information in the Certificate to determine the suitability of the Certificate for a particular use.

Relying Parties use PKI services in relation with various Sectigo Certificates for their intended purposes and may reasonably rely on such Certificates and/or digital signatures verifiable with reference to a Public Key listed in a Subscriber Certificate. Because not all Sectigo Certificate products are intended to be used in an e-commerce transaction or environment, parties who rely on Certificates not intended for e-commerce do not qualify as a Relying Party. Please refer to section 1.4 of this document to determine whether a particular product is intended for use in e-commerce transactions.

To verify the validity of a digital Certificate they receive, Relying Parties must refer to the CRL or Online Certificate Status Protocol (OCSP) response prior to relying on information featured in a Certificate to ensure that Sectigo has not revoked the Certificate. The CRL location is detailed within the Certificate. OCSP responses are sent through the OCSP responder.

1.3.5. Other Participants

The CAs and RAs operating under this document MAY require the services of other security, community, and application authorities. Sectigo has several categories of partner which assist in the provision of certification services.

1.3.5.1. Reseller Partners

Sectigo operates a Reseller Partner network that allows authorized partners to integrate Sectigo digital Certificates into their own product portfolios. Reseller Partners are responsible for referring digital

Certificate customers to Sectigo, who maintain full control over the Certificate lifecycle process, including application, issuance, renewal and revocation. Due to the nature of the reseller program, the Reseller Partner must authorize a pending customer order made through its Reseller Partner account prior to Sectigo instigating the validation of such Certificate orders. All Reseller Partners are required to provide proof of organizational status (refer to section 3.2.2 of this document for examples of documentation required) and must enter into a Sectigo Reseller Partner agreement prior to being provided with Reseller Partner facilities.

1.3.5.2. EPKI Manager Accounts

Sectigo Enterprise PKI (EPKI) Manager is a fully outsourced enterprise public key infrastructure service that allows authorized EPKI Manager account holders to control the entire Certificate lifecycle process, including application, issuance, renewal and revocation, for Certificates designated to company servers, intranets, extranets, partners, employees and hardware devices.

These accounts are able to streamline the verification and issuance process by restricting the subject identifying information in the Certificates to refer only to the organization's name and address previously verified by Sectigo.

The EPKI Manager account holder is obliged to request Certificates only for legitimate company resources, including domain names (servers), intranets, extranets, partners, employees and hardware devices.

1.4. Certificate Usage

A digital Certificate is formatted data that cryptographically binds an identified Subscriber with a Public Key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital Certificates are used in commercial environments as a digital equivalent of an identification card.

Sectigo currently offers a portfolio of digital Certificates and related products that can be used to address the needs of users for secure personal and business communications, protection of online transactions and identification of persons, whether legal or physical, or devices on a network or within a community.

Sectigo may update or extend its list of products, including the types of Certificates it issues, as it sees fit. The publication or updating of the list of Sectigo products creates no claims by any third party.

1.4.1. Appropriate Certificate Uses

As detailed in this document, Sectigo offers a range of distinct Code Signing Certificate types. The different Certificate types have differing intended usages and differing policies. Pricing and Subscriber fees for the Certificates are made available on the relevant official Sectigo websites. The maximum warranty associated with each Certificate is set forth in detail in section 9.2.3 of this document.

As the suggested usage for a digital Certificate differs on a per application basis, Subscribers are urged to appropriately study their requirements for their specific application before applying for a specific Certificate. Revoked Certificates are appropriately referenced in CRLs and published in Sectigo directories.

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

Code Signing Certificates MAY be either OV or EV based upon the level of identity verification undertaken.

1.4.2. Prohibited Certificate Uses

Certificates are prohibited from being used to the extent that the use is inconsistent with applicable law. Certificates are prohibited from being used 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 damage to persons or property.

1.5. Policy Administration

Information located in this section includes the contact information of the organization responsible for drafting, registering, maintaining, updating, and approving this document.

1.5.1. Organization Administering the Document

The Sectigo Policy Authority: - Establishes and maintains this document, related agreements and policies referenced within this document, - Approves the establishment of trust relationships with external PKIs that offer appropiately comparable assurance - Ensures that all aspects of the CA services, operations, and infrastructure as described in this document are performed in accordance with the requirements, representations, and warranties.

1.5.2. Contact Person

The Sectigo Policy Authority may be contacted at the following address:

Sectigo Policy Authority Unit 7, Campus Road, Listerhills Science Park, Bradford, BD7 1HR, United Kingdom

Tel: +44 (0) 161 874 7070

Attention: Legal Practices

URL: https://www.sectigo.com

Email: legalnotices@sectigo.com

1.5.2.1. Problem Reporting Address

To report abuse, fraudulent, or malicious use of Certificates issued by Sectigo, please see the supported methods below. All these methods can be found at: https://sectigo.com/support/revocation

We encourage the use of our automated revocation portal.

1.5.2.1.1. Revocation Portal

To revoke one or more certificates issued by Sectigo for which you (i) are the Subscriber or (ii) have in your possession the private key, you may use our automated Revocation Portal here:

- https://secure.sectigo.com/products/RevocationPortal

1.5.2.1.2. Notifying Us Via Email

For other issues or if you are unable to use the above automated revocation methods please send email to: signedmalwarealert@sectigo.com

1.5.3. Person Determining CPS Suitability for the Policy

The Sectigo Policy Authority is responsible for determining the suitability of Certificate policies illustrated within this document. The Sectigo Policy Authority is also responsible for determining the suitability of proposed changes to this document prior to the publication of an amended edition.

1.5.4. CPS approval procedures

This document and any subsequent changes, amendments, or addenda, shall be approved by the Sectigo Policy Authority as specified in the *Sectigo Policy Authority (PA) Membership and Procedures* document.

1.6. Definitions and Acronyms

The list of definitions and acronyms located in this section are for use within this document.

1.6.1. Definitions

Capitalized terms used throughout this document shall have the meanings set forth below:

Term	Definition
Air-Gapped	Physically and logically separated, disconnected, and isolated from all other Systems.
Applicant	Means 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.
Applicant Representative	Means 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.
Anti-Malware Organization	An entity that maintains information about Suspect Code and/or develops software used to prevent, detect, or remove malware.
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	Means 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 the Baseline Requirements.
Basic Constraints	Means an extension that specifies whether the subject of the Certificate may act as a CA or only as an end-entity
CA Infrastructure	Collectively the infrastructure used by the CA or Delegated Third Party which qualifies as a: Certificate Management System; Certificate System; Delegated Third Party System; Issuing System; Root CA System (Air-Gapped and otherwise); or Security Support System.
Certificate	Means an electronic document that uses a digital signature to bind a Public Key and an entity.
Certificate Management System	Means a system used by Sectigo to process, approve issuance of, or store Certificates or Certificate status information, including the database, database server, and storage.
Certificate Management	Means the functions that include but are not limited to the following: verification of the identity of an Applicant of a Certificate; authorizing the issuance of Certificates; issuance of Certificates; revocation of Certificates; listing of Certificates; distributing Certificates; publishing Certificates; storing Certificates; storing Private Keys; escrowing Private Keys; generating, issuing, decommissioning, and destruction of Key Pairs; and retrieving Certificates in accordance with their particular intended use.
Certificate Manager	Means the software issued by Sectigo and used by Subscribers to download Certificates.
Certificate Policy	Means a statement of the issuer that corresponds to the prescribed usage of a digital Certificate within an issuance context.

Term	Definition
Certificate System	Means the system used by Sectigo or a delegated third party to access, process, or manage data or provide services related to: 1. identity validation; 2. identity authentication; 3. account registration; 4. certificate application; 5. certificate approval; 6. certificate issuance; 7. certificate revocation; 8. authoritative certificate status; or 9. key escrow.
Certification Authority	An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.
Code	A contiguous set of bits that has been or can be digitally signed with a Private Key that corresponds to a Code Signing Certificate
Code Signing BR	Means the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, published at https://www.cabforum.org.
Code Signing Certificate	A digital certificate issued by a CA that contains a code Signing EKU
Common Criteria	is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) in a Security Target (ST), and may be taken from Protection Profiles (PPs). It is an international standard (ISO/IEC 15408) for computer security certification
Critical Vulnerability	A system vulnerability that has a CVSS v2.0 score of 7.0 or higher according to the NVD or an equivalent to such CVSS rating (see http://nvd.nist.gov/home.cfm https://nvd.nist.gov/vuln-metrics/cvss), or as otherwise designated as a Critical Vulnerability by the CA or the CA/Browser Forum.
Demand Deposit Account	a deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as: a checking account, a share draft account, or a current account
EV Code Signing Certificate	A Code Signing Certificate validated and issued in accordance the EV Code Signing requirements as per the CS BRs.
Grace Period	Means the period during which the Subscriber must make a revocation request.
IP Address Registration Authority	The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).
Issuing System	Means a system used to sign Certificates or validity status information.
Key Pair	The Private Key and its associated Public Key
Legal Entity	Means an association, corporation, partnership, proprietorship, trust, government entity, or other entity with legal standing in a country's legal system.
Lifetime Signing OID	An optional extended key usage OID (1.3.6.1.4.1.311.10.3.13) used by Microsoft Authenticode to limit the lifetime of the code signature to the expiration of the code signing certificate.
Multi-Factor Authentication	An authentication mechanism consisting of two or more of the following independent categories of credentials (i.e. factors) to verify the user's identity for a login or other transaction: 1. something the user knows (knowledge factor); 2. something the user has (possession factor); and 3. something the user is (inherence factor). Each factor is independent of the other(s).
Multi-Party Control	An access control mechanism which requires two or more separate, authorized users to successfully authenticate with their own unique credentials prior to access being granted.
Physically Secure Environment	A controlled and protected physical space consisting minimally of a physical environment which is: 1. protected by security controls which address the topics outlined in section 4.5.1 of RFC 3647; and 2. designed, built, and maintained in accordance with Risk Assessments conducted by the CA.

Term	Definition
Private Key	The cryptographic key of an asymmetric Key Pair that is kept secret by the holder of the Key Pair. It may be used to create digital signatures and/or to decrypt data that were encrypted by the corresponding Public Key
Public Key	The cryptographic key of an asymmetric Key Pair that can be made public without compromising the security of the Key Pair. It may be used to verify digital signatures and/or to encrypt data that can be decrypted by the corresponding Private Key
Random Value	Means a value specified by Sectigo to the Applicant that exhibits at least 112 bits of entropy.
Registration Authority	Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA MAY assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
Reliable Method of Communication	Means 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	Means an entity that relies upon the information contained within the Certificate.
Relying Party Agreement	means an agreement between Sectigo and a Relying Party that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference in the Repository.
Repository	Means Sectigo's repository, available at www.sectigo.com/legal.
Request Token	Means a value derived in a method specified by Sectigo which binds a demonstration of control to the certificate request.
Risk Assessment	A formal process that: 1. Identifies and documents foreseeable internal and external threats to the CA Infrastucture that could result in: unauthorized access to the CA Infrastructure; disclosure of data stored in the CA Infrastructure; misuse of the CA Infrastructure; or unapproved alteration or destruction of any part of the CA Infrastructure; 2. Assesses and documents the likelihood and potential damage of each identified threat, taking into consideration minimally the sensitivity and criticality of the CA Infrastructure; and 3. Assesses and documents the sufficiency of the policies, procedures, controls, information systems, technology, and other arrangements that the CA has in place to counter each identified threat.
Root CA Certificate	A self-signed and self-issued certificate where: 1. the issuer and subject of the certificate are the same; and 2. the digital signature of the certificate is: generated using the Private Key of a Key Pair whose corresponding Public Key is bound to the certificate; and verified using the Public Key contained in the certificate.
Root CA Private Key	The Private Key associated with a Root CA Certificate.
Root CA System	A system used to: 1. generate a Key Pair whose Private Key is or will be a Root CA Private Key; 2. store a Root CA Private Key; or 3. create digital signatures using a Root CA Private Key.
Sectigo Policy Authority	Means the entity charged with the maintenance and publication of this CPS.
Security Support System	A system or set of systems supporting the security of the CA Infrastructure, which minimally includes: 1. authentication; 2. network boundary control; 3. audit logging; 4. audit log reduction and analysis; 5. vulnerability scanning; 6. physical intrusion detection; 7. host-based intrusion detection; and 8. network-based intrusion detection
Subscriber	Means is an entity that has been issued a Certificate.
Subscriber Agreement	Means an agreement that must be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the digital Certificate product type as presented during the product online order process and is available for reference in the Repository.

Term	Definition
Suspect Code	Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, code that compromises user security and/or code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the Platforms on which it executes.
Takeover attack	An attack where a Private Key associated with a Code Signing Certificate has been compromised by means of fraud, theft, intentional malicious act of the Subject's agent, or other illegal conduct.
Timestamp Authority	A service operated by the CA or a delegated third party for its own code signing certificate users that timestamps data using a certificate chained to a public root, thereby asserting that the data (or the data from which the data were derived via a secure hashing algorithm) existed at the specified time.
Timestamp Certificate	A certificate issued to a Timestamp Authority to use to timestamp data.
Trusted Role	An employee or contractor of a CA or Delegated Third Party who has authorized access to any component of CA Infrastructure.
Verified Method of Communication	Method of communication as defined and verified in conformance with TLSEVG
WebTrust for Certification Authorities	Means the current program for CAs located at CPA Canada Webtrust Principles and Criteria.
Workstation	A device, such as a phone, tablet, or desktop or laptop computer, which is: 1. connected to the same network as CA Infrastructure and/or Network Equipment; and 2. capable of accessing CA Infrastructure and/or Network Equipment
X.509	Means the ITU-T standard for Certificates and their corresponding authentication framework

1.6.2. Acronyms

Acronyms and abbreviations used throughout this CPS shall stand for the phrases or words set forth below:

Acronym	Full Name
BIPM	International Bureau of Weights and Measures
CA	Certificate Authority
CA/B (or CAB)	Certificate Authority/Browser (Forum)
CMS	Certificate Management System
CPS	Certification Practice Statement
CRL(s)	Certificate Revocation List(s)
CS BRs	Code Signing Baseline Requirements (see Definitions)
CSR	Certificate Signing Request
DN	Distinguished Name
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EPKI	Enterprise Public Key Infrastructure Manager
EV	Extended Validation
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
HSM	Hardware Security Module
JoI	Jurisdiction of Incorporation
NIST	National Institute for Standards and Technology

Acronym	Full Name
OCSP	Online Certificate Status Protocol
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
RA(s)	Registration Authority(ies)
RFC	Request for Comments
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
TSA	Time Stamping Authority
UTC	Coordinated Universal Time

1.6.3. Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in these Requirements shall be interpreted in accordance with RFC 2119.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

Sectigo publishes this document, Certificate terms and conditions, the Relying Party Agreement and copies of all Subscriber Agreements and a list of EV Jurisdiction of Incorporation/Registration data sources in the Repository. The Sectigo Policy Authority maintains the Sectigo Repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in section 5.4 of this document.

Published critical information may be updated from time to time as prescribed in this document. Such updates shall be indicated through appropriate version numbering and publication date on any new version.

2.1. Repositories

Sectigo publishes a repository of legal notices regarding its PKI services, including this document, agreements and notices, references within this document, as well as any other information it considers essential to its services. The Repository may be accessed at sectigo.com/legal and is available on a 24x7 basis.

2.2. Publication of Certification Information

The Sectigo Certificate services and the Repository are accessible through several means of communication:

- On the web: www.sectigo.com/legal
- By email: legalnotices@sectigo.com
- By mail:

Sectigo Ltd. Attention: Legal Practices, Unit 7, Campus Road, Listerhills Science Park, Bradford, BD7 1HR, United Kingdom

Tel: + 44(0) 161 874 7070

As specified in section 1.2, this document is structured in accordance with RFC 3647 and includes all material required by RFC 3647.

2.3. Time or Frequency of Publication

Issuance and revocation information regarding Certificates will be published as soon as possible. Updated or modified versions of Subscriber Agreements and Relying Party Agreements are usually published within seven days after approval. This document is reviewed and updated or modified versions are published at least once per year and in accordance with section 9.12 of this document. For CRL issuance frequency, see section 4.9.7 of this document.

2.4. Access Controls on Repositories

All documents (certificate policies and practices), published in the Repository are, and will be, for public information and access is freely available. Sectigo has security control measures in place to prevent unauthorized modification of the Repository.

2.5. Accuracy of Information

Sectigo, recognizing its trusted position, makes all reasonable efforts to ensure that parties accessing the Repository receive accurate, updated and correct information. Sectigo, however, cannot accept any liability beyond the limits set in this document and the Sectigo insurance policy.

3. IDENTIFICATION AND AUTHENTICATION

Sectigo offers different Certificate types. Prior to the issuance of a Certificate, Sectigo will validate an application in accordance with this document that may involve the request by Sectigo to the Applicant for relevant official documentation supporting the application.

Sectigo conducts the overall certification management within the Sectigo PKI; either directly or through a Sectigo approved RA.

3.1. Naming

3.1.1. Types of Names

Sectigo issues Certificates with non-null subject DNs. The constituent elements of the subject DN conform with ITU X.500.

Sectigo does not issue pseudonymous Certificates except as detailed in section 3.1.3 of this document.

3.1.2. Need for Names to be Meaningful

Sectigo puts meaningful names in both the subjectDN and the issuerDN extensions of Certificates. The names in the Certificates identify the subject and issuer respectively.

End entity Certificates SHALL contain meaningful names with commonly understood semantics permitting the determination of the identity of the Subject of the Certificate. CA Certificates that assert this policy SHALL identify the subject as a CA and include the name-space for which the CA is authoritative. For example: c= country, o = Issuer Organization Name, cn = OrganizationX CA-3 The subject name in CA Certificates MUST match the issuer name in Certificates issued by the CA, as required by the RFC5280.

3.1.3. Anonymity or Pseudonymity of Subscribers

Sectigo does not issue pseudonymous Certificates for code-signing.

3.1.4. Rules for Interpreting Various Name Forms

The name forms used in Certificate subjectDNs and issuerDNs conform to a subset of those defined and documented in RFC 2253 and ITU-T X.520.

3.1.5. Uniqueness of Names

Sectigo does not in general enforce uniqueness of subject names. However, Sectigo assigns Certificate serial numbers that appear in Sectigo Certificates. Assigned serial numbers are unique. Sectigo generates at least 64-bit serial numbers. These numbers are the output of a CSPRNG. We have a separate uniqueness check that verifies that serial numbers are never re-used.

3.1.6. Recognition, Authentication, and Role of Trademarks

Subscribers and Applicants may not request Certificates with content that infringes the intellectual property rights of another entity. Unless otherwise specifically stated in this document, Sectigo does not verify an Applicant's or Subscriber's right to use a trademark. Sectigo does not resolve trademark disputes. Sectigo may reject any application or revoke any Certificate that is part of a trademark dispute.

Sectigo does check subject names against a limited number of trademarks and brand names which are perceived to be of high value. A match between a part of the subject name and one of these high value names triggers a more careful examination of the subject name and Applicant.

3.2. Initial Identity Validation

This section contains information about Sectigo's identification and authentication procedures for registration of subjects such as Applicants, RAs, CAs, and other participants. Sectigo MAY use any legal means of communication or investigation to validate the identity of these subjects.

From time to time, Sectigo MAY modify the requirements related to application information to respond to Sectigo's requirements, the business context of the usage of a digital Certificate, other industry requirements, or as prescribed by law.

3.2.1. Method to Prove Possession of Private Key

If the Applicant generates the Certificate key pair, then the CA SHALL prove that the Applicant possesses the Private Key. This will typically be done by verifying the Applicant's digital signature on the PKCS #10 Certificate Signing Request (CSR) with the Public Key in the CSR.

In the case where key generation is performed under the CA or RA's direct control, proof of possession is not required. Sectigo MAY approve other methods to prove possession of the Private Key by an Applicant. If other methods are approved, they SHALL be stipulated in this document.

Verification of a digital signature is used to determine that:

- the Private Key corresponding to the Public Key listed in the signer's Certificate created the digital signature, and
- the signed data associated with this digital signature has not been altered since the digital signature was created.

3.2.2. Authentication of Organization Identity

Authentication of an organization identity is performed through the validation processes specified below. Applications for Sectigo Certificates are supported by appropriate documentation to establish the identity of an Applicant.

3.2.2.1. Authentication of Organization Identity for OV Code Signing Certificates

Sectigo verifies the identity and address of the Applicant in accordance with the CA/Browser Forum Code Signing Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (commonly referred to as the Code Signing Baseline Requirements), using documentation that is provided by, or through communication with at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence or recognition;
2. A third-party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or,
4. An attestation letter;

Sectigo MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address. Alternatively, Sectigo MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that Sectigo determines to be reliable.

If the organization´s date of formation is less than 3 years prior to the date of the certificate request, Sectigo will verify the identity of the certificate requester as per section 3.2.3.1.

If the Subject Identity Information in the certificate is to include a DBA or Trade Name, Sectigo shall verify the Applicant's right to use such DBA/Trade Name using number 1, 2, or 4 above, or:

1. Communication directly with a government agency responsible for the management of such DBAs or trade names, or;
2. A utility bill, bank statement, credit card statement, government issued tax document, or other form of identification that Sectigo determines to be reliable.

3.2.2.2. Authentication of Organization Identity for EV Code Signing Certificates

Before issuing an EV Code Signing Certificate, Sectigo ensures that all Subject organization information to be included in the EV Code Signing Certificate conforms to the requirements of, and is verified in

accordance with the Baseline Requirements *For The Issuance And Management Of Publicly Trusted Code Signing Certificates* (commonly referred to as Code Signing BR) as applicable.

Sectigo will verify:

- Applicant's Legal Existence and Identity
- Applicant's Assumed Name (if applicable)
- Applicant's Physical Existence and Business Presence
- Verified Method of Communication with the Applicant
- Applicant's Operational Existence
- The Name, Title, and Authority of Contract Signer and Certificate Approver
- Signature on Subscriber Agreement and EV Certificate Requests
- Approval of EV Certificate Request

These verifications are performed as specified and required in section 3.2.2.2.1, 3.2.2.4 and 3.2.2.2 of the EV Guidelines including:

- Verification of the name and title of contract signers and certificate approvers; and
- Verification of signatures on the subscriber agreement and certificate request.

Sectigo MAY accept or require, at its discretion, other official documentation supporting an application, possibly including, but not limited to, requiring face to face verification of the Applicant's identity before an authorized agent of Sectigo, an attorney, a CPA, a Latin notary, a notary public or equivalent.

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

For purposes of verifying the Applicant's Legal Existence/Jurisdiction of Incorporation or Registration information Sectigo uses the data sources as published at https://sectigo.com/legal

3.2.2.3. Data source accuracy

All data sources are evaluated for reliability, accuracy, and for their protection from alteration and falsification before they are used for any identification or authentication purposes. Data sources are revalidated in accordance with the CA/Browser Forum Baseline Requirements for code signing certificates or other best practices documentation.

3.2.3. Authentication of Individual Identity

Authentication of an individual identity is performed through the validation processes specified below and depends on the type of Certificate. Applications for Sectigo Certificates are supported by appropriate documentation to establish the identity of an Applicant.

3.2.3.1. Individual Identity Verification for OV Code Signing Certificates

Sectigo verifies the identity and address of the Applicant in accordance with the Code Signing Baseline Requirements using:

1. Verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government issued photo ID (passport, driver's license, military ID, national ID or equivalent document type)
2. Verify the Applicant's address using a form of identification that Sectigo determines to be reliable such as a government ID, utility bill, or bank or credit card statement. Sectigo MAY rely on the same government issued ID that was used to verify the Applicant's name.

Sectigo MAY accept or require, at its discretion, other official documentation supporting an application, possibly including, but not limited to, requiring face to face verification of the Applicant's identity before an authorized agent of Sectigo, an attorney, a CPA, a Latin notary, a notary public or equivalent.

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

3.2.3.2. Individual Identity Verification for EV Code Signing Certificate

Sectigo does not issue EV Code Signing Certificates to Individual Applicants.

3.2.4. Non-Verified Subscriber Information

Notwithstanding the limited warranties provided under this document, Sectigo shall not be responsible for non-verified Subscriber information submitted to Sectigo, or the Sectigo directory or otherwise submitted with the intention to be included in a Certificate.

Information that is not verified SHALL NOT be included in certificates. For Extended Validation Code Signing Certificates, Sectigo verifies the subject elements as defined in section 7.1.4.2 of the EVG.

3.2.5. Validation of Authority

Validation of authority involves a determination of whether a person has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a Certificate. Validation of authority is dependent on the type of Certificate requested and is performed in accordance with section 3.2.7 of this document.

3.2.5.1. OV Code Signing Certificates

If the Applicant for a Certificate containing Subject Identity Information is an organization, then Sectigo SHALL use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.

Sectigo MAY use the sources listed in section 3.2.2.1 to verify the Reliable Method of Communication. Provided that a Reliable Method of Communication is used, Sectigo MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that Sectigo deems appropriate.

In addition, Sectigo SHALL establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then Sectigo SHALL NOT accept any certificate requests that are outside this specification. Sectigo SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.5.2. EV Code Signing Certificates

The request for EV Code Signing certificates is verified in accordance with the CA/B Forum Baseline Requirements For The Issuance And Management Of Publicly Trusted Code Signing Certificates section 3.2.2.2.

3.2.6. Criteria for Interoperation

Sectigo MAY provide services allowing for another CA to operate within, or interoperate with, its PKI. Such interoperation MAY include cross-certification, unilateral certification, or other forms of operation. Sectigo reserves the right to provide interoperation services and to interoperate transparently with other CAs; the terms and criteria of which are to be set forth in the applicable agreement.

All Cross Certificates that identify a Sectigo CA as the Subject are listed in the Repository, provided that Sectigo has arranged for or accepted the establishment of the trust relationship.

In addition to the repository, Sectigo MAY issue Code Signing and Timestamp Certificates that allow Application Software Suppliers to test their software with Subscriber Certificates which chain up to Sectigo's publicly trusted Root Certificates.

3.2.7. Application Validation

Prior to issuing a Certificate Sectigo employs controls to validate the identity of the Subscriber information featured in the Certificate application. Such controls are indicative of the product type.

3.3 Identification and Authentication for Re-Key Requests

Sectigo supports rekeys on:

- Replacement, which is when a Subscriber wishes to change some (or none) of the subject details in an already issued Certificate and may (or may not) also wish to change the key associated with the new Certificate; and
- Renewal, which is when a Subscriber wishes to extend the lifetime of a Certificate which has been issued, they may at the same time vary some (or none) of the subject details and may also change the key associated with the Certificate.

In both cases, Sectigo requires the Subscriber to use the same authentication details (typically username and password) which they used in the original purchase of the Certificate. In either case, if any of the subject details are changed during the replacement or renewal process then the subject must be reverified.

3.3.1. Identification and Authentication for Routine Re-Key

As stated above - in both cases, Sectigo requires the Subscriber to use the same authentication details (typically username and password) which they used in the original purchase of the Certificate. Identity MAY be established through the use of the device's current valid signature key.

3.3.2. Identification and Authentication for Re-Key after Revocation

Sectigo does not routinely permit rekeying (or any form of reissuance or renewal) after revocation. Revocation is a terminal event in the Certificate lifecycle.

Where a request for replacement or renewal of a Certificate after revocation is considered, Sectigo requires the Subscriber to authenticate itself using the original authentication details (typically username and password) used in the initial purchase of the Certificate. However, this may be varied, or rekeying may be refused after revocation, where the exact circumstances and reasons for which the Certificate was revoked are not adequately explained. Reissuance or replacement after revocation is solely at Sectigo's discretion.

3.4. Identification and Authentication for Revocation Request

Revocation at the Subscriber's request:

The Subscriber must either be in possession of the authentication details (typically username and password) to log in the correspondent site which were used to purchase the Certificate originally OR the Subscriber must be able to send an email to our abuse accounts which will be authenticated in a later stage (for example, this email can be signed with the Private Key associated with the Certificate).

Revocation at the RA's request:

The RA must be in possession of the authentication details used to effect the original Certificate request to the CA.

Revocation at the CA's request:

Sectigo does not revoke Certificates at the request of other CAs. Sectigo can and does revoke Subscriber Certificates for cause as set out in section 4.9 of this document, but identification and authentication are not required in these cases.

Sectigo employs the following procedure for authenticating a revocation request:

- The revocation request MAY be sent by the administrator contact associated with the Certificate application. Sectigo MAY, if necessary, also request that the revocation request be made by either / or

the organizational contact and billing contact.

- Upon receipt of the revocation request Sectigo will request confirmation.
- Sectigo validation personnel will then command the revocation of the Certificate and logging of the identity of validation personnel and reason for revocation will be maintained in accordance with the logging procedures covered in this document.

4. CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS

This section describes the Certificate application process, including the information required to make and support a successful application. Additionally, this section describes some of the requirements imposed upon RAs, Subscribers, and other participants with respect to the lifecycle of a Certificate.

The validity period of Sectigo Certificates varies dependent on the Certificate type, but typically, a Code Signing Certificate will be valid for either 1 year, 2 years, or 3 years. Sectigo reserves the right to, at its discretion, issue Certificates that may fall outside of these set periods.

Note: In contracts and day to day operations, Certificate Renewal, Re-key, and Modification, are all colloquially referred to using the umbrella term 'renewal'.

4.1. Certificate Application

The Certificate application process MUST provide sufficient information to: • Establish the applicant's authorization (by the employing or sponsoring organization) to obtain a Certificate. (per Section 3.2.3) • Establish and record identity of the applicant. (per Section 3.2.3) • Obtain the applicant's Public Key and verify the applicant's possession of the Private Key for each Certificate required, if the private key is generated by the applicant. (per Section 3.2.1) • Verify any role, authorization, or other subject information requested for inclusion in the Certificate.

These steps MAY be performed in any order that is convenient that does not compromise security, but all MUST be completed before Certificate issuance.

A Certificate request can be done according to the following means:

On-line: Via the Web (https). The Certificate Applicant submits an application via a secure online link according to a procedure provided by Sectigo. Additional documentation in support of the application may be required so that Sectigo verifies the identity of the Applicant. The Applicant submits to Sectigo such additional documentation. Upon verification of identity, Sectigo issues the Certificate and sends a notice to the Applicant. The Applicant must notify Sectigo of any inaccuracy or defect in a Certificate promptly after receipt of the Certificate or earlier notice of informational content to be included in the Certificate.

Sectigo may at its discretion, accept applications via email.

4.1.1. Who can Submit a Certificate Application

An authorized representative of the applicant CA shall submit an application for a CA Certificate. The Subscriber, or an RA on behalf of the Subscriber SHALL submit a Subscriber Certificate application to the CA. Multiple Certificate requests from one RA MAY be submitted as a batch.

Generally, Applicants will complete the online forms made available by Sectigo or by approved RAs at the respective official websites. Under special circumstances, the Applicant MAY submit an application via email; however, this process is available at the discretion of Sectigo or its RAs. Sectigo maintains an internal database of all previously revoked Certificates and previously rejected certificate requests. That database is used to identify subsequent suspicious certificate requests.

Sectigo does not issue Certificates to entities on a government denied list, list of prohibited persons, or other list that prohibits doing business with maintained by the US or UK or that is located in a country with which the laws of the US or UK prohibit doing business.

4.1.2. Enrollment Process and Responsibilities

All communications among PKI Authorities supporting the Certificate application and issuance process SHALL be authenticated and protected from modification; any electronic transmission of shared secrets and personally identifiable information SHALL be protected. Communications MAY be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with

the strength of the public/Private Key pair SHALL be used. Out-of-band communications SHALL protect the confidentiality and integrity of the data.

Applicants are responsible for providing accurate information on their Certificate applications. The enrollment process, for an Applicant, SHALL include the following: • Completing the Certificate Application package • Providing the requested information • Responding to authentication requests in a timely manner • Submitting required payment, where applicable

All Certificate Applicants must complete the enrollment process, which may include:

- Make all reasonable efforts to protect the integrity and confidentiality of the Private Key.
- Submit to Sectigo a Certificate application, including application information as detailed in this document, and agree to the terms of the relevant Subscriber Agreement.
- Provide proof of identity through the submission of official documentation as requested by Sectigo during the enrolment process.

4.2. Certificate Application Processing

Certificate applications are submitted to either Sectigo or a Sectigo approved RA.

Sectigo performs the applicable certificate validation procedures and as required verifies the completeness, accuracy and authenticity of the information provided by the Applicant prior to issuing a Certificate. The procedure includes:

• Verifying that the Applicant is permitted to obtain a Certificate under the relevant stipulations of this document.

• Verifying that the Applicant has executed the Subscriber Agreement;

• Validating that the requested Certificate meets the requirements in section 3.1;

• Performing the validation procedures set out in section 3.2 and the relevant subsections

4.2.1. Performing Identification and Authentication Functions

Upon receipt of an application for a digital Certificate and based on the submitted information, Sectigo confirms the following information:

- The Certificate Applicant is the same person as the person identified in the Certificate request.
- The information to be published in the Certificate is accurate, except for non-verified Subscriber information.
- Any agents who apply for a Certificate listing the Certificate Applicant's Public Key are duly authorized to do so.

Sectigo MAY use the services of a third party to confirm information on a business entity that applies for a digital Certificate. Sectigo accepts confirmation from third party organizations, other third-party databases, and government entities.

Sectigo's controls MAY also include trade registry transcripts that confirm the registration of the Applicant company and state the members of the board, the management and directors representing the company.

Sectigo MAY use any means of communication at its disposal to ascertain the identity of an organizational or individual Applicant. Sectigo reserves the right of refusal in its absolute discretion.

Sectigo has a system in place which examines subject details for matches or near matches to some known high profile or pre-notified names that may indicate that a certificate is at a higher-than-normal risk of fraudulent applications being made and in those cases the certificate application is flagged for manual review.

Prior to issuing a Code Signing Certificate, Sectigo MAY check at least one database containing information about known or suspected producers, publishers, or distributors of Suspect Code, as identified or indicated by an Anti-Malware Organization and any database of deceptive names maintained by an Application Software Provider. Sectigo maintains and checks an internal database listing Certificates revoked due to Code Signatures on Suspect Code and previous certificate requests rejected.

Sectigo performs a "due diligence" verification as specified in the EV guidelines.

4.2.2. Approval or Rejection of Certificate Applications

Following successful completion of all required validations of a Certificate application Sectigo approves an application for a digital Certificate.

If the validation of a Certificate application fails, Sectigo rejects the Certificate application. Sectigo reserves its right to reject applications to issue a Certificate to Applicants if, on its own assessment, by issuing a Certificate to such parties the good and trusted name of Sectigo might get tarnished, diminished or have its value reduced and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal. Sectigo MAY issue new or replacement Code Signing Certificates to an entity who is the victim of a documented Takeover Attack, resulting in a loss of control of the Private Key associated with their Code Signing Certificate.

Applicants whose applications have been rejected may subsequently reapply.

In all types of Sectigo Certificates, the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Sectigo of any changes that would affect the validity of the Certificate. Failure to comply with the obligations as set out in the Subscriber Agreement will result in the revocation of the Subscriber's Certificate without further notice to the Subscriber and the Subscriber shall pay any charges payable but that have not yet been paid under the Subscriber Agreement.

Sectigo does not issue new or replacement Code Signing Certificates to an entity that the CA determined intentionally signed Suspect Code. Sectigo keeps the reason for revoking a Code Signing Certificate as proof that the Code Signing Certificate was revoked because the Applicant was intentionally signing Suspect Code.

4.2.3. Time to Process Certificate Applications

Sectigo makes reasonable efforts to confirm Certificate application information and issue a digital Certificate within a reasonable time frame. The time frame is greatly dependent on the Subscriber providing the necessary details and/or documentation in a timely manner. Upon the receipt of the necessary details and/or documentation, Sectigo aims to confirm submitted application data and to complete the validation process and issue/reject a Certificate application within 2 working days.

From time to time, events outside of the control of Sectigo MAY delay the issuance process, however Sectigo will make every reasonable effort to meet issuance times and to make Applicants aware of any factors that may affect issuance times in a timely manner.

4.3. Certificate Issuance

Sectigo issues a Certificate upon approval of a Certificate application. A digital Certificate is deemed to be valid at the moment a Subscriber accepts it (refer to section 4.4 of this document). Issuing a digital Certificate means that Sectigo accepts a Certificate application.

Sectigo Certificates are issued to organizations or individuals.

Subscribers shall solely be responsible for the legality of the information they present for use in Certificates issued under this document, in any jurisdiction in which such content may be used or viewed.

4.3.1. CA Actions during Certificate Issuance

Sectigo's automated systems receive and collate:

- evidence gathered during the verification process, and/or
- assertions that the verification has been completed according to the policy and internal documentation that sets out the acceptable means of verifying subject information.

Sectigo's automated systems record the details of the business transaction associated with the submission of a Certificate request and the eventual issuance of a Certificate, one example of which is a sales process involving a credit card payment.

Sectigo's systems record the source of, and all details submitted with, evidence of verification, having been performed either by external RAs or by Sectigo's internal RA.

The correct authentication of verification evidence provided by external RAs is required before that evidence will be considered for Certificate issuance.

Sectigo´s CAs have no facility for the automated signature of certificates/CRLs/OCSPs issued/signed from its root CAs, so this activity necessarily involves manual intervention by privileged users to sign such certificates/CRLs/OCSPs. Certificate issuance by the Root CA requires an individual authorized by the CA (i.e., the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command for the Root CA to perform a certificate signing operation.

Certificate System:

- SHALL NOT backdate notBefore dates to avoid deadlines, prohibitions, or code-enforced restrictions.
- have in place pre-issuance and post-issuance mechanisms to reduce the potential mis-issuances that may occur. The use of linting tools help to achieve this goal.
- Provide OCSP services for certificates presumed to exist based on an existing precertificate including the ability to revoke such a certificate.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

Sectigo notifies Subscriber of the issuance of a Certificate either via email and/or through delivery. Delivery of Subscriber Certificates to the associated Subscriber is dependent on the Certificate product type:

Code Signing Certificates

Notification of issuance of Code Signing Certificates are delivered via email to the Subscriber using the administrator contact email address provided during the application process. The certificate is then retrieved by the Subscriber via secure connection to Sectigo servers in the case of a certificate to be installed in the customer´s HSM.

In the case of a certificate provisioned in an USB token by Sectigo, this will be delivered by post.

4.3.3. Refusal to Issue a Certificate

Sectigo reserves its right to refuse to issue a Certificate to any party as it sees fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. Sectigo reserves the right not to disclose reasons for such a refusal.

4.4. Certificate Acceptance

This section describes some of the actions by Subscriber in accepting a Certificate. Additionally, it describes how Sectigo publishes a Certificate and how Sectigo notifies other entities of the issuance of a Certificate.

Before a Subscriber can make effective use of its Private Key, Sectigo SHALL explain to the Subscriber its responsibilities and obtain the Subscriber's acknowledgement, as defined in Section 9.6.3.

4.4.1. Conduct Constituting Certificate Acceptance

A Subscriber is deemed to have accepted a Certificate when:

- the Subscriber uses the Certificate, or

- 30 days pass from the date of the issuance of a Certificate

4.4.2. Publication of the Certificate by the CA

A Certificate is published through various means: (1) by Sectigo making the Certificate available in the Repository; and (2) by Subscriber using the Certificate subsequent to Sectigo's delivery of the Certificate to Subscriber.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

The Policy Authority MUST be notified whenever a CA operating under this policy issues a CA Certificate. RAs MAY receive notification of the issuance of Certificates they approve

Other than to the Subscriber, Sectigo provides notification of Certificate issuance to certain other entities as detailed below.

4.4.3.1. Reseller Partner

Issued Subscriber Code Signing Certificates applied for through a Reseller Partner on behalf of the Subscriber are emailed to the administrator contact of the Reseller Partner account.

4.5. Key Pair and Certificate Usage

This section is used to describe the responsibilities relating to the use of keys and Certificates.

4.5.1. Subscriber Private Key and Certificate Usage

The intended scope of usage for a private key shall be specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2. Relying Party Public Key and Certificate Usage

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the Relying Party. Reliance on a digital signature should only occur if:

- the digital signature was created during the operational period of a valid Certificate and it can be verified by referencing a validated Certificate;
- the Relying Party has checked the revocation status of the Certificate by referring to the relevant CRLs and the Certificate has not been revoked;
- the Relying Party understands that a digital Certificate is issued to a Subscriber for a specific purpose and that the digital Certificate may only be used in accordance with the usages suggested in this document and named as Object Identifiers in the Certificate profile; and
- the Certificate applied for is appropriate for the application it is used in.

Reliance is accepted as reasonable under the provisions made for the Relying Party under this document and within the Relying Party agreement. If the circumstances of reliance exceed the assurances delivered by Sectigo under the provisions made in this document, the Relying Party must obtain additional assurances.

Warranties are only valid if the steps detailed above have been carried out.

4.6. Certificate Renewal

Certificate renewal means the issuance of a new Certificate to the Subscriber without changing the Subscriber's, or other participant's, Public Key or any other information in the Certificate.

Depending on the option selected during application, the validity period of Sectigo Certificates is typically 1 year, 2 years or 3 years from the date of issuance and is detailed in the relevant field within the Certificate.

Renewal fees are detailed on the official Sectigo websites and within communications sent to Subscribers approaching the Certificate expiration date.

4.6.1. Circumstance for Certificate Renewal

End entity Certificate renewal MAY be supported for Certificates where the Private Key associated with the Certificate has not been compromised. End entity Certificates MAY be renewed to maintain continuity of Certificate usage An end entity Certificate MAY be renewed after expiration. The original Certificate MAY or MAY NOT be revoked, but SHALL NOT be further re-keyed, renewed, or modified.

Sectigo shall make reasonable efforts to notify Subscribers via e-mail of the imminent expiration of a digital Certificate. Notice shall ordinarily be provided within a 60-day period prior to the expiry of the Certificate.

4.6.2. Who May Request Renewal

Those who may request renewal of a Certificate include, but are not limited to, a Subscriber on behalf of itself, and an RA on behalf of a Subscriber. Sectigo does not automatically renew Certificates.

4.6.3. Processing Certificate Renewal Requests

In order to process Certificate renewal requests, Sectigo gets the Subscriber to reauthenticate itself. Renewal application requirements and procedures are the same as those employed for the application validation and issuance requirements detailed for new customers.

4.6.4. Notification of New Certificate Issuance to Subscriber

Notification to the Subscriber about the issuance of a renewed Certificate is given using the same means as a new Certificate, described in section 4.3.2 of this document.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Subscriber's conduct constituting acceptance of a renewal Certificate is the same as listed in section 4.4.1 of this document.

4.6.6. Publication of the Renewal Certificate by the CA

Sectigo publishes a renewed Certificate by delivering it to the Subscriber. In the limited circumstances where Sectigo publishes a renewed Certificate by alternate means, Sectigo does so by using the LDAP server–a publicly accessible directory of client Certificates.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

Generally, Sectigo does not notify other entities of a renewed Certificate. In limited circumstances, Sectigo will notify other entities through the means described in section 4.6.6 of this document. Sectigo MAY also notify an RA, if the RA was involved in the renewal process.

4.7. Certificate Re-key

The section is used to describe elements/procedures generating a new Key Pair and applying for the issuance of a new Certificate that certifies the new Public Key. Rekeying (or re-keying) a Certificate MAY comprise of creating a new Certificate with a new Public Key and serial number, while retaining the Certificate's subject information.

4.7.1. Circumstances for Certificate Re-Key

Certificate rekey will ordinarily take place as part of a Certificate renewal or Certificate replacement, as stated in section 3.2 of this document. Certificates rekey MAY also take place when a key has been compromised.

Examples of circumstances requiring Certificate re-key include: expiration, loss or compromise, issuance of a new hardware token, and hardware token failure.

4.7.2. Who May Request certification of a new public key

Those who may request a certification of a new public key include, but are not limited to, the Subscriber, the RA on behalf of the Subscriber, or Sectigo at its discretion.

4.7.3. Processing Certificate Rekeying Requests

Depending on the circumstances, the procedure to process a Certificate rekey MAY be the same as issuing a new Certificate. Under other circumstances, Sectigo MAY process a rekey request by having the Subscriber authenticate its identity.

CA Certificate re-key SHALL be approved by the Policy Authority.

4.7.4. Notification of new certificate issuance to Subscriber

Sectigo will notify Subscriber of a new Certificate issuance by the means delineated in section 4.3.2 of this document.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Subscriber's conduct constituting acceptance of a rekeyed Certificate is the same as listed in section 4.4.1 of this document.

4.7.6. Publication of the Re-Keyed Certificate by the CA

Publication a rekeyed Certificate is performed by delivering it to the Subscriber.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

Generally, Sectigo does not notify other entities of the issuance of a rekeyed Certificate. Sectigo MAY notify an RA of the issuance of a rekeyed Certificate when an RA was involved in the issuance process.

4.8. Certificate Modification

Sectigo does not offer Certificate modification.

If not a renewal nor a rekey, Sectigo will issue a new Certificate with different/new subscriber´s information and new (or not) public key and MAY revoke the old Certificate.

4.9. Certificate Revocation and Suspension

Revocation of a Certificate is to permanently end the operational period of the Certificate prior to reaching the end of its stated validity period. In other words, upon revocation of a Certificate, the operational period of that Certificate is immediately considered terminated. The serial number of the revoked Certificate will be placed within the CRL and remains on the CRL until sometime after the end of the Certificate's validity period.

Sectigo specifies the revocation reasons for the certificates that have been revoked. For subscriber´s certificates only if the subscriber has provided the revocation reason, otherwise this will be unspecified.

Sectigo does not utilize Certificate suspension.

4.9.1. Circumstances for Revocation

A Certificate SHALL be revoked when the binding between the subject and the subject's Public Key defined within the Certificate is no longer considered valid. When this occurs, the associated Certificate SHALL be revoked and placed on the CRL and/or added to the OCSP responder. Revoked Certificates SHALL be included onin all new publications of the Certificate status information until the Certificates expire.

Sectigo SHALL revoke a Code Signing Certificate within 24 hours if one or more of the following occurs:

- The Subscriber requests in writing that the CA revoke the Certificate;
- The Subscriber notifies Sectigo that the original Certificate request was not authorized and does not retroactively grant authorization;
- Sectigo reasonably believes or obtains evidence that there has been loss, theft, modification, unauthorized disclosure, or other compromise of the Private Key associated with the Certificate;

- Sectigo is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate;
- Sectigo is made aware of 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, or if there is clear evidence that the specific method used to generate the Private Key was flawed;
- Sectigo reasonably believes that the Certificate was used to sign Suspect Code

Sectigo SHOULD revoke within 24 hours but MUST revoke within 5 days if one or more of the following occurs:

- The Subscriber or Sectigo has breached a material obligation under this document or the relevant Subscriber Agreement;
- The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the Code Signing Baseline Requirements;
- Either the Subscriber's or Sectigo's obligations under this document or the relevant Subscriber Agreement are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
- Sectigo is made aware of a material change in the information contained in the Certificate, or the information contained in the Certificate is inaccurate;
- A personal identification number, Private Key or password has, or is likely to become known to someone not authorized to use it, or is being or is likely to be used in an unauthorized way
- The Certificate has not been issued in accordance with the policies set out in this document;
- The Subscriber has used the Certificate contrary to law, rule or regulation, or Sectigo reasonably believes that the Subscriber is using the Certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The Certificate was issued as a result of fraud or negligence;
- Sectigo right to issue Certificates under the Code Signing Baseline Requirements expires or is revoked or terminated, unless Sectigo has made arrangements to continue maintaining the CRL/OCSP Repository; or
- The Certificate, if not revoked, will compromise the trust status of Sectigo.

Sectigo MAY delay revocation based on a request from Application Software Suppliers where immediate revocation has a potentially large negative impact to the ecosystem.

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

- The Subordinate CA requests revocation in writing;
- The Subordinate CA notifies Sectigo that the original certificate request was not authorized and does not retroactively grant authorization;
- Sectigo 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 Code Signing Baseline Requirements;
- Sectigo obtains evidence that the Subordinate CA Certificate was misused;
- Sectigo is made aware that the Subordinate CA Certificate was not issued in accordance with, or that Subordinate CA has not complied with, the Code Signing Baseline Requirements or this document;
- Sectigo determines that any of the information appearing in the Subordinate CA Certificate is inaccurate or misleading;
- Sectigo or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- Sectigo's, or Subordinate CA's, right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless Sectigo has made arrangements to continue maintaining the CRL/OCSP

Repository;
- Revocation is required by this document;
- The Subordinate CA has used the Certificate contrary to law, rule or regulation, or Sectigo reasonably believes that the Subordinate CA is using the Certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The Subordinate CA Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The Subordinate CA Certificate was issued as a result of fraud or negligence;
- The Subordinate CA Certificate, if not revoked, will compromise the trust status of Sectigo.

4.9.1.1. Code Signing Certificates

When revocation of a Code Signing Certificate is done due to a Key Compromise or use in Suspect Code, Sectigo SHALL determine an appropriate value for the revocationDate based on its own investigation. Sectigo SHALL set a historic date as revocationDate if deemed appropriate.

4.9.2. Who Can Request Revocation

A Subscriber or another appropriately authorized party can request revocation of a Certificate. An authorized party includes an RA, regardless of whether on behalf of the Subscriber may request revocation through their account. Sectigo MAY revoke a Certificate without receiving a request and without reason. Other parties may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, using the contact details set out in section 1.5.2.1 of this document.

4.9.3. Procedure for Revocation Request

Sectigo accepts and responds to revocation requests and problem reports on a 24/7 basis as indicated in section 1.5.2 of this document.

Prior to the revocation of a Certificate, Sectigo will verify that the revocation request has been:

- Made by the organization or individual entity that has made the Certificate application.
- Made by the RA on behalf of the organization or individual entity that used the RA to make the Certificate application, and
- Has been authenticated by the procedures in section 3.4 of this document.

4.9.4. Revocation Request Grace Period

The revocation request grace period ("Grace Period") means the period during which the Subscriber must make a revocation request. The Grace Period is defined in the Subscriber Agreement applicable to the individual Subscriber. In the event that a Grace Period is not defined in the Subscriber Agreement, Subscribers are required to request revocation within 24 hours after detecting the loss or compromise of the Private Key.

4.9.5. Time Within which CA Must Process the Revocation Request

Sectigo SHALL process revocation requests in accordance with CS BRs sections 4.9.1.1 and 4.9.5. Once a certificate has been revoked the revocation will be reflected in the OCSP responses issued within 1 hour, and in the CRLs within 24 hours.

Sectigo will inform the subscriber and the entity reporting the issue.

4.9.6. Revocation Checking Requirement for Relying Parties

Parties relying on a digital Certificate must verify a digital signature at all times by checking the validity of a digital Certificate against the relevant CRL published by Sectigo or using the Sectigo OCSP responder. Note that CRL MAY lag behind OCSP creating a situation where a revoked certificate MAY show as Revoked on OCSP yet MAY NOT show as revoked in the most recent CRL available. Therefore, it is recommended to

obtain revocation information from Sectigo's OCSP responder whenever possible. Relying parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the Subscriber.

Sectigo MAY specify the time at which the Certificate is first considered to be invalid in the revocationDate field of a CRL entry or the revocationTime field of an OCSP response to time-bind the set of software affected by the revocation , and software should continue to treat objects containing a timestamp dated before the revocation date as valid.

Relying on an unverifiable digital signature may result in risks that the Relying Party, and not Sectigo, assume in whole.

By means of this document, Sectigo has adequately informed relying parties on the usage and validation of digital signatures through this document and other documentation published in the Repository or by contacting via out of bands means via the contact address as specified in the Document Control section of this document.

4.9.7. CRL Issuance Frequency

Sectigo publishes CRLs to allow relying parties to verify a digital signature made using a Sectigo issued digital Certificate. Each CRL contains entries for all revoked un-expired Certificates issued.

For the status of Subscriber Certificates:

Sectigo issues a new CRL at least once every seven (7) days, and the value of the nextUpdate field MUST NOT be more than ten (10) days beyond the value of the thisUpdate field. Sectigo includes a monotonically increasing sequence number for each CRL issued.

For the status of Subordinate CA Certificates:

Sectigo updates and reissues CRLs at least

- once every twelve (12) months and
- within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field MUST NOT be more than twelve months beyond the value of the thisUpdate field.

For the status of Timestamp Certificates:

Sectigo updates and reissues CRLs at least

1. once every twelve (12) months and
2. within 24 hours after revoking a Timestamp Certificate, and the value of the nextUpdate field MUST NOT be more than twelve months beyond the value of the thisUpdate field.

Under special circumstances, Sectigo MAY publish new CRLs prior to the expiry of the current CRL. All expired CRLs are archived (as described in section 3.4 of this document) for a period of 7 years or longer if applicable. For Code Signing Certificates revoked due to key compromise or that have been issued to unauthorized persons, Sectigo will maintain Certificate information on CRLs for at least 10 years.

4.9.8. Maximum Latency for CRLs

Each CRL SHALL be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

The maximum latency for CRLs means the maximum time between the generation of CRLs and posting of the CRLs to the repository (i.e., the maximum number of processing- and communication-related delays in posting CRLs to the repository after the CRLs are generated). Sectigo does not employ a maximum latency for CRLs. Generally, however, CRLs are published within 1 hour.

4.9.9 On-Line Revocation/Status Checking Availability

In addition, Certificate System is configured to generate and serve OCSP responses. This provides real-time information regarding the validity of the Certificate making the revocation information immediately available through the OCSP protocol. CRLs and OSCP are available 24/7 to anyone.

OCSP responses conform to RFC6960 and/or RFC5019.

4.9.10. On-Line Revocation Checking Requirements

OCSP responders operated by Sectigo SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

Sectigo's OCSP responses are either:

- Signed by the CA that issued the Certificates whose revocation status is being checked, or;
- The OCSP response is signed by a separate OCSP Responder Certificate which is signed by the CA that issued the Certificate whose revocation status is being checked. In this case the signing certificate will contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

For the status of Code Signing Certificates, Sectigo SHALL update information provided via an Online Certificate Status Protocol

- At least every 4 days
- have a validity interval less than or equal to ten days;
- Sectigo SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.

For the status of Subordinate CA Certificates, Sectigo SHALL update information provided via an Online Certificate Status Protocol

- 1. at least every twelve months; and
  2. within 24 hours after revoking a Subordinate CA Certificate.

For the status of Timestamp Certificates, Sectigo SHALL update information provided via an Online Certificate Status Protocol

1. at least every twelve months; and
2. within 24 hours after revoking a Timestamp Certificate.

A certificate serial number within an OCSP request is "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject.

Sectigo´s OCSP responder does not respond with a "good" status when receives a request for the status of a certificate serial number that is not "assigned".

Relying parties must perform online revocation/status checks in accordance with section 4.9.6 of this document prior to relying on the Certificate.

4.9.11. Other Forms of Revocation Advertisements Available

Because some Application Software Suppliers utilize non-standard revocation mechanisms, Sectigo MUST, if requested by the Application Software Supplier and using a method of communication specified by the Application Software Vendor, notify the Application Software Supplier whenever Sectigo revokes a Code Signing Certificate because (i) the CA mis-issued the Certificate, (ii) the Certificate was used to sign Suspect Code, or (iii) there is a suspected or actual compromise of the Applicant's or CA's Private Key.

4.9.12. Special Requirements for Key Compromise

In the event of Compromise or suspected Compromise of the CA signing key, the Sectigo Policy Authority SHALL be immediately notified.

Sectigo offers some methods for reporting key compromise:

- https://secure.sectigo.com/products/RevocationPortal
- ACME Directory: https://acme.sectigo.com/v2/keyCompromise
- revokeCert API: https://acme.sectigo.com/v2/keyCompromise/revokeCert

4.9.13. Circumstances for Suspension

No stipulation.

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

CRL and OCSP are Certificate status checking services available to relying parties.

4.10.1. Operational Characteristics

Lightweight OCSP conforms to RFC 5019. Sectigo provides revocation information for Certificates through 1 day after the expiry date of the Certificate, except for Code Signing Certificates where Sectigo provides revocation information past the expiry date.

Revocation entries on an OCSP response MUST remain for the same amount of time as for the CRL entries, as described in Section 7.2.

Revocation entries on a CRL or OCSP Response SHALL NOT be removed until after the Expiry Date of the revoked Certificate

4.10.2. Service Availability

Certificate status services are available 24/7.

Sectigo operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

4.10.3. Optional Features

No stipulation.

4.11. End of Subscription

A Subscriber's subscription service ends if:

- Sectigo ceases operation,
- All of Subscriber's Certificates issued by Sectigo are revoked without the renewal or rekey of the Certificates, or
- The Subscriber's Subscriber Agreement terminates or expires without renewal.

4.12. Key Escrow and Recovery

In general, Sectigo does not provide key escrow or key backup services. Sectigo expects an Applicant to generate key-pairs in its own environment and to pass only the Public Key to Sectigo for inclusion in the Certificates issued.

In certain enterprise scenarios, where specifically provided for by contract between Sectigo and the Subscriber enterprise, Sectigo provides key escrow for Certificates.

4.12.1. Key Escrow and Recovery Policy and Practices

An escrowed Private Key can only be recovered after Sectigo confirms the authority of the party requesting the Private Key. Private Keys MAY only be recovered for lawful and legitimate purposes. Sectigo recommends to its Certificate Manager users that they notify their customers and Subscribers that their Private Keys are escrowed, that they protect escrowed keys from unauthorized disclosure, and that they do not disclose or allow to be disclosed any escrowed keys or (escrowed) key-related information to a third party unless required by law. Certificate Manager users are required to revoke the Certificate associated with an escrowed Private Key prior to retrieving the escrowed key from Sectigo.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This section outlines the security policy, physical access control mechanisms, service levels and personnel policy in use to provide trustworthy and reliable CA operations.

Sectigo asserts that it makes every reasonable effort to detect and prevent material breaches, loss, damage or compromise of assets, and interruption to business activities.

All CA and RA equipment, SHALL be protected from theft, loss, and unauthorized access at all times.

5.1. Physical Controls

All sites operate under a security policy designed to provide reasonable assurance of the detection, deterrence and prevention of unauthorized logical or physical access to CA related facilities.

All of the physical control requirements specified below apply equally to the Root and Sub-CAs, and any remote workstations used to administer the CAs, except where specifically noted.

5.1.1. Site Location and Construction

Sectigo operates within the United Kingdom and the United States, with separate operations, research & development and server operation sites. Physical barriers are used to segregate secure areas within buildings and are constructed so as to extend from real floor to real ceiling to prevent unauthorized entry. External walls of the site are of solid construction.

All Sectigo CA systems are be located within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CA, SHALL be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, SHALL provide robust protection against unauthorized access to the CA equipment and records. Such environments are based in part on the establishment of physical security tiers. A tier is a barrier such as a locked door or closed gate that provides mandatory Access Control for individuals and requires a positive response (e.g., door unlocks or gate opens) for each individual to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorized access. Moreover, each physical security tier encapsulates the next inner tier, such that an inner tier MUST be fully contained in an outside tier and cannot have a common outside wall with the outside tier, the outermost tier being the outside barrier of the building (e.g., a perimeter fence or outside wall). Sectigo´s facilities housing their operational and standby CA functions have at least four physical security tiers. Sectigo performs all validation operations within Tier 2 or higher. Sectigo places Information Services systems necessary to support CA functions in Tier 4 or higher. Online and offline cryptographic modules SHALL only be activated for signing when in Tier 4 or higher.

5.1.2. Physical Access

Access to each tier of physical security, constructed in accordance with section 5.1.1, SHALL be controlled.

Card access systems are in place to control and monitor access to all areas of the facility. Access to the Sectigo physical machinery within the secure facility is protected with locked cabinets and logical access controls. Security perimeters are clearly defined for all Sectigo locations. All of Sectigo's entrances and exits are secured or monitored by security personnel, reception staff, or monitoring/control systems.

All physical access to Sectigo PKI facilities is restricted to authorized Sectigo employees, vendors, and contractors, for whom access is required in order to execute their jobs.

RA equipment SHALL be protected from unauthorized access while the RA cryptographic module is installed and activated. The RA SHALL implement physical Access Controls to reduce the risk of equipment

tampering even when the cryptographic module is not installed and activated. These security mechanisms SHALL be commensurate with the level of threat in the RA equipment environment.

5.1.3. Power and Air Conditioning

Sectigo secure facilities have a primary and secondary power supply and ensure continuous, uninterrupted access to electric power. Heating/air ventilation systems are used to prevent overheating and to maintain a suitable humidity level.

The Sectigo´s facilities have backup capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The repositories (containing CA Certificates and CRLs) SHALL be provided with uninterrupted power sufficient for a minimum of six (6) hours of operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4. Water Exposures

Sectigo has made reasonable efforts to ensure its secure facilities are protected from flood and water damage. Sectigo has personnel located on-site to reduce the extent of damage from a flood and any subsequent water exposure.

5.1.5. Fire Prevention and Protection

Sectigo has made reasonable efforts to ensure its secure facilities are protected from fire and smoke damage (fire protection is made in compliance with local fire regulations). IT equipment is located to reduce the risk of damage or loss by fire. The level of protection from fire reflects the importance of the equipment.

These measures SHALL meet all local applicable safety regulations.

5.1.6. Media Storage

Amongst other ways, Sectigo protects media by storing it away from known or obvious fire/water hazards. Media is also backed up on-site and off-site.

Media containing Private Key material SHALL be handled, packaged, and stored in a manner compliant with the requirements for the sensitivity level of the information it protects or to which it provides access. Storage protection of CA and RA Private Key material SHALL be consistent with stipulations in Section 5.1.2.

5.1.7. Waste Disposal

Sectigo disposes of waste in accordance with industry best practice. Sectigo has procedures in place to dispose of all media types, including, but not limited to, paper documents, hardware, damaged devices, and read only optical devices. These procedures apply to all information classification levels, with the method of disposal dependent on the classification.

Sensitive media and paper SHALL be destroyed in accordance with the applicable policy for destruction of such material. Destruction of media and documentation containing sensitive information, such as Private Key material, SHALL employ methods commensurate with those in NIST Special Publication 800-88.

5.1.8. Off-Site Backup

Sectigo backs up much of its information to a secure, off-site location that is sufficiently distant to escape damage from a disaster at the primary location. The frequency, retention, and extent of the backup is determined by the infrastructure team, taking into account the criticality and security requirements of the information. Backup of critical CA software is performed weekly and is stored offsite. Backup of critical business information is performed daily and is stored offsite. Access to backup servers/media is restricted to authorized personnel only. Backup media is regularly tested through restoration to ensure it can be relied on in the event of a disaster. Backup servers/media is appropriately labeled according to the confidentiality of the information.

5.2. Procedural Controls

5.2.1. Trusted Roles

Sectigo has defined Trusted Roles for the personnel who design, build, develop, implement, operate, and maintain its CA Infrastructure and Network Equipment. Each Trusted Role has its responsibilities, privileges, and access documented.

Trusted roles are assigned by senior members of the management team who decide permissions on the "principle of least privilege" basis through a formal authorization process with authorizations being archived.

The list of personnel appointed to Trusted Roles is maintained and reviewed annually.

The functions and duties performed by persons in Trusted Roles are distributed so that a lone person cannot subvert the security and trustworthiness of PKI operations. All personnel in Trusted Roles must be free from conflicts of interest that might prejudice the impartiality of Sectigo PKI operations. Sectigo ensures personnel assigned to a Trusted Role act only within the scope of their Trusted Role(s) when performing responsibilities, using privileges, or using access assigned to that Trusted Role.

Persons acting in Trusted Roles are only allowed to access a CMS after they are authenticated using a method approved as being suitable for the control of PIV-I Hardware.

The CA MUST ensure personnel assigned to Trusted Roles that are authorized to access or authenticate to CA Infrastructure and/or Network Equipment use unique authentication credentials created by or assigned to the authorized individual.

5.2.1.1. CA Administrators

The CA Administrator installs and configures the CA software, including key generation, and key backup (as part of key generation) and subsequent recovery.

CA Administrators do not issue certificates to Subscribers.

5.2.1.2. CA Officers (e.g., CMS, RA, Validation and Vetting Personnel)

The CA Officer role is responsible for issuing and revoking certificates, the verification of identity, and compliance with the required issuance steps including those defined in this document and recording the details of approval and issuance steps taken identity vetting tasks are completed.

CA Officers must identify and authenticate themselves to systems before access is granted. Identification is via a username, with authentication requiring a password and digital Certificate.

5.2.1.3. Operator (e.g., System Administrators/ System Engineers)

Operators install and configure system hardware, including servers, routers, firewalls, and networks. The Operator also keeps CA, CMS and RA systems updated with software patches and other maintenance needed for system stability, security, and recoverability.

5.2.1.4. Internal Auditors

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if Sectigo, an external CA, or RA is operating in accordance with this document and, where relevant, an RA's contract.

5.2.2. Number of Persons Required per Task

Multiparty control procedures are designed to ensure that at a minimum, the desired number of Trusted Persons are present to gain either physical or logical access to the CA equipment. Access to Certificate

Systems SHALL be defined and assigned to multiple Trusted Persons. Access to CA Root Systems SHALL be strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction.

Sectigo requires that at least two CA Administrators take action for: • Physical Access; • CA key generation; • CA signing key activation; and • CA Private Key backup and restore.

Where multiparty control is required, at least one of the participants SHALL be an Administrator. All participants MUST serve in a Trusted Role as defined in Section 5.2.2. Multiparty control SHALL NOT be achieved using personnel that serve in the Internal Auditors Trusted Role.

Sectigo requires that at least two CA Administrators take action to activate Sectigo's CA Private Keys for signing, to generate new CA key-pairs, or to restore Private Keys.

No single person has the capability to issue a PIV-I credential, or to issue an EV Code-signing certificate.

For EV Code Signing Certificates, once verification is complete, a Sectigo validation employee who was not responsible for the collection of information will review and evaluate the corpus of information and performs the final cross-correlation and due diligence.

5.2.3. Identification and Authentication for Each Role

Sectigo SHALL confirm the identity and authorization of all personnel seeking to become Trusted Persons before such personnel are: • Issued access devices and granted access to the required facilities; • Given electronic credentials to access and perform specific functions on CA systems.

Authentication of identity SHALL include the personal (physical) presence of such personnel before Trusted Persons performing HR or security functions within an entity and a check of well recognized forms of identification, such as passports and driver's licenses. Identity SHALL be further confirmed through background checking procedures in Section 5.3.

All personnel are required to authenticate themselves to CA and RA systems before they may perform the duties of their role involving those systems.

CA Private Keys can only be backed up, stored, and recovered by personnel in Trusted Roles using, at least, dual control in a Physically Secure Environment.

5.2.4. Roles Requiring Separation of Duties

Individual CA personnel SHALL be specifically designated to the roles defined in Section 5.2.1 above as applicable. Individuals MAY NOT assume more than one role, except Operator.

Individuals serving as Security Auditors shall not perform or hold any other Trusted Role.

Only an individual serving in a Security Auditor role may perform internal auditing functions, with the exception of those security audit functions (e.g., configuring, archiving, deleting) that require Multi-Party Control.

An individual that performs any Trusted Role shall only have one identity when accessing CA equipment.

5.3. Personnel Controls

Access to the secure parts of Sectigo's facilities is limited using physical and logical access controls and is only accessible to appropriately authorized individuals filling Trusted Roles for which they are properly qualified and to which they have been appointed by management.

Sectigo requires that all personnel filling Trusted Roles are properly trained and have suitable experience before being permitted to adopt those roles.

5.3.1. Qualifications, Experience, and Clearance Requirements

Consistent with this document, Sectigo follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties.

All persons filling Trusted Roles SHALL be selected based on loyalty, trustworthiness, and integrity, and SHALL be subject to a background investigation. Personnel appointed to Trusted Roles shall: • Possess the expert knowledge, experience and qualifications necessary for the offered services and appropriate job function; • Have successfully completed an appropriate training program; • Have demonstrated the ability to perform their duties; • Be trustworthy; • Have no other duties that would interfere or conflict with their duties for the Trusted Role; • Have not been previously relieved of duties for reasons of negligence or non-performance of duties; • Have not been convicted of a serious crime or other offense which affects his/her suitability for the position; and • Have been appointed in writing by the CA management.

The Operator Role is only granted on Sectigo IT systems when there is a specific business need. New Operators are not given full administrator rights until they have demonstrated a detailed knowledge of Sectigo IT systems & policies and that they have reached a suitable skill level satisfactory to the Server Systems Manager/Administrator or CEO. New administrators are closely monitored by the Server Systems Manager/Administrator for the first three months. Where systems allow, administrator access authentication is via a public/Private Key specifically issued for this purpose. This provides accountability of individual administrators and permits their activities to be monitored.

The CA Officer Role is granted certificate issuance privileges only after sufficient training in Sectigo's validation and verification policies and procedures. This training period MUST be at least six months before issuance privileges will be granted for EV Code Signing certificates.

5.3.2. Background Check Procedures

All trusted personnel, except those working for external RAs, have background checks before access is granted to Certificate System. These checks may include, but are not limited to, verification of the individual's identity using a government issued photo ID, credit history, employment history, education, character references, social security number, criminal background, and a Companies House cross-reference to disqualified directors.

5.3.3. Training Requirements

Sectigo provides suitable training to all staff before they take on a Trusted Role should they not already have the complete skill-set required for that role. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached.

Training SHALL be conducted in the following areas: • CA or RA security principles and mechanisms; • All PKI software versions in use on the CA or RA system; • All PKI duties they are expected to perform; • Incident and Compromise reporting and handling • Disaster recovery and business continuity procedures; and • Stipulations of this document.

CA Administrators are trained in the operation and installation of CA software.

Operators are trained in the maintenance, configuration, and use of the specific software, operating systems, and hardware systems used by Sectigo.

Internal Auditors are trained to proficiency in the general principles of systems and process audit as well as familiarity with Sectigo's policies and procedures.

CA Officers are trained in Sectigo's validation and verification policies and procedures and are required to pass an examination on the applicable information validation and verification requirements.

Sectigo maintains records of who received training.

5.3.4. Retraining Frequency and Requirements

Sectigo SHALL provide refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily. All individuals responsible for PKI roles SHALL be made aware of changes in the CA operation. Any significant change to the operations SHALL have a training (awareness) plan, and the execution of such plan SHALL be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment. Documentation SHALL be maintained identifying all personnel who received training and the level of training completed.

Personnel in Trusted Roles have additional training when changes in industry standards or changes in Sectigo's operations require it. Sectigo provides refresher training and informational updates sufficient to ensure that Trusted Personnel retain the requisite degree of expertise.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

Any personnel who, knowingly or negligently, violate Sectigo's security policies, exceed the use of their authority, use their authority outside the scope of their employment, or allow personnel under their supervision to do so may be liable to disciplinary action up to and including termination of employment. Should the unauthorized actions of any person reveal a failure or deficiency of training, sufficient training or retraining will be employed to rectify the shortcoming.

5.3.7. Independent Contractor Requirements

Sectigo SHALL permit independent contractors or consultants to become Trusted Persons only to the extent necessary to accommodate clearly defined outsourcing relationships. Sectigo SHOULD only use contractors or consultants as Trusted Persons if there are not suitable employees available to fill the roles of Trusted Persons. Independent contractors and consultants SHALL be escorted and directly supervised by Trusted Persons when they are given access to the CA and its secure facility.

Independent contractors must meet the same training requirements as Sectigo employees working in the same role.

Once the independent contractor completes the work for which it was hired, or the independent contractor's employment is terminated, all access rights assigned to that contractor are removed as soon as possible and within 24 hours, except for external RA users, from the time of termination.

5.3.8. Documentation Supplied to Personnel

Sectigo SHALL give their personnel the requisite training and documentation needed to perform their job responsibilities competently and satisfactorily.

The selection of documentation supplied to Sectigo personnel is based on the role(s) they are to fill. Such documentation may include a copy of this document and the Code Signing BR and other technical and operational documentation necessary to maintain Sectigo's CA operations.

5.4. Audit Logging Procedures

For audit purposes, Sectigo maintains electronic or manual logs of the following events for core functions.

5.4.1. Types of Events Recorded

5.4.1.1. Types of events recorded for CAs

An audit log is maintained of each movement of the removable media.

CA & Certificate Lifecycle Management Events:

- CA Root signing key functions, including key generation, backup, storage, archival, recovery and destruction
- Subscriber Certificate lifecycle management, including successful and unsuccessful Certificate applications, Certificate issuances, Certificate re-issuances and Certificate renewals Subscriber Certificate revocation requests, including revocation reason
- Subscriber changes of affiliation that would invalidate the validity of an existing Certificate
- CRL updates, generations and issuances
- Signing of OCSP responses
- Custody of keys and of devices and media holding keys
- Compromise of a Private Key
- Certificate profiles

Security Related Events:

- System downtime, software crashes and hardware failures
- CA system actions performed by Sectigo personnel, including software updates, hardware replacements and upgrades
- Cryptographic hardware security module events, such as usage, de-installation, service or repair and retirement
- Successful and unsuccessful Sectigo PKI access attempts
- Secure CA facility visitor entry and exit

Certificate Application Information:

- The documentation and other related information presented by the Applicant as part of the application validation process
- Storage locations, whether physical or electronic, of presented documents

All logs include the following elements:

- Date and time of entry
- Identity of entity making log entry
- Description of the entry

5.4.1.2. Types of events recorded for TSAs

The Timestamp Authority MUST log the following information and make these records available to its Qualified Auditor as proof of the Timestamp Authority's compliance with these Requirements:

1. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server,
2. History of the timestamp server configuration,
3. Any attempt to delete or modify timestamp logs,
4. Security events, including:
    a. Successful and unsuccessful Timestamp Authority access attempts;
    b. Timestamp Authority server actions performed;
    c. Security profile changes;
    d. System crashes and other anomalies; and
    e. Firewall and router activities;
5. Revocation of a timestamp certificate,
6. Major changes to the timestamp server's time, and
7. System startup and shutdown.

5.4.2. Frequency of Processing Log

Logs are archived by the system administrator on a weekly basis and event journals reviewed on a weekly basis by CA management.

5.4.3. Retention Period for Audit Log

Audit logs SHALL be retained for a minimum of two (2) years.

Those are:

- CA certificate and key lifecycle management event records (as set forth in Section 5.4.1) after the later occurrence of:
  - the destruction of the CA Private Key; or
  - the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;
- Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1) after the revocation or expiration of the Subscriber Certificate.
- Any security event records (as set forth in Section 5.4.1) after the event occurred.
- Timestamp Authority data records after the revocation or renewal of the Timestamp Certificate Private Key

5.4.4. Protection of Audit Log

Only CA Administrators have the system level access required to modify or delete logs.

Both current and offsite archived logs are maintained in a form that prevents unauthorized modification, substitution or destruction.

5.4.5. Audit Log Backup Procedures

All logs are backed up on a daily basis and archived to an off-site location on a weekly basis.

All logs are backed up on separate local servers and transferred off-site over encrypted VPN to remote servers.

5.4.6. Audit Collection System (Internal vs. External)

Automatic audit collection processes run from system startup to system shutdown under the control of the Trusted Roles. The failure or alert of the audit collection system which may adversely affect the integrity of the system or the confidentiality of the information protected by the system will lead to Sectigo's Operators and/or CA Administrators evaluating whether a suspension of operations is required until the problem is remedied.

Sectigo ensures that Trusted Roles create and follow an incident response plan for all legitimate alerts.

5.4.7. Notification to Event-Causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

A vulnerability is a weakness in the organization or in an information system that might be exploited by a threat, with the possibility of causing harm to assets. In order to mitigate the risk or possibility of causing harm to assets, Sectigo performs regular vulnerability assessment by taking a two-pronged approach. Sectigo assesses vulnerabilities by (1) making an assessment of the threats to, impacts on, and the vulnerabilities of assets and the likelihood of their occurrence, and (2) by developing a process of selecting and implementing security controls in order to reduce the risks identified in the Risk Assessment to an acceptable level. Sectigo routinely performs vulnerability assessments by identifying the vulnerability

categories that face an asset. Some of the vulnerability categories that Sectigo evaluates are technical, logical, human, physical, environmental, and operational.

Vulnerability scans are run by Sectigo trusted staff on a quarterly schedule. Additional scans are run following system updates, changes, or when deemed necessary.

Sectigo will triage any critical vulnerability within a period of 48 hours after its discovery. If a Critical Vulnerability is discovered, not previously addressed, Sectigo will do in the next 96 hours one of the following:

- remediate the Critical Vulnerability
- If not possible in the 96 hours assigned, create and implement a plan to mitigate this Critical Vulnerability
- document the factual basis for which Sectigo thinks that the Critical Vulnerability does not require remediation

Sectigo employs external parties to perform regular annual vulnerability scans & penetration testing on our Certificate System/infrastructure.

In more detail • Patches, packages, & updates, however identified, with a critical risk rating shall be patched within 5 days. This timeline may be reduced if the vulnerability has a high likelihood of posing a risk to Sectigo. • Patches, packages, & updates, however identified, with a high-risk rating shall be patched within 90 days. • Patches, packages, & updates, however identified, with a medium or low risk rating do not have defined patching timelines and are uniquely evaluated.

5.5. Records Archival

Sectigo implements a backup standard for all business-critical systems located at its data centers. Sectigo retains records in electronic or in paper-based format in conformance with this subsection of this document.

5.5.1. Types of Records Archived

Sectigo backs up both application and system data. Sectigo SHALL archive the following information:

- Audit data, as specified in section 5.4 of this document;
- Certificate application information;
- Documentation supporting a Certificate application;
- Certificate lifecycle information.

5.5.2. Retention Period for Archive

The retention period for archived information depends on the type of information, the information's level of confidentiality, and the type of system the information is stored on.

Sectigo retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof for a term of not less than 2 years after any Certificate based on that documentation ceases to be valid, or as necessary to comply with applicable laws. The retention term begins on the date of expiration or revocation. Copies of Certificates are held, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that Sectigo MAY see fit.

User data backed up from a Workstation is retained for a minimum period of 6 months.

5.5.3. Protection of Archive

Records are archived at a secure off-site location and are maintained in a form that prevents unauthorized modification, substitution or destruction. Access to backup servers and/or backup media, whether Windows or Linux, backup utilities, or backup data, is restricted to authorized personnel only and adheres to a strict default deny policy.

5.5.4. Archive Backup Procedures

Electronic information SHALL be incrementally backed up on a daily basis and perform full backups on a weekly basis.

Administrators at each Sectigo location are responsible for carrying out and maintaining backup activities. Sectigo employs both scheduled and unscheduled backups. Scheduled backups are automated using approved backup tools. Scheduled backups are monitored using automated tools. Unscheduled backups occur before carrying out major changes to critical systems and are part of any change request that has a possible impact on data integrity or security. All backup media is labeled according to the information classification, which is based on the backup information stored on the media.

5.5.5. Requirements for Time-Stamping of Records

Sectigo archive records SHALL be automatically time-stamped as they are created. System clocks used for time-stamping SHALL be maintained in synchrony with an authoritative time standard.

Records that are time-stamped include, but are not limited to, the following:

- Visitor entry,
- Visitor exit,
- Emails within Sectigo,
- Emails sent between Sectigo and third parties,
- Subscriber Agreements,
- Certificate issuance, and
- Certificate revocation.

5.5.6. Archive Collection System (Internal or External)

Sectigo's archive collection system is both internal and external. As part of its internal collection procedures, Sectigo MAY require Subscribers to submit appropriate documentation in support of a Certificate application.

As part of Sectigo's external collection procedures, RAs MAY require documentation from Subscribers to support Certificate applications, in their role as a Sectigo RA. In such circumstances, RAs are obliged to retain such records in line with the practices of record retention and protection as used by Sectigo and as stated in this document.

5.5.7. Procedures to Obtain and Verify Archive Information

Sectigo RAs are required to submit appropriate documentation as detailed in the Reseller Partner agreements and EPKI Manager Account Holder agreement, and prior to being validated and successfully accepted as an approved Sectigo RA.

5.6. Key Changeover

Towards the end of each root or subCA's lifetime, a new CA signing Key Pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both keys may be concurrently active.

When a CA Certificate is rekeyed only the new key is used to sign Certificates from that time on. If the old Private Key is used to sign OCSP responder Certificates or CRLs that cover Certificates signed with that key, the old key SHALL be retained and protected.

The corresponding new CA Public Key Certificate is provided to Subscribers and relying parties through the delivery methods detailed below.

Sectigo makes all its CA Root Certificates available in the Repository.

Sectigo provides the full Certificate chain to the Subscriber upon issuance and delivery of the Subscriber Certificate.

5.7. Compromise and Disaster Recovery

Organizations are regularly faced with events that may disrupt their normal business activities or may lead to loss of information and assets. These events may be the result of natural disasters, accidents, equipment failures, or deliberate actions. This section details the procedures Sectigo employs in the event of a compromise or disaster.

5.7.1. Incident and Compromise Handling Procedures

All incidents (including compromises), both suspected and actual, are reported to the appropriate authority for investigation. Depending on the nature and immediacy of the incident, the reporter of an incident is to document the incident details to help with incident assessment, investigation, solution, and future operational changes. Once the incident is reported, the appropriate authority makes an initial assessment. Next, a containment strategy is chosen and implemented. After an incident has been contained, eradication is necessary to eliminate components of the incident. During eradication, importance is given to identifying all affected areas so they can be remedied.

These procedures are in place to ensure that:

- a consistent response to incidents happening to Sectigo's assets,
- incidents are detected, reported, and logged, and
- clear roles and responsibilities are defined.

To maintain the integrity of its services Sectigo implements, documents, and periodically tests appropriate contingency and disaster recovery plans and procedures. These procedures define and contain a formal incident management reporting process, incident response, and incident escalation procedures to ensure professional incident management and the return to normal operations within a timely manner as defined in our Information Security Management System. The process also enables incidents to be analyzed in a way as to identify possible causes such that any weaknesses in Sectigo's processes may be improved in order to prevent reoccurrence. Such plans are revised and updated as may be required at least once a year.

5.7.2. Computing Resources, Software, and/or Data are Corrupted

If Sectigo determines that its computing resources, software, or data operations have been compromised, Sectigo will investigate the extent of the compromise and the risk presented to affected parties. Depending on the extent of the compromise, Sectigo reserves the right to revoke affected Certificates, to revoke entity keys, to provide new Public Keys to users, and to recertify subjects.

5.7.3. Entity Private Key Compromise Procedures

Due to the nature of the CA Private Keys, these are classified as highly critical to Sectigo's business operations and continuity. If any of the CA's private signing keys were compromised or were suspected of having been compromised, Sectigo would make an assessment to determine the nature and extent of the compromise. In the most severe circumstances, Sectigo would revoke all Certificates ever issued by the use of those keys, notify all owners of Certificates (by email) of that revocation, and offer to re-issue the Certificates to the customers with an alternative or new private signing key. In addition, Sectigo SHALL notify all Application Software Suppliers of a CA Private Key compromise.

5.7.4. Business Continuity Capabilities after a Disaster

Sectigo operates a fully redundant CA system. In the event of a short- or long-term loss of an office location, operations at other offices will be increased. The backup CA is readily available in the event that the primary CA should cease operation. All of Sectigo's critical computer equipment is housed in a co-location facility run by a commercial data-center, and all of the critical computer equipment is duplicated within the facility. Incoming power and connectivity feeds are duplicated. The duplicate equipment is ready to take over the

role of providing the implementation of the CA, and allows Sectigo to specify a maximum system outage time (in case of critical systems failure) of 1 hour. Sectigo operations are distributed across several sites worldwide. All sites offer facilities to manage the lifecycle of a Certificate, including but not limited to the application, issuance, revocation and renewal of such Certificates. As well as a fully redundant CA system, Sectigo maintains provisions for the activation of a backup CA and a secondary site should the primary site suffer a total loss of systems. This disaster recovery plan states that Sectigo will endeavor to minimize interruptions to its CA operations.

5.8. CA or RA Termination

In case of termination of CA operations for any reason whatsoever, Sectigo will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, Sectigo will take the following steps, where possible:

- Providing Subscribers of valid Certificates, Relying Parties, and other affected parties with ninety (90) days' notice of its intention to cease acting as a CA.
- Revoking all Certificates that are still un-revoked or un-expired at the end of the ninety (90) day notice period without seeking Subscriber's consent.
- Giving timely notice of revocation to each affected Subscriber.
- Making reasonable arrangements to preserve its records according to this document.
- Reserving its right to provide succession arrangements for the re-issuance of Certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as Sectigo's.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

6. TECHNICAL SECURITY CONTROLS

This section addresses certain technological aspects of the Sectigo infrastructure and PKI services.

Sectigo is not involved in functions associated with the generation, issuance, decommissioning or destruction of a Subscriber Key Pair, other than from suitably enabled enterprise accounts operated through the Sectigo Certificate Manager service which provide Key Pair generation.

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

6.1.1.1. Subscriber Key Pairs

Key pairs for Code Signing Certificates SHALL be generated, stored and used in a crypto module that meets or exceeds the requirements of FIPS 140-2 level 3 or Common Criteria EAL 4+. Acceptable methods of satisfying this requirement include (but are not limited to) the following:

- Sectigo ships a suitable hardware crypto module, with a preinstalled Key Pair, in the form of a smartcard or USB device or similar
- The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate or manufacturers key indicating that the subscriber key is managed in a suitable hardware module,
- The Subscriber provides a suitable IT audit indicating that its operating environment achieves a level of security at least equivalent to that of FIPS 140-2 level 3 or Common Criteria EAL 4+.
- Where the Subscriber is generating, managing and/or storing keys in Cloud providers, the subscriber must provide sufficient evidence to prove that all end entity Key Pairs have been generated and stored in a FIPS 104-2 level 3 or Common Criteria EAL 4+ certified Hardware crypto module.

Sectigo SHALL reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in the CS BRs, Section 6.1.5 and/or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. Sectigo is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. Sectigo has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1;
5. Sectigo is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see *https://wiki.debian.org/SSLkeys*).

6.1.1.2. CA and subCA Key Pairs

For Root CA Key Pairs created under this document, Sectigo:

- prepares and follows a Key Generation Script,
- has a Qualified Auditor witness the Root CA Key Pair generation process or records a video of the entire Root CA Key Pair generation process, and
- has a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

For other CA Key Pairs created for Sectigo or an Affiliate, Sectigo:

- prepares and follows a Key Generation Script and
- has a Qualified Auditor witness the Root CA Key Pair generation process or records a video of the entire Root CA Key Pair generation process.

Sectigo's CA keys are generated in Hardware Security Modules (HSM)s that SHALL be compliant, as a minimum, to FIPS 140-2 level 3 or Common Criteria EAL 4+. CA keys are never available outside the HSM or key ceremonies in plain text form. All CA key operations are performed within the security of the HSM, whether this be the initial key generation or their end use in the live production environment. All keys that are exported from the HSM are encrypted with a suitable encryption algorithm with the encryption key generated by the HSM.

Access to CA keys is restricted to authorized, trusted personnel of Sectigo. CA key data must be stored securely at all times unless attended by authorised personnel of Sectigo.

CA key generation that involves an HSM is performed in a 'CA key ceremony'. All CA key ceremonies are performed in a secure, controlled area. During the ceremony, at least two authorised Sectigo personnel are present at all times. It may be required that authorised auditors be present to witness the CA key ceremonies. No other persons are allowed in the secure area during the key ceremonies to protect against information loss through tampering or overseeing. All visible 'Sensitive' information is kept to a minimum at all times during the CA key ceremonies.

All CA key ceremonies are performed on a computer with a verified clean installation of the operating system that is isolated from all computer networks. The Cryptographic operation control software shall be a fresh install and verified to be operating correctly before use.

All media created from a CA key ceremony that contains CA key backup data must be classified and stored in accordance with this classification.

All obsolete media from a CA Key ceremony must be disposed of in a secure manner i.e. destruction, at the end of the CA key ceremony, or within a maximum period of 1 working day. All media that is not fully disposed of immediately, must be partially destroyed and securely stored until full disposal takes place.

6.1.2. Private Key Delivery to Subscriber

When CAs generate key pairs on behalf of the Subscriber, the Private Key SHALL be delivered securely to the Subscriber. Private keys SHALL be delivered electronically or on a FIPS certified hardware cryptographic module. In all cases, the following requirements SHALL be met: • Except in cases where the Sectigo operates a key archiving service on behalf of the Subscriber, Sectigo SHALL NOT retain any copy of the key for more than two weeks after delivery of the Private Key to the Subscriber. • Where key pairs are pre-generated on hardware tokens, the entities distributing such tokens SHALL use best efforts to provide physical security of the tokens to prevent the loss, disclosure, modification, or unauthorized use of the Private Keys on them. The RA SHALL maintain a record of the Subscriber acknowledgment of receipt of the token. • The Subscriber SHALL acknowledge receipt of the Private Key(s). • Delivery SHALL be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.

Where Key Pairs for Code Signing Certificates are generated by Sectigo, Sectigo authorized personnel will provide the FIPS-140-2 Level 3 or Common Criteria EAL 4+ crypto module's random, unguessable PIN to the subscriber named in the subscriber certificate after validating that their identity matches the subscriber certificate. The cryptographic device will be configured to not allow the export of the private key.

6.1.3. Public Key Delivery to Certificate Issuer

Code Signing Certificate requests generated using the Subscriber's hardware security module and submitted automatically to Sectigo in the form of a PKCS#10 Certificate Signing Request (CSR) will be checked with a key attestation.

6.1.4. CA Public Key Delivery to Relying Parties

Sectigo's Public Keys are provided to Relying Parties in a few ways. One way is through the Repository. Additionally, Public Keys of Sectigo's Root CAs are embedded in browsers.

6.1.5. Key Sizes

This document requires use of RSA PKCS #1, RSASSA-PSS, DSA, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy SHOULD contain RSA or elliptic curve Public Keys. All Certificates that expire on or before December 31, 2030 SHOULD contain subject Public Keys of at least 2048 bits for RSA/DSA, at least 256 bits for elliptic curve, and be signed with the corresponding Private Key. All Certificates that expire after December 31, 2030 SHOULD contain subject Public Keys of at least 3072 bits for RSA/DSA, at least 256 bits for elliptic curve, and be signed with the corresponding Private Key.

CAs that generate Certificates and CRLs under this policy SHOULD use the SHA-256, or SHA-384 hash algorithm when generating digital signatures. ECDSA signatures on Certificates and CRLs SHOULD be generated using SHA-256 or SHA-384, as appropriate for the key length.

For Root CA Certificates' key sizes, see section 6.3.2

Code Signing certificate key sizes SHALL be governed by NIST key management guidelines.

6.1.5.1. Root CA and subCA Key sizes

For Keys corresponding to Root and Subordinate CAs:

- If the Key is RSA, then the modulus MUST be at least 4096 bits in length.
- If the Key is ECDSA, then the curve MUST be one of NIST P-256, P-384, or P-521.

6.1.5.2. Code Signing Certificate and Timestamp Authority Key sizes

For Keys corresponding to Subscriber code signing and Timestamp Authority Certificates:

- If the Key is RSA, then the modulus MUST be at least 3072 bits in length.
- If the Key is ECDSA, then the curve MUST be one of NIST P-256, P-384, or P-521.

6.1.6. Public Key Parameters Generation and Quality Checking

Sectigo generates the Public Key parameters. Sectigo's CA keys SHALL be generated within at least a FIPS 140-2 Level 3 or Common Criteria EAL 4+ certified HSM.

RSA: Sectigo confirms that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 2^16+1 and 2^256-1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89]

ECC: Sectigo confirms the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2]

6.1.7. Key Usage Purposes (as per X.509 v3 key usage field)

Sectigo Certificates are general purpose and MAY be used without restriction on geographical area or industry. In order to use and rely on a Sectigo Certificate the Relying Party must use X.509v3 compliant software. Sectigo Certificates include key usage extension fields to specify the purposes for which the Certificate MAY be used and to technically limit the functionality of the Certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of Sectigo.

The possible key purposes identified by the X.509v3 standard are the following:

1. Digital signature, for verifying digital signatures that is, for entity authentication and data origin authentication with integrity

2. Non-repudiation, for verifying digital signatures used in providing a nonrepudiation service which protects against the signing entity falsely denying some action
3. Key encipherment, for enciphering keys or other security information, e.g., for key transport
4. Data encipherment, for enciphering user data, but not keys or other security information
5. Key agreement, for use as a Public Key agreement key
6. Key Certificate signing, for verifying a CA's signature on Certificates, used in CA Certificates only
7. CRL signing, for verifying a CA's signature on CRLs
8. Encipher only, Public Key agreement key for use only in enciphering data when used with key agreement
9. Decipher only, Public Key agreement key for use only in deciphering data when used with key agreement

The appearance of a key usage in this section does not indicate that Sectigo does or will issue a certificate with that key usage.

Private Keys corresponding to Root Certificates SHALL NOT be used to sign Certificates except in the following cases:

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

6.2. Private Key Protection and Cryptographic Module Engineering Controls

The Sectigo Infrastructure uses trustworthy systems to provide Certificate services. A trustworthy system is computer hardware, software and procedures that provide an acceptable resilience against security risks, provide a reasonable level of availability, reliability and correct operation, and enforce a security policy.

6.2.1. Cryptographic Module Standards and Controls

Sectigo securely generates and protects its own Private Key(s), using trustworthy HSMs and takes necessary precautions to prevent the compromise or unauthorized usage of them. Such HSMs SHALL be certified to at least FIPS 140-2 Level 3 or Common Criteria EAL 4+.

The Sectigo Root keys were generated in accordance with the guidelines detailed in the Root Key Generation Ceremony document. The activities undertaken and the personnel involved in the Root Key Generation Ceremony are recorded for audit purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

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

The decryption key is split across **m** removable media and requires **n** of **m** to reconstruct the decryption key. Custodians in the form of two or more authorized Sectigo officers are required to physically retrieve the removable media from the distributed physically secure locations.

Except during Key Pair generation, export, and import, access to the cryptographic operation software on the HSM is controlled through the use of Smart Cards (or cryptographic tokens of other forms) and their associated PINs which must be entered/presented before any key operations may be performed. Access to the Smart Cards & PINs is restricted to authorized Sectigo Officers. The HSMs are configured to require N from M cards to be present. A list is maintained of authorized Sectigo personnel with access to Smart Cards & PINs.

6.2.3. Private Key Escrow

Where Subscriber Private Keys are escrowed, Sectigo acts as the escrow agent and does not delegate this task to any third party. The Subscriber Private Key is stored in an encrypted form. A suitably authorized administrator of the enterprise account within which the Certificate has been requested may trigger the escrow. Triggering the escrow automatically revokes the Certificate ensuring that the Certificate cannot be used further.

6.2.4. Private Key Backup

The CA private signature keys SHALL be backed up under the same multi-person control as the original signature key. At least one copy of the private signature key SHALL be stored off-site. All copies of the CA private signature key SHALL be accounted for and protected in the same manner as the original.

Generally, the Subscriber is solely responsible for protection of their Private Keys. However, Sectigo offers certain Subscribers the optional feature of having Sectigo back up the Private Keys Sectigo generates on Subscriber's behalf. Sectigo protects these keys by having an agent or agents of the Certificate Manager Subscriber (typically, the employer of the individual receiving the client Certificate) encrypt a PKCS#12 format that contains the keys before they are stored on a secure server. Keys stored by Sectigo can only be decrypted using the keys held by the selected agents of the Certificate Manager Subscriber. Encrypted keys are sent via a secure connection and decrypted by the agent of the Certificate Manager Subscriber on their own computers.

6.2.5. Private Key Archival

Private Keys belonging to Sectigo CAs are not archived by parties other than Sectigo.

When any CA Root Signing Key pair expires, they will be archived for at least 7 years. The keys will be archived in a secure cryptographic hardware module, as per their secure storage prior to expiration, as detailed in section 6.3.2 of this document. Sectigo MAY store archived CA keys in backup form at secure vault locations.

6.2.6. Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module into backup tokens only for HSM transfer, offline storage, and backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form.

Where CA Root signing keys are backed up to another cryptographic hardware security module, such keys are transferred between devices in encrypted format only.

All transfers of Private Keys into or from a cryptographic module are performed in accordance with the procedures specified by the vendor of the relevant cryptographic module.

6.2.7. Private Key Storage on Cryptographic Module

Private Keys for CAs and TSAs are generated and stored inside Sectigo's Hardware Security Modules (HSMs). HSMs SHALL be certified to at least FIPS 140-2 Level 3 or Common Criteria EAL 4+.

For CA Root Private Key recovery purposes, the Root CA keys are encrypted and stored within a secure environment.

6.2.7.1. Subscriber Private Key protection

Subscriber Private Keys for Code Signing Certificates SHALL be protected per the following requirements.

Sectigo MUST obtain a contractual representation from the Subscriber that the Subscriber will use one of the following options to generate and protect their Code Signing Certificate Private Keys in a Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+:

1. Subscriber uses a Hardware Crypto Module meeting the specified requirement;
2. Subscriber uses a cloud-base key generation and protection solution with the following requirements:

a. Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements;

b. Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.

3. Subscriber uses a Signing Service which meets the requirements of the CS BRs Section 6.2.7.3.

6.2.7.2. Subscriber Private Key verification

Sectigo SHALL ensure that the Subscriber's Private Key is generated, stored, and used in a suitable Hardware Crypto Module that meets or exceeds the requirements specified in the CS BRs, section 6.2.7.4.1.

One of the following methods MUST be employed to satisfy this requirement:

1. Sectigo ships a suitable Hardware Crypto Module, with one or more pre-generated Key Pairs that the CA has generated using the Hardware Crypto Module;
2. The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate, commonly known as key attestation, indicating that the Private Key was generated in a non-exportable way using a suitable Hardware Crypto Module;
3. The Subscriber uses a CA prescribed crypto library and a suitable Hardware Crypto Module combination for the Key Pair generation and storage;
4. The Subscriber provides an internal or external IT audit indicating that it is only using a suitable Hardware Crypto Module to generate Key Pairs to be associated with Code Signing Certificates;
5. The Subscriber provides a suitable report from the cloud-based key protection solution subscription and resources configuration protecting the Private Key in a suitable Hardware Crypto Module;
6. Sectigo relies on a report provided by the Applicant that is signed by an auditor who is approved by Sectigo and who has IT and security training or is a CISA witnesses the Key Pair creation in a suitable Hardware Crypto Module solution including a cloud-based key generation and protection solution; or
7. The Subscriber provides an agreement that they use a Signing Service meeting the requirements of the CS BRs, section 6.2.7.3.

6.2.8. Method of Activating Private Key

Depending on the circumstances and the type of Certificate, a Private Key can be activated by Sectigo, Subscriber, or other authorized personnel. Sectigo's Private Keys are activated in accordance with the specifications of the cryptographic module. Subscriber must make all reasonable efforts to protect the integrity and confidentiality of its Private Key(s). Private Keys remain active until deactivated.

6.2.8.1. CA Administrator Activation

Method of activating the CA system by a CA Administrator SHALL require: • Use a smart card, biometric access Device, password in accordance with Section 6.4.1, or security of equivalent strength to Authenticate the Administrator before the activation of the Private Key, which includes, for instance, a password to operate the Private Key, a Windows logon or screen saver password, or a network logon password; and • Take commercially reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated Private Key without the Administrator's authorization.

6.2.8.2. Offline CAs Private Key

Once the CA system has been activated, a threshold number of shareholders SHALL be required to supply their activation data in order to activate an offline CA's Private Key, as defined in Section 6.2.2. Once the Private Key is activated, it SHALL be active until termination of the session.

6.2.8.3. Online CAs Private Keys

An online CA's Private Key SHALL be activated by a threshold number of shareholders, as defined in Section 6.2.2, supplying their activation data (stored on secure media). Once the Private Key is activated, the Private Key MAY be active for an indefinite period until it is deactivated when the CA goes offline.

6.2.9. Method of Deactivating Private Key

Cryptographic modules that have been activated SHALL NOT be available to unauthorized access. After use, the cryptographic module SHALL be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity. CA cryptographic modules SHALL be stored securely when not in use. When an online CA is taken offline, Sectigo SHALL remove the token containing the Private Key from the reader in order to deactivate it.

With respect to the Private Keys of offline CAs, after the completion of a Key Generation Ceremony, in which such Private Keys are used for Private Key operations, Sectigo SHALL remove the token containing the Private Keys from the reader in order to deactivate them. Once removed from the reader, tokens SHALL be securely stored. When deactivated, Private Keys SHALL be kept in encrypted form only. They SHALL be cleared from memory before the memory is de-allocated. Any disk space where Private Keys were stored SHALL be overwritten before the space is released to the operating system.

Depending on the circumstances and the type of Certificate, a Private Key can be deactivated by Sectigo, Subscriber, or other authorized personnel.

6.2.10. Method of Destroying Private Key

Destroying a Private Key means the destruction of all active keys, both backed-up and stored. Destroying a Private Key MAY comprise of removing it from the HSM or removing it from the active backup set. Private Keys are destroyed in accordance with NIST SP 800-88.

This process will be witnessed and signed by 2 trusted roles of Sectigo.

6.2.11. Cryptographic Module Rating

See section 6.2.1 of this document.

6.3. Other Aspects of Key Pair Management

This section considers other areas of key management. Particular subsections may be applicable to issuing CAs, repositories, subject CAs, RAs, Subscribers, and other participants.

6.3.1. Public Key Archival

When Public Keys are archived, they are archived according to procedures outlined in section 5.5 of this document.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The validity period for a Code Signing Certificate issued to a Subscriber MUST NOT exceed 39 months.

The Timestamp Authority MUST use a new Timestamp Certificate with a new Private Key no later than every 15 months to minimize the impact to users in the event that a Timestamp Certificate's Private Key is compromised.

The validity for a Timestamp Certificate must not exceed 135 months.

Sectigo verifies all information that is included in Code Signing Certificates at time intervals of 825 days or less.

In the case of EV Code Signing Certificates, the age of all data used to support issuance does not exceed the limit of 398 days.

The expiration of Sectigo's Root CA Certificates is set out in Table 6.3.2.

Subordinate CA certificates lifetimes are either the same or shorter than those of the CA by which they are signed.

Table 6.3.2

COMMON_NAME	VALID_TO	KEY_SIZE	SIGNATURE
AAA Certificate Services	31/12/2028	RSA 2048	sha1WithRSA
Secure Certificate Services	31/12/2028	RSA 2048	sha1WithRSA
Trusted Certificate Services	31/12/2028	RSA 2048	sha1WithRSA
COMODO Certification Authority	31/12/2030	RSA 2048	sha1WithRSA
COMODO RSA Certification Authority	18/1/2038	RSA 4096	sha384WithRSA
USERTrust RSA Certification Authority	18/1/2038	RSA 4096	sha384WithRSA
COMODO ECC Certification Authority	18/1/2038	ECDSA 384	ecdsa-with-SHA384
USERTrust ECC Certification Authority	18/1/2038	ECDSA 384	ecdsa-with-SHA384
Sectigo Public Code Signing Root E46	21/3/2046	ECDSA 384	ecdsa-with-SHA384
Sectigo Public Code Signing Root R46	21/3/2046	RSA 4096	sha384WithRSA
Sectigo Public Root E46	21/3/2046	ECDSA 384	ecdsa-with-SHA384
Sectigo Public Root R46	21/3/2046	RSA 4096	sha384WithRSA
Sectigo Public Time Stamping Root E46	21/3/2046	ECDSA 384	ecdsa-with-SHA384
Sectigo Public Time Stamping Root R46	21/3/2046	RSA 4096	sha384WithRSA
Entrust.net Certification Authority (2048)	24/7/2029	RSA 2048	sha1WithRSAEncryption
Entrust Root Certification Authority - G2	7/12/2030	RSA 2048	sha256WithRSAEncryption
Entrust Code Signing Root Certification Authority - CSBR1	30/12/2040	RSA 4096	sha512WithRSAEncryption
Entrust Digital Signing Root Certification Authority - DSR1	30/12/2040	RSA 4096	sha512WithRSAEncryption
Entrust Root Certification Authority	26/11/2026	RSA 2048	sha1WithRSAEncryption
Entrust Root Certification Authority - EC1	18/12/2027	ECDSA 384	ecdsa-with-SHA384
Entrust Root Certification Authority - G4	27/12/2030	RSA 4096	sha256WithRSAEncryption

6.4. Activation Data

Activation data refers to data values other than whole Private Keys that are required to operate Private Keys or cryptographic modules containing Private Keys. Examples of activation data include, but are not limited to, PINs, passphrases, and portions of Private Keys used in a key-splitting regime.

6.4.1. Activation Data Generation and Installation

Activation data is generated in accordance with the specifications of the HSM. This hardware SHALL be certified to at least FIPS 140-2 level 3 or Common Criteria EAL 4+.

6.4.2. Activation Data Protection

The procedures used to protect activation data is dependent on whether the data is for smartcards or passwords. Smartcards are held by highly trusted personnel. Passwords and smartcards are subject to Sectigo's Cryptographic Policy.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

Sectigo ensures the integrity of its computer systems by implementing controls, such as

- Applying the same security controls to all systems co-located in the same zone with a Certificate System;
- Maintaining Root CA Systems in a high security zone and in an offline state or Air-Gapped from other networks;
- Maintaining and protecting Issuing Systems, Certificate Management Systems, and Security Support Systems;
- Configuring Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End/Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in Sectigo's operations and allowing only those that are approved by Sectigo;
- Reviewing configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End/Internal-Support Systems on a weekly basis;
- Undergoing penetration tests on a periodic basis and after significant infrastructure or application upgrades;
- Granting administration access to Certificate System only to persons acting in Trusted Roles and requiring their accountability for the Certificate System's security; and
- Changing authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked.

CA systems enforce Multi-Factor Authentication for all accounts capable of directly causing certificate issuance.

6.5.2. Computer Security Rating

No stipulation.

6.6. Lifecycle Technical Controls

6.6.1. System Development Controls

Sectigo has formal policies in place to control, document and monitor the development of its CA systems. Development requests may only be raised by a restricted set of personnel. Development tasks are prioritized by the 'task requesters' within their area and then further prioritized by the development manager whilst considering the development task list in its entirety. The majority of changes are developed in-house by Sectigo. In the event that Sectigo 'buys-in' services (hardware and/or software), vendors are selected based on reputation and ability to supply products 'fit for purpose'.

On receipt of each development request a unique task ID and title are assigned that stay with the task throughout the development lifecycle.

Each development task has an associated Risk Assessment carried out as a part of the development lifecycle. All tasks are viewed as carrying some form of risk, from issues relating to task scope and complexity to a lack of availability of resources. The management of risk is addressed through a formal risk management process with the request not being applied to the production environment until an acceptable level of risk is achieved.

The work-product of all development requests undergo peer review prior to release to the production environment to prevent malicious or erroneous software being loaded into the production environment.

Each task must be tested and signed off by the QA team before being deployed to the production environment. Developers are not permitted to be involved in the testing of their own work. When issues are found by QA the QA team provide feedback to the developer to resolve the issues before development may proceed to release.

Development and QA team members do not generally have any access to the production environment, however they MAY be given limited access to investigate/resolve issues. Access to these areas is strictly controlled.

Once the change has gone live to the production environment the task requester along with the testing team are advised and the change re-tested.

6.6.2. Security Management Controls

Sectigo has tools and procedures to ensure that Sectigo's operational systems and applications retain their integrity and remain configured securely. These tools and procedures include checking the integrity of the application and security software.

6.6.3. Lifecycle Security Controls

No stipulation.

6.7. Network Security Controls

Sectigo develops, implements, and maintains a comprehensive security program designed to protect its networks according to the industry best practices. Sectigo conforms with the latest version of the CAB Forum Network and Certificate System Security Requirements.

6.7.1. Network Segmentation

Network segmentation SHOULD be designed and implemented in a manner that:

1. minimizes attack surfaces;
2. limits lateral movement within networks;
3. restricts traffic flow between different network segments; and
4. protects all CA Infrastructure components from unauthorized access.

At Sectigo, in its security program, general protections for the network include, among others:

• Segmenting Certificate Systems into networks or zones based on their functional, logical, and physical relationship; • Applying the same security controls to all systems co-located in the same zone with a Certificate System; • Maintaining Root CA Systems in a high security zone and in an offline state or air-gapped from other networks; • Implementing and configuring Security Support Systems that protect systems and communications between systems inside secure zones and communications with non-Certificate Systems outside those zones; • Configuring network boundary controls (firewalls, switches, routers, and gateways) with rules that support only the services, protocols, ports, and communications that Sectigo has identified as necessary to its operations; • For Certificate Systems, implementing detection and prevention controls to guard against viruses and malicious software; and • Changing authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked.

6.7.2. CA Infrastructure Security

Sectigo´s CA Infrastructure is in a Physically Secure Environment.

For Certificate System, Sectigo has implemented detection and prevention controls to guard against viruses and malicious software; and is also changing authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked.

Sectigo has implemented and configured Security Support Systems that protect systems and communications between:

1. between CA Infrastructure components; and
2. between CA Infrastructure and non-CA Infrastructure.

Equivalent security is implemented on all Systems on the same network as any CA Infrastructure component.

6.7.3. Timeline for addressing vulnerabilities

The following timelines apply for the application and infrastructure critical and non-critical vulnerabilities. Risk Assessment for every issue shall be completed within 48 hours and Resolution time shall be within:

Critical: 96 hours High: 30 days Medium: 90 days Low: 90 days

6.8. Time-Stamping

All CA components SHALL regularly synchronize with a time service such as National Institute of Standards and Technology (NIST) Atomic Clock or NIST Network Time Protocol Service. Time derived from the time service SHALL be used for establishing the time of: • Initial validity type of a Device's Certificate; • Revocation of a Device's Certificate; • Posting of CRL updates; and • OCSP or other responses. Certificates, CRLs, and other revocation database entries SHALL contain time and date information. Electronic or manual procedures MAY be used to maintain system time. Clock adjustments are auditable events (see Section 5.4.1).

Sectigo operates two Time-Stamping Authorities (TSA) and both are compliant with the RFC 3161. The Sectigo TSAs are intended only for use in signing software when used in conjunction with a Sectigo Code-signing Certificate.

The Timestamp Authority MUST ensure that clock synchronization is maintained when a leap second occurs. A Timestamp Authority MUST synchronize its timestamp server at least every 24 hours with a UTC(k) time source. The timestamp server MUST automatically detect and report on clock drifts or jumps out of synchronization with UTC. Clock adjustments of one second or greater MUST be auditable events. Any changes to its signing process MUST be an auditable event.

The Sectigo Authenticode time-stamping service is available at the URL:

http://timestamp.sectigo.com/authenticode.

Sectigo also offers a RFC3161 TSA, whose URL is:

http://timestamp.sectigo.com/rfc3161.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Sectigo uses version 3 of the X.509 standard to construct digital Certificates for use within the Sectigo PKI. X.509v3 allows a CA to add certain Certificate extensions to the basic Certificate structure. Sectigo uses a number of Certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. X.509v3 is a standard of the International Telecommunications Union for digital Certificates.

7.1. Certificate Profile

Sectigo incorporates by reference the following information in every digital Certificate it issues:

- Terms and conditions of the digital Certificate.
- Any other applicable Certificate policy as may be stated on an issued Sectigo Certificate, including the location of this document.
- The mandatory elements of the standard X.509v3.
- Any non-mandatory but customized elements of the standard X.509v3.
- Content of extensions and enhanced naming that are not fully expressed within a Certificate.
- Any other information that is indicated to be so in a field of a Certificate.

A Certificate profile contains fields as specified below:

- key usage extension field (section 6.1.7)
- extension criticality field (section 7.1.9)
- basic constraints extension (section 7.1.7)

Typical content of information published on a Sectigo Certificate MAY include but is not limited to the following elements of information:

- Code-signing Certificates
- Applicant's name or organizational name.
- Code of Applicant's country.
- Locality, state.
- Issuing certification authority (Sectigo).
- Applicant's Public Key.
- Sectigo digital signature.
- Signing algorithm.
- Validity period of the digital Certificate.
- Serial number of the digital Certificate.
- Sectigo generates non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.1. Version Number(s)

Certificate versions are all X.509 version 3. The Certificate version number SHALL be set to the integer value of "2" for Version 3 Certificates.

7.1.2. Certificate Extensions

Certificate extensions are in conformance to RFC 5280 and the Code Signing Baseline Requirements.

Enhanced naming is the usage of an extended organization field in an X.509v3 Certificate.

7.1.2.1. Root CAs

Sectigo Root CA Certificates contain:

- a basicConstraints extension marked critical. The cA field is set true. The pathLenConstraint is not present. -a keyUsage extension marked critical. Bit positions for keyCertSign and cRLSign are set. Some Sectigo Root CA Certificates also have the digitalSignature bit set.

Sectigo Root CA Certificates MAY contain:

- a non-critical cRLDistributionPoints extension containing the HTTP URL of the CA's CRL service.

Sectigo Root CA Certificates do not contain:

- a certificatePolicies nor the Extended Key Usage extension.

7.1.2.2. Subordinate CAs

Sectigo Subordinate CA certificates contain a certificatePolicies extension, not marked critical, that includes one or more policyIdentifiers and usually contains a policyQualifier referring to the CPS URI but not including a userNotice.

Sectigo Subordinate CA certificates contain a non-critical cRLDistributionPoints extension containing the HTTP URL of the Issuing CA's CRL service.

Sectigo Subordinate CA certificates contain a non-critical authorityInformationAccess extension containing the HTTP URL of the Issuing CA's OCSP responder and also containing the HTTP URL of the Issuing CA's certificate.

Sectigo Subordinate CA certificates contain a basicConstraints extension marked critical. The cA field is set true. The pathLenConstraint is often present and the pathLenConstraint is usually set to 0.

Sectigo Subordinate CA certificates contain a keyUsage extension marked critical. Bit positions for keyCertSign and cRLSign are set. The digitalSignature bit is also set if this CA also signs OCSP responses.

Sectigo Subordinate CA certificates contain an ExtendedKeyUsage extension not marked critical.

If the Subordinate CA will be used to issue Code Signing Certificates:

- id-kp-codeSigning MUST be present.
- id-kp-timeStamping MUST NOT be present.

If the Subordinate CA will be used to issue Timestamp Certificates:

- id-kp-timeStamping MUST be present.
- id-kp-codeSigning MUST NOT be present.

Additionally, the following EKUs MUST NOT be present:

- anyExtendedKeyUsage
- id-kp-serverAuth
- id-kp-emailProtection
- Other values SHOULD NOT be present.

7.1.2.3. Code Signing and Timestamping Certificates

These Certificates contain:

- a non-critical certificatePolicies extension that includes one or more policyIdentifiers and usually contains a policyQualifier referring to the CPS URI but not including a userNotice.
- a non-critical cRLDistributionPoints extension containing the HTTP URL of the Issuing CA's CRL service.
- a non-critical authorityInformationAccess extension containing the HTTP URL of the Issuing CA's OCSP responder and also containing the HTTP URL of the Issuing CA's certificate. This extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It SHOULD also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).
- a basicConstraints extension marked critical. The cA field is not set.

- a keyUsage extension marked critical. Bit positions for keyCertSign and cRLSign are NOT set but the bit position for digitalSignature is set
- an extKeyUsage extension
- If the Certificate is a Code Signing Certificate, then id-kp-codeSigning MUST be present
- If the Certificate is a Timestamp Certificate, then id-kp-timeStamping MUST be present and MUST be marked critical.
- a non-critical authorityKeyIdentifier

7.1.2.4. All Certificates

All other fields and extensions are in accordance with RFC5280.

Sectigo does not issue certificates containing keyUsage or extendedKeyUsage values, or Certificate extensions, or other data not specified in sections 7.1.2.1, 7.1.2.2, or 7.1.2.3 above unless Sectigo is aware of a reason for including the data in the Certificate.

Sectigo does not issue certificates containing Extensions that do not apply in the context of the public Internet unless:

i. such value falls within an OID arc for which the Applicant demonstrates ownership, or
ii. the Applicant can otherwise demonstrate the right to assert the data in a public context

Sectigo does not issue certificates containing semantics that, if included, will mislead a Relying Party about the certificate information verified by Sectigo (e.g., including extendedKeyUsage value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

7.1.3. Algorithm Object Identifiers

Sectigo Certificates are signed using algorithms with one of these identifiers:

sha-1WithRSAEncryption | OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)pkcs-1(1) 5 } |
sha256WithRSAEncryption | OBJECT IDENTIFIER ::= { iso(1)member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 } |
sha384WithRSAEncryption | OBJECT IDENTIFIER ::= { iso(1)member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 } |
ecdsa-with-SHA256 | OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 } |
ecdsa-with-SHA384 | OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 } |

Sectigo does not sign Certificates using RSA with PSS padding. CA, Code Signing and OCSP Certificates are not signed with sha-1WithRSAEncryption

For ECDSA, Sectigo uses and accepts only the NIST “Suite B” curves for those keys submitted to Sectigo for inclusion in end entity certificates.

7.1.4. Name Forms

Name forms are as stipulated in 3.1.1 of this document.

7.1.4.1. Name Encoding

For every valid Certification Path (as defined by RFC 5280, Section 6):

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.

- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate SHALL be byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

7.1.4.2. Subject Information – Subscriber Certificates

Sectigo represents that it followed the procedure set forth in its Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.2.1. Subject Alternative Name Extension

No stipulation.

7.1.4.2.2. Subject Distinguished Name Fields

1. subject:commonName
   this field contains the Subject´s legal name
2. subject:organizationName
   this field contains the Subject's name and/or DBA as verified under Section 3.2.2.
3. Sectigo MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that any abbreviations used are locally accepted abbreviations, e.g., if the official record shows "Company Name Incorporated", Sectigo MAY use "Company Name Inc." or "Company Name".
4. Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, Sectigo MAY use the subject:organizationName field to convey a natural person Subject's name or DBA.
5. (omitted)
6. subject:stateOrProvinceName
   If present this field contains the Subject's state or province information as verified under Section 3.2.2.2 or 3.2.2.3.
7. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(7), the subject:stateOrProvinceName field may contain the full name of the Subject's country information as verified under Section 3.2.2.2 or 3.2.2.3.
8. subject:countryName
   This field contains the Subject's two-letter ISO 3166-1 country code information as verified under Section 3.2.2.2 or 3.2.2.3.
9. If a Country is not represented by an official ISO 3166-1 country code, Sectigo will specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.
10. EV Codesigning Certificates SHALL also include the following fields as per Section 7.1.4.2 of the EVG:
11. Subject Business Category
12. subject:businessCategory (OID: 2.5.4.15)
13. Subject Jurisdiction of Incorporation or Registration
14. subject:jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1) (if required)
15. subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2) (if required)
16. subject:jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)
17. Subject Registration Number or Date
18. subject:serialNumber (OID: 2.5.4.5)
19. Other Subject Attributes
    Sectigo SHALL NOT include any Subject Distinguished Name attributes except as specified in Section 7.1.4.2 of the EVG. If present in other types of certificates, all other optional attributes, will contain information that has been verified by Sectigo.

7.1.4.3. Subject Information – Root Certificates and Subordinate CA Certificates

Sectigo represents that it followed the procedure set forth in thisCertification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.3.1. Subject Distinguished Name Fields

1. commonName
2. This field will be present and may be used as an identifier for the CA certificate. Across all CA certificates issued by Sectigo, each unique subject:commonName will be paired with only one CA keypair.
3. organizationName
4. This field will be present and contains the Subject CA's name or DBA as verified under Section 3.2.2.2.
5. Sectigo MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that any abbreviations used are locally accepted abbreviations, e.g., if the official record shows "Company Name Incorporated", Sectigo MAY use "Company Name Inc." or "Company Name".
6. countryName
7. This field will be present and contains the Subject's two-letter ISO 3166-1 country code information as verified under Section 3.2.2.2.

7.1.5. Name Constraints

Sectigo includes Name Constraints in Subordinate CA Certificates when relevant. Sectigo places Name Constraints in a non-critical nameConstraints extension within the CA certificate.

Sectigo does not include the anyExtendedKeyUsage EKU in Name Constrained CA certificates.

7.1.5.1. Code Signing

For Name Constrained CAs that include the id-kp-codeSigning extended key usage, the CA certificate includes the Name Constraints X.509v3 extension with constraints on DirectoryName as follows:

For each DirectoryName in permittedSubtrees Sectigo confirms the Applicant's and/or Subsidiary's Organizational name and location.

7.1.6. Certificate Policy Object Identifier

Sectigo uses policy OIDs under the arcs:

iso(1)
identified-organization(3)
dod(6)
internet(1)
private(4)
enterprise(1)

6449

certificates(1)
policies(2),

and:

joint-iso-itu-t(2)
international-organizations(23)
ca-browser-forum(140)
certificate-policies(1)

and:

iso(1)
identified-organization(3)
dod(6)
internet(1)
private(4)
enterprise(1)

5923

For example:

End entity certificate policies	
1.3.6.1.4.1.6449.1.2.1.3.2	Software Publisher
1.3.6.1.4.1.6449.1.2.1.3.8	Timestamping Certificate
1.3.6.1.4.1.6449.1.2.1.6.1	Sectigo EV Code-signing Certificates
2.23.140.1.4.1	Code Signing Certificates
2.23.140.1.3	EV Code Signing Certificates
Arc for intermediate CA policy identifiers	
1.3.6.1.4.1.6449.1.2.2	Intermediate CA policies
2.23.140.1.4.2	Timestamp CA policy
Other Policy OIDs	
1.3.6.1.4.1.6449.2.1.1	Default Time-stamping Policy

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

Sectigo includes in End Entity Certificates a non-critical Certificate Policies extension as defined in RFC5280. We include a single PolicyInformation extension that includes the Certificate Policy Identifier and a single Policy Qualifier referring to the CPS URI but not including a userNotice.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL Profile

Sectigo manages and makes publicly available directories of revoked Certificates using CRLs. All CRLs issued by Sectigo are X.509v2 CRLs, in particular as profiled in RFC5280. Users and relying parties are strongly urged to consult the directories of revoked Certificates at all times prior to relying on information featured in a Certificate. Sectigo updates and publishes a new CRL at least every 7 days. The CRL for any certificate issued by Sectigo (whether Subscriber certificate or CA certificate) MAY be found at the URL encoded within the CRLDP field of the certificate itself.

The profile of the Sectigo CRL for end user´s certificate is as per the table below:

Version	[Value 1]
Issuer Name	CountryName = [Root Certificate Country Name], OrganizationName=[Root Certificate Organization],CommonName=[Root Certificate Common Name][UTF8String encoding]
This Update	[Date of Issuance]
Next Update	[Date of Issuance + no more than 10 days]
Revoked Certificates	CRL Entries
Certificate Serial Number	[Certificate Serial Number]
Date and Time of Revocation	[Date and Time of Revocation]

7.2.1. Version Number(s)

Sectigo issues version 2 CRLs.

7.2.2. CRL and CRL Entry Extensions

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the authority key identifier listed in the Certificate.
Invalidity Date	Date in UTC format
Reason Code	Optional reason for revocation

reasonCode (OID 2.5.29.21)

If present, this extension MUST NOT be marked critical.

Sectigo does a byte-for-byte issuer name matching between CA certs and CRLs.

If a CRL entry is for a Root CA or Subordinate CA Certificate, including Cross Certificates, this CRL entry extension MUST be present. If a CRL entry is for a Certificate not technically capable of causing issuance, this CRL entry extension SHOULD be present, but MAY be omitted.

The CRLReason indicated MUST NOT be unspecified (0).

If a reasonCode CRL entry extension is present, the CRLReason MUST indicate the most appropriate reason for revocation of the certificate (picked by the subscriber when made the revocation request), as defined below:

- cessationOfOperation: this reason is used when the subscriber no longer controls or is authorized to use the domain names, or the subscriber is not using the certificate or the CA is made aware of any circumstances that the certificate is no longer permitted
- keyCompromise: this reason is used when Sectigo has received proof or reasonable suspicion of key compromise for revoked leaf certs
- caCompromise: this reason is used when Sectigo has received proof or reasonable suspicion of key compromise for revoked CA certs
- privilegeWithdrawn: this reason is used when there´s a subscriber-side infraction that has not resulted in keyCompromise, e.g., misleading information in the certificate
- affiliationChanged: this reason is used when the subject´s name or other subject identity information in the certificate has changed
- superseded: this reason is used when the subscriber has requested a replacement or Sectigo has obtained information that the domain validated information is not reliable or not in compliance with

this document or CAB Forum Baseline Requirements

7.3. OCSP Profile

Sectigo also publishes Certificate status information using Online Certificate Status Protocol (OCSP). Sectigo's OCSP responders are capable of providing a 'good' or 'revoked' status for all Certificates issued under the terms of this document. If queried for a certificate which was not issued by Sectigo the responder will provide 'unauthorized'. In the case of Code Signing Certificates, the OCSP responders will continue to give a 'good' status for unrevoked Certificates even after their expiry – for at least 10 years from expiration. The OCSP responders will give an 'unknown' response for expired Certificates or for those with fake serial numbers.

Sectigo operates an OCSP service at http://ocsp.sectigo.com. Revocation information is made immediately available through the OCSP services. The OCSP responder and responses are available 24x7.

The profile of Sectigo OCSP responses is as per this table:

Extension		**Value**
OCSP Response Status		successful (0x0)
Response Type		Basic OCSP Response
Version		1 (0x0)
Responder ID		Same as the subject key identifier listed in the signing certificate.
Produced At		[the time at which this response was signed]
Responses		
Certificate	ID	
	Hash Algorithm	Sha1
	Issuer Name Hash	Hash of issuer's DN
	Issuer Key Hash	Hash of issuer's public key
	Serial Number	CertificateSerialNumber
Cert Status		Good/Revoked/Unknown
Revocation Time (if Revoked)		[The time at which the certificate was revoked or placed on hold]
Reason code		If present SHALL contain a value permitted for CRLs, as specified in Section 7.2.2.
This Update		[The most recent time at which the indicated certificate status is known by the responder to have been correct]
Next Update		[The time at or before which newer information will be available about the status of the certificate.]
Signature Algorithm		sha256WithRSAEncryption

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus MUST be present and MUST contain a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1. Version Number(s)

Sectigo's OCSP responder conforms to RFC 6960 and 5019.

7.3.2. OCSP Extensions

The singleExtensions of an OCSP response MUST NOT contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices specified in this document have been designed to meet or exceed the requirements of generally accepted and developing industry standards related to the operation of CAs.

A regular audit is performed by an independent external auditor to assess Sectigo's compliancy.

8.1. Frequency or Circumstances of Assessment

The audit mandates that the period during which a CA issues Certificates be divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration.

8.2. Identity/Qualifications of Assessor

Sectigo's audit SHALL be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.1);
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;
5. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
6. Bound by law, government regulation, or professional code of ethics; and
7. Except in the case of an Internal Government Auditing Agency, 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

The auditor is independent of Sectigo, and does not have a financial interest, business relationship, or course of dealing that would create a conflict of interest or create a significant bias (for or against) Sectigo.

8.4. Topics Covered by Assessment

Topics covered by the annual audit include but are not limited to the following: • Business Practices Disclosure, meaning o the CA discloses its business practices, and o the CA provides its services in accordance with its CPS • Key Lifecycle Management, meaning o the CA maintains effective controls to provide reasonable assurance that the integrity of keys and Certificates it manages is established and protected throughout their lifecycles. • Certificate Lifecycle Management, meaning that o The CA maintains effective controls to provide reasonable assurance that Subscriber information was properly authenticated for specific registration activities, and o The CA maintains effective controls to provide reasonable assurance that subordinate CA Certificate requests are accurate, authenticated, and approved. • CA Environmental Control, meaning that o the CA maintains effective controls to provide reasonable assurance that Logical and physical access to CA systems and data is restricted to authorized individuals, The continuity of key and Certificate management operations is maintained, and CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity.

8.4.1. CA and TSA assessment

Sectigo undergoes a conformity assessment audit for compliance with these Requirements performed in accordance with one of the schemes accepted.

Whichever scheme is chosen, it MUST incorporate periodic monitoring and/or accountability procedures to

ensure that its audits continue to be conducted in accordance with the requirements of the scheme. The audit MUST be conducted by a Qualified Auditor, as specified in Section 8.2. The audit MUST cover all CA obligations of the CS BRs regardless of whether they are performed directly by the CA, an RA, or subcontractor.

8.5. Actions Taken as a Result of Deficiency

Either remediate or the auditor posts "qualified report." Auditor would report or document the deficiency and notify Sectigo of the findings. Depending on the nature and extent of the deficiency, Sectigo would develop a plan to correct the deficiency, which could involve changing its policies or practices, or both. Sectigo would then put its amended policies or practices into operation and require the auditors to verify that the deficiency is no longer present. Sectigo would then decide whether to take any remedial action with regard to Certificates already issued.

8.6. Communication of Results

The audit requires that Sectigo make the Audit Report available to the public no later than 3 months after of the audit period. Sectigo is not required to make publicly available any general audit finding that does not impact the overall audit opinion.

The Audit Report MUST contain at least the following clearly labelled information:

1. name of the organization being audited;
2. name and address of the organization performing the audit;
3. the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit;
4. audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
5. a list of the CA policy documents, with version numbers, referenced during the audit;
6. whether the audit assessed a period of time or a point in time;
7. the start date and end date of the Audit Period, for those that cover a period of time;
8. the point in time date, for those that are for a point in time;
9. the date the report was issued, which will necessarily be after the end date or point in time date
10. all incidents disclosed by the CA, discovered by the auditor, or reported by a third party, that, at any time during the audit period, occurred or were open in Mozilla's Bugzilla reporting system;

The Audit Report MUST be available as a PDF and SHALL be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report MUST be uppercase letters and MUST NOT contain colons, spaces, or line feeds.

8.7. Self-Audits

Code Signing certificates: Sectigo performs regular self-audits and audits of Registration Authorities in accordance with section 8.7 of the Code Signing BRs.

9. OTHER BUSINESS AND LEGAL MATTERS

This part describes the legal representations, warranties and limitations associated with Sectigo digital Certificates.

9.1. Fees

Sectigo charges Subscriber fees for some of the Certificate services it offers, including issuance, renewal and reissues (in accordance with the Sectigo Reissue Policy stated in 9.1.6 of this document). Such fees are detailed on the official Sectigo websites (this is not an exhaustive list: www.sectigo.com, www.comodoca.com, ...).

Sectigo retains its right to affect changes to such fees. Sectigo partners, including Reseller Partners and EPKI Manager Account Holders, will be suitably advised of price amendments as detailed in the relevant partner agreements.

9.1.1. Certificate Issuance or Renewal Fees

Sectigo is entitled to charge Subscribers for the issuance, management, and renewal of Certificates. In most circumstances, applicable Certificate fees will be delineated in the Subscriber Agreement between Sectigo and Subscriber.

9.1.2. Certificate Access Fees

Sectigo MAY charge a reasonable fee for access to its Certificate databases.

9.1.3. Revocation or Status Information Access Fees

Sectigo does not charge fees for the revocation of a Certificate or for a Relying Party to check the validity status of a Sectigo issued Certificate using CRLs.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

Sectigo offers a 30-day refund policy. During a 30-day period (beginning when a Certificate is first issued) the Subscriber MAY request a full refund for their Certificate. Under such circumstances, the original Certificate MAY be revoked and a refund provided to the Applicant. Sectigo is not obliged to refund a Certificate after the 30-day refund policy period has expired.

9.1.6. Reissue Policy

Sectigo offers a 30-day reissue policy. During a 30-day period (beginning when a Certificate is first issued) the Subscriber MAY request a reissue of their Certificate and incur no further fees for the reissue. If details other than just the Public Key require amendment, Sectigo reserves the right to revalidate the application in accordance with the validation processes detailed within this CPS. If the reissue request does not pass the validation process, Sectigo reserves the right to refuse the reissue application. Under such circumstances, the original Certificate MAY be revoked and a refund provided to the Applicant.

Sectigo is not obliged to reissue a Certificate after the 30-day reissue policy period has expired.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

Sectigo maintains professional Errors and Omissions Insurance.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for end-entities

If Sectigo was negligent in issuing a Certificate that resulted in a Covered Loss to a Relying Party, the Relying Party MAY be eligible under Sectigo's Relying Party Warranty to receive up to the Maximum Certificate Coverage per Incident, subject to the Total Payment Limit**,** for all claims related to that Certificate. For complete terms and conditions, see the Relying Party Agreement and the Relying Party Warranty located in the Repository.

9.3. Confidentiality of Business Information

Sectigo observes applicable rules on the protection of personal data deemed by law or the Sectigo privacy policy (see section 9.4.1 of this document) to be confidential.

9.3.1. Scope of Confidential Information

Sectigo keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- Subscriber Agreements.
- Certificate application records and documentation submitted in support of Certificate applications whether successful or rejected.
- Transaction records and financial audit records.
- External or internal audit trail records and reports, except for audit reports that may be published at the discretion of Sectigo.
- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of Sectigo infrastructure, Certificate management and enrolment services and data.
- Private keys

9.3.2. Information Not Within the Scope of Confidential Information

Subscribers acknowledge that revocation data of all Certificates issued by the Sectigo is public information and is published every 24 hours. Subscriber application data marked as "Public" in the relevant Subscriber Agreement or Certificate request form that is submitted as part of a Certificate application is published within an issued Certificate. Such information is not within the scope of confidential information.

9.3.3. Responsibility to Protect Confidential Information

All Sectigo personnel in trusted positions handle all confidential information in strict confidence and are required to sign confidentiality agreements before being employed in a trusted position. Personnel of RA/LRAs especially must comply with the requirements of the English law on the protection of confidential information.

9.3.4. Publication of Certificate Revocation Data

Sectigo reserves its right to publish a CRL as MAY be indicated.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

Sectigo has implemented a privacy policy, which complies with this document. The Sectigo privacy policy is published at https://sectigo.com/privacy-policy.

9.4.2. Information Treated as Private

See Sectigo Limited Privacy Policy. Additionally, personal information obtained from an Applicant during the application or identity verification process is considered private information if the information is not included in the Certificate and if the information is not public information.

9.4.3. Information not Deemed Private

In addition to the information not deemed private in the Sectigo Limited Privacy Policy, information made public in a Certificate, CRL, or OCSP is not deemed private.

9.4.4. Responsibility to Protect Private Information

Sectigo participants are expected to handle private information with care, and in compliance with local privacy laws in the relevant jurisdiction.

9.4.5. Notice and Consent to Use Private Information

Sectigo provides notices to Applicants and Subscribers about Sectigo's use of private information through its Privacy Policy. Sectigo also provides notices to Applicants and Subscribers about Sectigo's use of private information at the time such information is collected.

Sectigo will only use private information after obtaining consent or as required by applicable laws or regulations.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

Sectigo reserves the right to disclose personal information if Sectigo reasonably believes that

- disclosure is required by law or regulation, or
- disclosure is necessary in response to judicial, administrative, or other legal process.

9.4.7. Other Information Disclosure Circumstances

See Privacy Policy. Further, Sectigo is not required to release any personal information, unless as otherwise required by law, without an authenticated, reasonably specific request by an authorized party specifying:

- The party to whom Sectigo owes a duty to keep information confidential.
- The party requesting such information.
- A court order, if any.

9.5. Intellectual Property Rights

Sectigo or its partners or associates own all intellectual property rights associated with its databases, web sites, Sectigo digital Certificates and any other publication originating from Sectigo including this document.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

Sectigo makes to all Subscribers and relying parties certain representations regarding its public service, as described below. Sectigo reserves its right to modify such representations as it sees fit or required by law.

Except as expressly stated in this documenmt or in a separate agreement with Subscriber, to the extent specified in the relevant sections of this document, Sectigo represents, in all material aspects, to:

- Comply with this document and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certification services, including but not limited to the establishment and operation of the Sectigo Repository and web site for the operation of PKI services.
- Provide trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its Private Key(s).
- Provide and validate application procedures for the various types of Certificates that it may make publicly available. For EV certificates, verify and confirm the legal existence of the organization or entity in the correspondent Jurisdiction of Incorporation (JoI) or Registration.
- Issue digital Certificates in accordance with this document and fulfill its obligations presented herein.

- Upon receipt of a request from an RA operating within the Sectigo network; act promptly to issue a Sectigo Certificate in accordance with this document.
- Upon receipt of a request for revocation from an RA operating within the Sectigo network; act promptly to revoke a Sectigo Certificate in accordance with this document.
- Publish accepted Certificates in accordance with this document.
- Provide support to Subscribers and relying parties as described in this document.
- Revoke Certificates according to this document.
- Provide for the expiration and renewal of Certificates according to this document.
- Make available a copy of this document and applicable policies to requesting parties.

As the Sectigo network includes RAs that operate under Sectigo practices and procedures Sectigo warrants the integrity of any Certificate issued under its own root within the limits of the Sectigo insurance policy and in accordance with this document.

The Subscriber also acknowledges that Sectigo has no further obligations under this document.

9.6.2. RA Representations and Warranties

A Sectigo RA operates under the policies and practices detailed in this document and also the associated Web Host Reseller agreement and/or EPKI Manager Account agreement. The RA is bound under contract to:

- Receive applications for Sectigo Certificates in accordance with this document.
- Perform all verification actions prescribed by the Sectigo validation procedures and this document.
- Receive, verify and relay to Sectigo all requests for revocation of a Sectigo Certificate in accordance with the Sectigo revocation procedures and this document.
- Abide by all laws, rules and regulations applicable to performance of their duties as an RA.

9.6.3. Subscriber Representations and Warranties

Subscribers represent and warrant that when submitting to Sectigo and using a domain and distinguished name (and all other Certificate application information) they do not interfere with or infringe any rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

Upon accepting a Certificate, the Subscriber represents to Sectigo and to relying parties that at the time of acceptance and until further notice:

- Digital signatures created using the Private Key corresponding to the Public Key included in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is properly operational 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 to Sectigo regarding the information contained in the Certificate are accurate and true.
- All information contained in the Certificate is accurate and true to the best of the Subscriber's knowledge or to the extent that the Subscriber had notice of such information whilst the Subscriber shall act promptly to notify Sectigo of any material inaccuracies in such information.
- The Certificate is used exclusively for authorized and legal purposes, consistent with this document.
- It will use a Sectigo Certificate only in conjunction with the entity named in the organization field of a digital Certificate (if applicable).
- The Subscriber retains control of her Private Key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.
- The Subscriber is an end-user Subscriber and not a CA and will not use the Private Key corresponding to any Public Key listed in the Certificate for purposes of signing any Certificate (or any other format of

certified Public Key) or CRL, as a CA or otherwise, unless expressly agreed in writing between Subscriber and Sectigo.
- The Subscriber agrees with the terms and conditions of this document and other agreements and policy statements of Sectigo.
- The Subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.
- The Subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

In all cases and for all types of Sectigo Certificates the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Sectigo of any such changes.

9.6.4. Relying Party Representations and Warranties

A party relying on a Sectigo Certificate accepts that in order to reasonably rely on a Sectigo Certificate they must:

- Minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected Certificate; the Relying Party must have reasonably made the effort to acquire sufficient knowledge on using digital Certificates and PKI.
- Study the limitations to the usage of digital Certificates and be aware through the Relying Party agreement the maximum value of the transactions that can be made using a Sectigo digital Certificate.
- Read and agree with the terms of this document and Relying Party agreement.
- Verify a Sectigo Certificate by referring to the relevant CRL and the CRLs of intermediate CA and root CA or by checking the OCSP response using the Sectigo OCSP responder.
- Trust a Sectigo Certificate only if it is valid and has not been revoked or has expired.
- Rely on a Sectigo Certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this document.

9.6.5. Representations and Warranties of other Participants

No stipulation.

9.7. Disclaimers of Warranties

9.7.1. Fitness for a Particular Purpose

Sectigo disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein and as cannot be excluded at law.

9.7.2. Other Warranties

Except as required by applicable law, Sectigo does not warrant:

- The accuracy, authenticity, completeness or fitness of any unverified information contained in Certificates or otherwise compiled, published, or disseminated by or on behalf of Sectigo except as it may be stated in the relevant product description below in this document and in the Sectigo insurance policy.
- In addition, shall not incur liability for representations of information contained in a Certificate except as it may be stated in the relevant product description in this document.
- Does not warrant the quality, functions or performance of any software or hardware device.
- Although Sectigo is responsible for the revocation of a Certificate, it cannot be held liable if it cannot execute it for reasons outside its own control.
- The validity, completeness or availability of directories of Certificates issued by a third party (including an agent) unless specifically stated by Sectigo.

Sectigo assumes that user software that is claimed to be compliant with X.509v3 and other applicable

standards enforces the requirements set out in this document. Sectigo cannot warrant that such user software will support and enforce controls required by Sectigo, whilst the user should seek appropriate advice.

9.8. Limitations of Liability

Sectigo Certificates MAY include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the Certificate and disclaimers of warranty that may apply. Subscribers must agree to Sectigo Terms & Conditions, or a Subscriber Agreement, before signing-up for a Certificate. To communicate information Sectigo MAY use:

- A Sectigo standard resource qualifier to a Certificate policy.
- Proprietary or other vendors' registered extensions.

9.8.1. Damage and Loss Limitations

In no event (except for fraud or willful misconduct) will the aggregate liability of Sectigo to all parties including without any limitation a Subscriber, an Applicant, a recipient, or a Relying Party for all digital signatures and transactions related to such Certificate exceed the cumulative maximum liability for such Certificate as stated in the Sectigo insurance plan detailed section 9.2.3 of this document.

9.8.2. Exclusion of Certain Elements of Damages

In no event (except for fraud or willful misconduct) shall Sectigo be liable for:

- Any indirect, incidental or consequential damages.
- Any loss of profits.
- Any loss of data.
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of Certificates or digital signatures.
- Any other transactions or services offered within the framework of this document.
- Any other damages except for those due to reliance, on the information featured on a Certificate, on the verified information in a Certificate.
- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful misconduct of the Applicant. Any liability that arises from the usage of a Certificate that has not been issued or used in conformance with this document.
- Any liability that arises from the usage of a Certificate that is not valid.
- Any liability that arises from usage of a Certificate that exceeds the limitations in usage and value and transactions stated upon it or on the document.
- Any liability that arises from security, usability, integrity of products, including hardware and software a Subscriber uses.
- Any liability that arises from compromise of a Subscriber's Private Key.

Sectigo does not limit or exclude liability for death or personal injury.

9.9. Indemnities

9.9.1. Indemnification by Sectigo

To the extent permitted by applicable law, Sectigo shall indemnify each Application Software Supplier against any third party claim, damage, or loss suffered by an Application Software Supplier related to a Certificate issued by Sectigo that is not in compliance with the Code Signing Baseline Requirements in effect at the date of issuance of the Certificate, regardless of the cause of action or legal theory involved, except where the claim, damage, or loss suffered by the Application Software Supplier was directly caused by the Application Software Supplier's software displaying either (1) a valid and trustworthy Certificate as not valid or trustworthy or (2) displaying as trustworthy (i) a Certificate that has expired or (ii) a revoked Certificate where the revocation status is available online but the Application Software Supplier's software failed to

check or ignored the status.

9.9.2. Indemnification by Subscriber

By accepting a Certificate, the Subscriber agrees to indemnify and hold Sectigo, as well as its agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that Sectigo, and the above mentioned parties may incur, that are caused by the use or publication of a Certificate, and that arises from:

- Any false or misrepresented data supplied by the Subscriber or agent(s).
- Any failure of the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CA, Sectigo, or any person receiving or relying on the Certificate.
- Failure to protect the Subscriber's confidential data including their Private Key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's confidential data.
- Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.

For Certificates issued at the request of a Subscriber's agent, both the agent and the Subscriber shall jointly and severally indemnify Sectigo, and its agents and contractors.

Although Sectigo will provide all reasonable assistance, Certificate Subscribers shall defend, indemnify, and hold Sectigo harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions on behalf of Sectigo.

9.9.3. Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify Sectigo, its partners, and any cross signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, an End-User License Agreement, this document, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

9.10. Term and Termination

9.10.1. Term

The term of this document, including amendments and addenda, begins upon publication to the Repository and remains in effect until replaced with a new version passed by the Sectigo Policy Authority.

9.10.2. Termination

This document, including all amendments and addenda, remain in force until replaced by a newer version.

9.10.3. Effect of Termination and Survival

The following rights, responsibilities, and obligations survive the termination of this document for Certificates issued under this document:

- All unpaid fees incurred under section 9.1 of this document;
- All responsibilities and obligations related to confidential information, including those stated in section 9.3 of this document;
- All responsibilities and obligations to protect private information, including those stated in section 9.4.4 of this document;
- All representations and warranties, including those stated in section 9.6 of this document;
- All warranties disclaimed in section 9.7 of this document for Certificates issued during the term of this document;
- All limitations of liability provided for in section 9.8 of this document; and

- All indemnities provided for in section 9.9 of this document.

Upon termination of this document, all PKI participants are bound by the terms of this document for Certificates issued during the term of this document and for the remainder of the validity periods of such Certificates.

9.11. Individual Notices and Communications with Participants

Sectigo accepts notices related to this document by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from Sectigo, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

Sectigo Policy Authority

Unit 7, Campus Road, Listerhills Science Park, Bradford, BD7 1HR, United Kingdom

Attention: Legal Practices

Email: legalnotices@sectigo.com

This document and related agreements are available online in the Repository.

9.12. Amendments

Upon the Sectigo Policy Authority accepting such changes it deems to have significant impact on the users of this document, an updated edition of this document will be published at the Sectigo repository (available at https://sectigo.com/legal), with suitable incremental version numbering used to identify new editions. This document SHALL be updated at least once per year.

Revisions not denoted “significant” are those deemed by the Sectigo Policy Authority to have minimal or no impact on Subscribers and Relying Parties using Certificates and CRLs issued by Sectigo. Such revisions may be made without notice to users and without changing the version number of this document.

Controls are in place to reasonably ensure that this document is not amended and published without the prior authorization of the Sectigo Policy Authority.

9.12.1. Procedure for Amendment

An amendment to this document is made by the Sectigo Policy Authority. The Sectigo Policy Authority will approve amendments to this document, and Sectigo will publish amendments in the Repository. Amendments can be an update, revision, or modification to this document, and can be detailed in this document or in a separate document. Additionally, amendments supersede any designated or conflicting provisions of the amended version of this document.

9.12.2. Notification Mechanism and Period

Sectigo provides notice of an amendment to this document by posting it to the Repository. Amendments become effective on the date provided in the document, when an amendment is written in a separate document, or on the date provided in this document, when written in this document.

Sectigo does not guarantee or establish a notice and comment period.

9.12.3. Circumstances Under Which OID Must be Changed

The Sectigo Policy Authority has the sole authority to determine whether an amendment to this document requires an OID change.

9.13. Dispute Resolution Provisions

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) all parties agree to notify Sectigo of the dispute with a view to seek dispute resolution.

9.14. Governing Law

9.14.1. Governing Law

This document is governed by, and construed in accordance with, English law. This choice of law is made to ensure uniform interpretation of this document, regardless of the place of residence or place of use of Sectigo digital Certificates or other products and services. English law applies in all Sectigo commercial or contractual relationships in which this document may apply or quoted implicitly or explicitly in relation to Sectigo products and services where Sectigo acts as a provider, supplier, beneficiary receiver or otherwise.

9.14.2. Interpretation

This document shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances and intended usage of a product or service. In interpreting this document, parties shall also take into account the international scope and application of the services and products of Sectigo and its international network of RAs as well as the principle of good faith as it is applied in commercial transactions.

The headings, subheadings, and other captions in this document are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this document.

Appendices and definitions to this document are for all purposes an integral and binding part of this document.

9.14.3. Jurisdiction

Each party, including Sectigo partners, Subscribers, and Relying Parties, irrevocably agrees that the courts of England and Wales have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this document or the provision of Sectigo PKI services.

9.15. Compliance with Applicable Law

This document 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. Sectigo complies with all applicable laws, rules, regulations, ordinances, decrees, and orders when providing services pursuant to this document.

In delivering its PKI services Sectigo complies in all material respects with high-level international standards and the relevant law on electronic signatures and all other relevant legislation and regulation.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

This document and all documents referred to herein constitute the entire agreement between the parties, superseding all other agreements that may exist with respect to the subject matter. Section headings are for reference and convenience only and are not part of the interpretation of this agreement.

9.16.2. Assignment

This document shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this document are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with the correspondent sections on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

9.16.3. Severability

If any term, provision, covenant, or restriction contained in this document, or the application thereof, is for any reason and to any extent held to be invalid, void, or unenforceable, (i) such provision shall be reformed to the minimum extent necessary to make it valid and enforceable as to affect the original intention of the parties, and (ii) the remainder of the terms, provisions, covenants, and restrictions of this document shall remain in full force and effect and shall in no way be affected, impaired or invalidated.

In the event of a conflict between the CABF documentation and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which Sectigo operates or issues certificates, Sectigo MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. Sectigo will notify the CA/Browser Forum of the relevant information newly added to this document by sending a message to questions@cabforum.org so that the CA/Browser Forum may consider possible revisions to the affected documents. This notification MUST be made within 90 days.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

This document shall be enforced as a whole, whilst failure by any person to enforce any provision of this document shall not be deemed a waiver of future enforcement of that or any other provision.

9.16.5. Force Majeure

Neither Sectigo nor any independent third-party RA operating under a Sectigo Certification Authority, nor any Resellers, Co-marketers, nor any subcontractors, distributors, agents, suppliers, employees, or directors of any of the forgoing shall be in default hereunder or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or related to delays in performance or from failure to perform or comply with the terms of this document, any Subscription Agreement, or any Relying Party Agreement due to any causes beyond its reasonable control, which causes include acts of God or the public enemy, riots and insurrections, war, accidents, fire, strikes and other labor difficulties (whether or not Sectigo is in a position to concede to such demands), embargoes, judicial action, failure or default of any superior certification authority, lack of or inability to obtain export permits or approvals, necessary labor materials, energy, utilities, components or machinery, acts of civil or military authorities.

9.16.6. Conflict of Rules

When this document conflicts with other rules, guidelines, or contracts, this document shall prevail and bind the Subscriber and other parties except as to other contracts either:

- Predating the first public release of the present version of this document.
- Expressly superseding this document for which such contract shall govern as to the parties thereto, and to the extent permitted by law.

9.17. Other Provisions

9.17.1. Subscriber Liability to Relying Parties

Without limiting other Subscriber obligations stated in this document, Subscribers are liable for any misrepresentations they make in Certificates to third parties that reasonably rely on the representations contained therein and have verified one or more digital signatures with the Certificate.

9.17.2. Duty to Monitor Agents

The Subscriber shall control and be responsible for the data that an agent supplies to Sectigo. The Subscriber must promptly notify the issuer of any misrepresentations and omissions made by an agent. The duty of this article is continuous.

9.17.3. Ownership

Certificates are the property of Sectigo. Sectigo gives permission to reproduce and distribute Certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. Sectigo reserves the right to revoke the Certificate at any time. Private and Public Keys are property of the Subscribers who rightfully issue and hold them. All secret shares (distributed elements) of the Sectigo Private Key remain the property of Sectigo.

9.17.4. Interference with Sectigo Implementation

Subscribers, Relying Parties, and any other parties shall not interfere with, or reverse engineer the technical implementation of Sectigo PKI services including the key generation process, the public web site and the Sectigo repositories except as explicitly permitted by this document or upon prior written approval of Sectigo. Failure to comply with this as a Subscriber will result in the revocation of the Subscriber's Certificate without further notice to the Subscriber and the Subscriber shall pay any charges payable but that have not yet been paid under the agreement. Failure to comply with this as a Relying Party will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the Sectigo repository and any Certificate or Service provided by Sectigo.

9.17.5. Choice of Cryptographic Method

Parties are solely responsible for having exercised independent judgment and employed adequate training in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as PKI as a solution to their security requirements.

9.17.6. Sectigo Partnerships Limitations

Partners of the Sectigo network shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the Sectigo products and services. Sectigo partners shall specifically refrain from seeking partnerships with other root authorities or apply procedures originating from such authorities. Failure to comply with this will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the Sectigo repository and any Digital Certificate or Service provided by Sectigo.

9.17.7. Subscriber Obligations

Unless otherwise stated in this document, Subscribers shall exclusively be responsible:

- To minimize internal risk of Private Key compromise by ensuring adequate knowledge and training on PKI is provided internally.
- To generate their own Private/Public Key pair to be used in association with the Certificate request submitted to Sectigo or a Sectigo RA.
- Ensure that the Public Key submitted to Sectigo or a Sectigo RA corresponds with the Private Key used.
- Ensure that the Public Key submitted to Sectigo or a Sectigo RA is the correct one.
- Provide correct and accurate information in its communications with Sectigo or a Sectigo RA.
- Alert Sectigo or a Sectigo RA if at any stage whilst the Certificate is valid, any information originally submitted has changed since it had been submitted to Sectigo.
- Generate a new, secure Key Pair to be used in association with a Certificate that it requests from Sectigo or a Sectigo RA.
- Read, understand and agree with all terms and conditions in this document and associated policies published in the Sectigo Repository at https://sectigo.com/legal.

- Refrain from tampering with a Sectigo Certificate.
- Use Sectigo Certificates for legal and authorized purposes in accordance with the suggested usages and practices in this document.
- Cease using a Sectigo Certificate if any information in it becomes misleading obsolete or invalid.
- Cease using a Sectigo Certificate if such Certificate is expired and remove it from any applications and/or devices it has been installed on.
- Refrain from using the Subscriber's Private Key corresponding to the Public Key in a Sectigo issued Certificate to issue end-entity digital Certificates or subordinate CAs.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the Private Key corresponding to the Public Key published in a Sectigo Certificate.
- Request the revocation of a Certificate in case of an occurrence that materially affects the integrity of a Sectigo Certificate.
- For acts and omissions of partners and agents, they use to generate, retain, escrow, or destroy their Private Keys.

Appendix A: Certificate Profiles

Root and Issuing CA certificates

See the list of our CA certificates at sectigo.com/legal

END ENTITY certificate

Example Code Signing Certificate:

Extension		Value
Version:		3 (0x2)
Serial Number:		containing at least 64 bits of output from a CSPRNG
Signature Algorithm:		sha256WithRSAEncryption or ecdsa-with-SHA256
Issuer:	commonName	Sectigo RSA Code Signing CA
	organizationName	Sectigo Limited
	locality	Salford
	stateOrProvince	Greater Manchester
	countryName	GB
Validity:	Not Before:	Feb 19 00:00:00 2019 GMT
	Not After:	Feb 19 23:59:59 2020 GMT
Subject:	commonName	Customer Example Inc.
	organizationName	Customer Example Inc.
	stateOrProvince	New Jersey
	countryName	US
Subject Public Key Info:		id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey
X509v3 Authority Key Identifier:		keyID: based on the subject key identifier in the issuer's certificate
X509v3 Subject Key Identifier:		SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)
X509v3 Key Usage: critical		Digital Signature, Key Encipherment
X509v3 Basic Constraints: critical		CA:FALSE
X509v3 Extended Key Usage:		Code Signing
X509v3 Certificate Policies:		1.3.6.1.4.1.6449.1.2.1.3.2 , CPS: https://sectigo.com/CPS
X509v3 CRL Distribution Points:		http://crl.sectigo.com/SectigoRSACodeSigningCA.crl
Authority Information Access:		CA Issuers - http://crt.sectigo.com/SectigoRSACodeSigningCA.crt OCSP - http://ocsp.sectigo.com

E.g., EV codesigning certificate. As codeSigning Certificate, except:

Extension		Value
Issuer:	commonName	Sectigo ECC **Extended Validation Code Signing CA**
Subject: (additional subject fields)	businessCategory	Private Organization
	jurisdictionST	New jersey
	jurisdictionC	US

Extension	Value
serialNumber	1234567
X509v3 Certificate Policies:	1.3.6.1.4.1.6449.1.2.1.6.1 , CPS: https://sectigo.com/CPS

Appendix B: ChangeLog

Version	Change Description	Date
1.0.0	New version specific for Code Signing certificates. Updated sections 1.6.1, 5.2.1, 5.4.6 and 6.7 due to the new NetSec version 2.0	26-Aug-24
1.0.2	Combined CP/CPS	05-Mar-2025
1.0.3	Update section 5.2.2	10-Mar-2025
1.0.4	Updated section 6.3.2 adding the Entrust root CAs	12-Sep-2025
1.0.5	Update section 6.2.10. Updated section 5.4.8 clarifying vulnerabilties issues. New section 6.7.3 for addressing vulnerabilities timelines	11-Nov-2025