Sectigo IoT Certificate Policy

Sectigo Limited

Version 1.2

Effective: February 24, 2023

3rd Floor, Building 26 Exchange Quay, Trafford Road,

Salford, Greater Manchester, M5 3EQ, United Kingdom

Tel: +44 (0) 161 874 7070

Fax: +44 (0) 161 877 1767

www.sectigo.com

SECTIGO

Contents

1. INTRODUCTION

1.1. Overview

This document defines the certificate policy for the Sectigo Internet of Things Public Key Infrastructure (IoT PKI) which governs communications within the network of computing devices, physical devices, mechanical and digital machines such as vehicles or home appliances, and other objects, animals, or people which have the ability to transfer data over a network.

Sectigo IoT PKI Certificates are the basis for several security services including authentication, confidentiality, integrity, and non-repudiation. For a Certificate to be in compliance with Sectigo specifications, it SHALL comply with this Certificate Policy.

A fundamental element of modern secure communications is establishing trust in Public Keys. This begins with a Relying Party obtaining a Subscriber's Public Key Certificate that is issued by a trusted entity certifying that the Public Key belongs to that Subscriber. End entity Certificates that are not trusted directly MAY become trusted through successive validation of a chain of CA Certificates from the Subscriber's Certificate to a trust anchor (typically a Root-CA Public Key). Trust anchors are explicitly trusted by Relying Parties. Relying parties are responsible for securely obtaining trust anchors and for securely managing their trust anchor store.

1.2. Document name and identification

This document is the *Sectigo IoT Certificate Policy (CP)*. It outlines the legal, commercial and technical principles and practices that Sectigo employs in providing certification services for IoT applications 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 (PKIX) in accordance with the Certificate Policies determined by Sectigo. It also defines the underlying certification processes for Subscribers and describes Sectigo's repository operations. The CP is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the Sectigo IoT PKI.

The Sectigo IoT CP is a public statement of the practices of Sectigo and the conditions of issuance, revocation and renewal of a Certificate issued under Sectigo's own hierarchy.

1.3. PKI participants

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

1.3.1. PKI Authorities

Policy Authority:

This is the entity that decides that a set of requirements for Certificate issuance and use are sufficient for a given application. The Policy Authority (PA):

- Establishes and maintains the Certificate Policy (CP).
- Approves the establishment of trust relationships with external PKIs that offer appropriately comparable assurance.
- Ensures that all aspects of the CA services, operations, and infrastructure as described in the CPS are performed in accordance with the requirements, representations, and warranties of the CP.

Trust Anchor Managers (TAMs): Authorities who manage a repository of trusted Root CA Certificates. They act on behalf of relying parties, basing their decisions on which CAs to trust on the results of compliance audits.

1.3.2. Certification authorities

Sectigo provides Certificate services within the Sectigo IoT PKI. These Certification Authorities will:

- Conform its operations to the CP (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 CP,
- Upon receipt of a valid request to revoke the Certificate from a person authorized to request revocation using the revocation methods detailed in this CP, revoke a Certificate issued for use within the Sectigo IoT PKI,
- Publish CRLs on a regular basis, in accordance with the applicable Certificate Policy and with provisions described in this CP,
- Distribute issued Certificates in accordance with the methods detailed in this CP,
- Update CRLs in a timely manner as detailed in this CP,

1.3.3. PKI Customers

PKI Customers are organizations which have entered into a business relationship with Sectigo for the hosting and operation of its PKI. In most cases the PKI Customer is also the Registration Authority and may operate some on premise PKI components such as the RA servers.

1.3.4. 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 a CPS approved by the Policy Authority. The RA is responsible for:

- The registration process.
- The identification and authentication process.

Registration Authority Staff: RA Staff are the individuals holding trusted roles that operate and manage RA components.

1.3.5. Subscribers

A Subscriber is the entity whose name appears as the subject in an end-entity Certificate (also known as a Subscriber Certificate), agrees to use its key and Certificate in accordance with the Certificate policy asserted in the Certificate, and does not itself issue Certificates. CAs are sometimes technically considered "Subscribers" in a PKI. However, the term "Subscriber" as used in this document refers only to those who request Certificates for uses other than signing and issuing Certificates or Certificate status information.

1.3.6. 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.

1.3.7. Other participants

The CAs and RAs operating under the CP MAY require the services of other security, community, and application authorities. The CPS will identify the parties responsible for providing such services, and the mechanisms used to support these services.

One such participant is the Compliance Auditor. CAs are required to engage organizationally independent parties to perform compliance audits on a regular basis. To be effective, it is expected that compliance auditors will have expertise in information security, cryptography, and PKI, risk mitigation strategies, and industry best practices.

1.4. Certificate usage

1.4.1. Appropriate Certificate uses

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 Certificates and related products that can be used in a way that addresses the needs of users for secure personal and business communications, including but not limited to secure email, 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.

Specific Certificate usage will be defined in the Sectigo´s IoT CPS and/or a customer CP/CPS.

1.4.2. Prohibited Certificate uses

Prohibited applications include the following:

- Any export, import, use or activity that contravenes any local or international laws or regulations;
- Any usage of Certificates in conjunction with illegal activities;
- Any usage of Certificates for personal use or purposes not related to the community's business;
- Any use of a Certificate after it has been revoked;
- Any use of a Certificate after it has expired; and
- Any use not expressly permitted in Section 1.4.1

1.5. Policy administration

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

1.5.1. Organization administering the document

The Sectigo Policy Authority maintains this CP, related agreements and Certificate policies referenced within this document.

1.5.2. Contact person

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

Sectigo Policy Authority
3rd Floor, 26 Exchange Quay, Trafford Road,
Salford, Greater Manchester, M5 3EQ, United Kingdom
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767
Attention: Legal Practices
URL: http://www.sectigo.com
Email: legalnotices@sectigo.com

1.5.3. Person determining CP suitability for the policy

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

1.5.4. CP approval procedures

This CP and any subsequent changes, amendments, or addenda, SHALL be approved by the Sectigo Policy Authority.

1.6. Definitions and acronyms

Unless otherwise defined in this CP, capitalized terms in this CP SHALL have the meaning attributed to them in this section.

1.6.1. Definitions

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.

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 WebTrust for CAs requirements.

Authorized Organizational Representative (AOR): A person (potentially among several) within an organization who is authorized to vouch for non-person identities. Any particular AOR is not permanently linked to any particular non-person identity; the CA MUST only ascertain that the AOR is legitimately associated with the organization, and that the AOR is identified as having authority for the identity in question.

Authorization Domain Name: Means the Domain Name used to obtain authorization for Certificate issuance for a given FQDN.

Basic Constraints: Means an extension that specifies whether the subject of the Certificate MAY act as a CA or only as an end-entity.

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; retrieving Certificates in accordance with their particular intended use; and verification of the domain of an Applicant of a Certificate.

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.

Certificate Systems: Means the system used by Sectigo or a delegated third party in providing identity verification, registration and enrollment, Certificate approval, issuance, validity status, support, and other PKI-related services.

Sectigo Policy Authority: Means the entity charged with the maintenance and publication of this CP.

Domain Name: Means the label assigned to a node in the Domain Name System.

Domain Name Registrant: Means the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar, and sometimes referred to as the "owner" of a Domain Name.

Domain Name Registrar: Means a person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Grace Period: Means the period during which the Subscriber MUST make a revocation request.

Issuing System: Means a system used to sign Certificates or validity status information.

Legal Entity: Means an association, corporation, partnership, proprietorship, trust, government entity, or other entity with legal standing in a country's legal system.

PKI-Customer: An organization that has entered into a business relationship with Sectigo for the hosting and operation of its PKI. The PKI-Customer may operate some on premise PKI components such as the RA servers.

Private Key: Means the key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: Means the key of a key pair that MAY be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Registration Authority (RA): An individual or organization or process responsible for verifying the identity of a Subscriber

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 https://www.sectigo.com/legal/.

Root CA System: Means a system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.

Security Support System: Means a system used to provide security support functions, such as authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and anti-virus.

Subscriber: Means 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.

WebTrust for Certification Authorities: Means the current program for CAs located at http://www.webtrust.org/homepage-documents/item27839.aspx.

X.509: Means the ITU-T standard for Certificates and their corresponding authentication framework

1.6.2. Acronyms

CA: Certificate Authority

CP: Certificate Policy

CPS: Certification Practice Statement

CRL(s): Certificate Revocation List(s)

CSR: Certificate Signing Request

DN: Distinguished Name

DSA: Digital Signature Algorithm

ECDSA: Elliptic Curve Digital Signature Algorithm

FIPS PUB: Federal Information Processing Standards Publication

FQDN: Fully Qualified Domain Name

HSM: Hardware Security Module

HTTP: Hypertext Transfer Protocol

ICANN: Internet Corporation for Assigned Names and Numbers

ITU: International Telecommunication Union

ITU-T: ITU Telecommunication Standardization Sector

NIST: National Institute for Standards and Technology

OCSP: Online Certificate Status Protocol

PIN: Personal Identification Number

PIV-I: Personal Identity Verification Interoperable

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

SAN: Subject Alternate Name

SHA: Secure Hash Algorithm

SSL: Secure Sockets Layer

TLS: Transport Layer Security

TSA: Time Stamping Authority

UTC: Coordinated Universal Time

URL: Uniform Resource Locator

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

Sectigo publishes this CP, Certificate terms and conditions, the Relying Party Agreement and copies of all Subscriber Agreements 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 CP.

Published critical information MAY be updated from time to time as prescribed in this CP. Such updates SHALL be indicated through appropriate version numbering and publication date on any updated version.

2.1. Repositories

Sectigo publishes a repository of legal notices regarding its PKI services, including this CP, agreements and notices, references within this CP, as well as any other information it considers essential to its services. The Repository MAY be accessed at https://www.sectigo.com/legal/.

2.2. Publication of certification information

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

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

Sectigo Ltd.
Attention: Legal Practices,
3rd Floor, 26 Exchange Quay, Trafford Road,
Salford, Greater Manchester, M5 3EQ, United Kingdom
Tel: + 44(0) 161 874 7070
Fax: + 44(0) 161 877 1767

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. Updated or modified versions of the Sectigo IoT CP are published in accordance with section 9.12 of this CP. For CRL issuance frequency, see section 4.9.7 of this CP.

2.4. Access controls on repositories

Documents published in the Repository are for public information and access is freely available. Sectigo has logical access control and version 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 CP and the Sectigo insurance policy.

3. IDENTIFICATION AND AUTHENTICATION

All requirements in this section that relate to verification of Subscriber information is the sole responsibility of the RA unless explicitly stated otherwise in the customer CP/CPS.

3.1. Naming

3.1.1. Types of names

The CA SHALL assign an X.501 Distinguished Name (DN) to each subscriber. This DN MAY or MAY NOT appear in a Certificate field. The subject field in Certificates SHALL be populated with a non-empty X.500 distinguished name as specified in CP Section 3.1.4. The issuer field of Certificates SHALL be populated with a non-empty X.500 Distinguished Name as specified in CP Section 3.1.4.

3.1.2. Need for names to be meaningful

End entity Certificates SHALL contain meaningful names with commonly understood semantics permitting the determination of the identity of the organization that is 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

This CP MAY permit the use of pseudonyms in subscriber common names under certain limited conditions as defined by the PA and specified in the customer CP/CPS. However, an authoritative source to identify the Subscriber must be available. Under normal operating conditions anonymous or pseudonymous Certificates are not issued.

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.

3.1.6. Recognition, authentication, and role of trademarks

CAs operating under this policy SHALL NOT issue a Certificate knowing that it infringes on the trademark of another. Applicants SHALL NOT use names in their Certificate applications that infringe upon the intellectual property rights of others. The CA SHALL NOT be required to determine whether an Applicant has intellectual property rights in the name appearing in a Certificate application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any intellectual property rights, including, without limitation, rights in a domain name, trade name, trademark, or service mark, and the CA SHALL be entitled, without liability to any Applicant, to reject or revoke any Certificate application because of such dispute.

3.1.7. 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 Certificate, other industry requirements, or as prescribed by law.

3.1.8. 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 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.

The CA MAY approve other methods to prove possession of the Private Key by an Applicant.

3.1.9. Authentication of organization identity

Sectigo verifies the identity and address of the Applicant 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 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.

3.1.10. Authentication of Individual Identity

Public key Certificates bind Public Keys to identities. However, the entity to be identified depends on the application for which the Public Keys are used. For instance, in a banking transaction, a Certificate MAY name a bank account holder (i.e., a person). When two networks pass information securely, each communicating part of the network MAY have a Certificate that identifies the device providing the security. Identifying different types of entity requires different evidence and procedures. For each type of entity engaged in the applications that this policy supports, there MUST be a subsection here that details the required evidence and procedure. Four are included here: human, device, application or service, and role holder. Not all PKIs operating under this policy will support all entity types. PKIs operating under this policy MAY support entity types not included here but defined in a customer CP/CPS.

3.1.10.1. Authentication of Natural Person Subscribers

If the Applicant is a natural person, Sectigo verifies the identity and address of the Applicant by:

1. Verifying 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. Verifying 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.

3.1.11. Authentication of Devices

Some computing and communications devices (routers, firewalls, etc.) will be named as Certificate subjects. In such cases, an Authorized Organizational Representative (AOR), or in certain cases the device itself, MUST provide identifying information for the device. The AOR/device is responsible for providing registration information which MAY include:

- Equipment identification (e.g., serial number)
- Equipment Certificate signing request CSR
- Equipment authorizations and attributes (if any are to be included in the Certificate)
- Contact information to enable the CA or RA to communicate with the AOR when required.

The registration information provided by the AOR/device SHALL be verified. If the device itself provides this information, the identity of the device SHALL be authenticated. If the information is provided by an AOR for a single device or batch of devices, the AOR SHALL be authenticated.

3.1.12. Authentication of Applications or Services

This section applies to identities assigned to the services offered via a network, irrespective of the hardware running the software that implements the service. This enables services to be replaced from backup in the event of a hardware failure, without re-provisioning keys.

Some software applications or services will be named as Certificate subjects. In such cases, an AOR MUST provide identifying information for the device. The AOR is responsible for providing registration information which MAY include:

• Unique software application or service name (e.g., DNS name).

• Software application or service CSR.

• Software application or service authorizations and attributes (if any are to be included in the Certificate).

• Contact information to enable the CA or RA to communicate with the AOR when required.

The registration information provided by the AOR SHALL be verified. The CA SHALL validate that the AOR is authorized to request a Certificate for the application or service.

3.1.12.1. Authentication for Role Certificates

A role Certificate SHALL identify a specific role on behalf of which the Subscriber is authorized to act rather than the Subscriber's name. A role Certificate SHALL NOT be a substitute for an individual Subscriber Certificate. Multiple Subscribers can be assigned to a role at the same time.

Subscribers issued role Certificates SHALL protect the corresponding role credentials to the same security level as individual credentials.

The procedures for issuing role Certificates SHALL comply with all other stipulations of this CP (e.g., Subscriber identity proofing, validation of organization affiliation, key generation, Private Key protection, and Subscriber obligations). The AOR MAY act on behalf of the Certificate subject for Certificate management activities such as issuance, renewal, re-key, modification, and revocation.

The CA or the RA SHALL record the information identified in Section 3.2.3.1 for an AOR associated with the role before issuing a role Certificate. The CA or RA SHALL verify the identity of the AOR using an individual Certificate in his or her own name issued by a CA with equivalent assurance as the role Certificate, or other commensurate methods.

AORs SHALL be responsible for:

- Authorizing Subscribers for a role Certificate;
- Recovery of the private decryption key;
- Revocation of Subscribers role Certificates;

- Always maintaining a current up-to-date list of Subscribers who are assigned the role; and
- Always maintaining a current up-to-date list of Subscribers who have been provided the Private Keys for the role.

Note: When determining whether a role Certificate is warranted, consider whether the role carries inherent authority beyond the job title. Role Certificates MAY also be used for Subscribers on temporary assignment, where the temporary assignment carries an authority not shared by the individuals in their usual occupation, for example: "Chair PKI Process Action Team".

3.1.13. Non-verified Subscriber information

Non-verified information MAY be included in Certificates under this policy, such as Organization Unit (OU), however the CA SHALL take steps to ensure that such non-verified information is not misleading.

3.1.14. 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. Before issuing CA Certificates or signature Certificates that assert organizational authority, the CA SHALL validate the Subscriber's authority to act in the name of the organization.

The CA's Certificate issuance process SHALL confirm that the:

- Corporate Contact listed in the Digital Certificate Subscriber Agreement is an officer in the organization who can sign on behalf of the organization and bind the organization to the terms and conditions of the agreement.
- Representative submitting the Digital Certificate Subscriber Agreement and Certificate application is authorized to act on behalf of the organization.
- Administrators listed on the Digital Certificate Subscriber Agreement and Certificate application are authorized to act on behalf of the organization.
- Contacts listed on the Digital Certificate Subscriber Agreement are authorized to act on behalf of the organization.

- For role Certificates that identify subjects by their organizational roles, the CA SHALL validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

3.1.15. Criteria for interoperation

The PA SHALL determine criteria for interoperation with this PKI.

3.2. Identification and authentication for re-key requests

3.2.1. Identification and authentication for routine re-key

CA and Subscriber Certificate re-key SHALL follow the same procedures as initial Certificate issuance. Identity MAY be established using the device's current valid signature key.

3.2.2. Identification and authentication for re-key after revocation

In the event of Certificate revocation, issuance of a new Certificate SHALL always require that the party go through the initial registration process per CP Section 3.1.

3.3. Identification and authentication for revocation request

Revocation requests MUST be authenticated. Requests to revoke a Certificate MAY be authenticated using that Certificate's Public Key, regardless of whether the associated Private Key has been compromised.

Other acceptable procedures for authenticating revocation requests include:

- Having the Subscriber log in to their account and revoking their Certificates via their account portal. The Subscriber will submit their request via their online account, which will employ two-factor authentication, e.g., a USB token with the account administrator's Certificate and a PIN.
- Communication with the Subscriber providing reasonable assurances that the person or organization requesting revocation is, in fact the Subscriber. Such communication SHALL include two or more of the following: telephone confirmation, signed facsimile, signed email, postal mail, or courier service.
- The representative is the Corporate Contact, Administrator, Legal, or Technical contact authenticated in CP section 3.2.5.
- If requested by the automated RA in the case of the automated issuance of end-entity Certificates.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

All requirements in this section that relate to verification of Subscriber information is the sole responsibility of the PKI Customer/RA unless explicitly stated otherwise in the customer CP/CPS.

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.
- Establish and record identity of the applicant.
- Obtain the applicant's Public Key and verify the applicant's possession of the Private Key for each Certificate required.
- 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 for the CA and applicants that does not compromise security, but all MUST be completed before Certificate issuance.

The CA and/or RA SHALL include the processes, procedures, and requirements of their Certificate application process in their CPS.

4.1.1. Who can submit a Certificate application

An application for a CA Certificate SHALL be submitted by an authorized representative of the applicant CA.

A Subscriber Certificate application SHALL be submitted to the CA by the Subscriber, AOR, or an RA on behalf of the Subscriber. Multiple Certificate requests from one RA or AOR MAY be submitted as a batch.

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

4.2. Certificate application processing

Information in Certificate applications MUST be verified as accurate before Certificates are issued. Procedures to verify information in Certificate applications SHALL be specified in the CPS.

4.2.1. Performing identification and authentication functions

The identification and authentication of the Subscriber SHALL meet the requirements specified for Subscriber authentication. The components of the PKI (e.g., CA or RA) that are responsible for authenticating the Subscriber's identity in each case SHALL be identified in the CPS.

4.2.2. Approval or rejection of Certificate applications

Any Certificate application that is received by the CA under this policy, for which the identity and authorization of the applicant has been validated, will be duly processed. However, the CA SHALL reject any application for which such validation cannot be completed, or when the CA has cause to lack confidence in the application or certification process.

Sectigo reserves the right to reject an application to issue a Certificate to an Applicant if, in Sectigo's sole opinion, by issuing a Certificate to such Applicant the good and trusted name of Sectigo might be 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.

An Applicant whose application has 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.

4.2.3. Time to process Certificate applications

Sectigo makes reasonable efforts to confirm Certificate application information and issue a Certificate within a reasonable time frame. The time frame is greatly dependent on the type of Certificate and the verification requirements as stated in the CPS or customer CP/CPS.

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.

4.2.4. Certificate Authority Authorization (CAA)

No stipulation.

4.3. Certificate issuance

4.3.1. CA actions during Certificate issuance

Upon receiving the request, the CAs/RAs shall:

- Verify the identity of the requester as specified in Section 3.
- Verify the authority of the requester and the integrity of the information in the Certificate request as specified in Section 4.1.
- Build and sign a Certificate if all Certificate requirements have been met (in the case of an RA, have the CA sign the Certificate).
- Make the Certificate available to the Subscriber after confirming that the Subscriber has formally acknowledged their obligations as described in Section 9.6.3.

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.

Sectigo's automated (and manual) 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.

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

CAs operating under this policy SHALL inform the Subscriber (or other Certificate subject) of the creation of a Certificate and make the Certificate available to the Subscriber. Certificates SHALL be made available to Subscribers, via download from the CA web site. For device Certificates, the CA SHALL issue the Certificate according to the Certificate requesting protocol used by the device (this MAY be automated) and, if the protocol does not provide inherent notification, also notify the authorized organizational representative of the issuance (this MAY be in batch).

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

Before a Subscriber can make effective use of its Private Key, the CA 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

The following conduct constitutes Certificate acceptance by the Subscriber:

- Downloading a Certificate
- Failing to object timely to the Certificate or its content

4.4.2. Publication of the Certificate by the CA

As specified in Section 2.1, all CA Certificates SHALL be published in repositories.

This policy makes no stipulation regarding publication of end entity Certificates, except as noted in Section 9.4.3

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.

4.5. Key pair and Certificate usage

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 to rely on a verified digital signature is exclusively that of the Relying Party. Certificates MAY specify restrictions on use through critical Certificate extensions, including the basic constraints and key usage extensions. All CAs enabled for revocation operating under this policy SHALL issue CRLs and MAY provide OCSP responses specifying the status of all unexpired Certificates except for OCSP responder Certificates. It is recommended that relying parties process and comply with this information whenever using Certificates in a transaction.

Some CAs operating under this policy may choose not to be enabled for revocation and in such case CRLs and OCSP responses will not be issued.

4.6. Certificate renewal

Certificate renewal is the issuance of a new Certificate for an existing key pair without changing any information in the Certificate except the validity period and serial number.

Using a key pair beyond its intended lifetime can increase its vulnerability to attack. CA Certificates SHOULD NOT be renewed in this manner. End entity Certificates MAY be renewed as long as the Subject is notified of the security risks.

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.

4.6.2. Who MAY request renewal

The Subscriber, RA, or AOR MAY request the renewal of a Subscriber Certificate.

4.6.3. Processing Certificate renewal requests

For a Certificate renewal request the identity of the Applicant SHALL be confirmed in accordance with the requirements specified in Section 3.

4.6.4. Notification of new Certificate issuance to Subscriber

As per Section 4.3.2.

4.6.5. Conduct constituting acceptance of a renewal Certificate

As per Section 4.4.1.

4.6.6. Publication of the renewal Certificate by the CA

As per Section 4.4.2.

4.6.7. Notification of Certificate issuance by the CA to other entities

As per Section 4.4.3.

4.7. Certificate re-key

Re-keying a Certificate consists of creating new Certificates with a different Public Key (and serial number and key identifier) while retaining the remaining contents of the old Certificate that describe the subject. The new Certificate MAY be assigned a different validity period, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a Certificate does not require a change to the subjectName and does not violate the requirement for name uniqueness.

An old Certificate MAY or MAY NOT be revoked, but SHALL NOT be further re-keyed, renewed, or modified.

Subscribers SHALL identify themselves for the purpose of re-keying as required in Section 3.3.

4.7.1. Circumstance for Certificate re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtain new keys. (Section 6.3.2 establishes usage periods for Private Keys for both CAs and Subscribers.) 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

Requests for certification of a new Public Key SHALL be considered as follows:

- Subscribers with a currently valid Certificate MAY request certification of a new Public Key.
- CAs and RAs MAY request certification of a new Public Key on behalf of a Subscriber.
- For device, application/service, or role Certificates, an AOR that owns or controls the device MAY request re-key.

4.7.3. Processing Certificate re-keying requests

For Certificate re-key, the CA SHALL confirm the identity of the Subscriber in accordance with the requirements specified in Section 3 for the authentication of an original Certificate Application.

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

4.7.4. Notification of new Certificate issuance to Subscriber

As per Section 4.3.2.

4.7.5. Conduct constituting acceptance of a re-keyed Certificate

As per Section 4.4.1.

4.7.6. Publication of the re-keyed Certificate by the CA

As per Section 4.4.2.

4.7.7. Notification of Certificate issuance by the CA to other entities

As per Section 4.4.3.

4.8. Certificate modification

Sectigo does not offer Certificate modification. Instead, Sectigo MAY revoke the old Certificate and issue a new Certificate as a replacement.

4.8.1. Circumstance for Certificate modification

Not applicable.

4.8.2. Who May Request Certificate Modification
Not applicable.

4.8.3. Processing Certificate modification requests
Not applicable.

4.8.4. Notification of new Certificate issuance to Subscriber
Not applicable.

4.8.5. Conduct constituting acceptance of modified Certificate
Not applicable.

4.8.6. Publication of the modified Certificate by the CA
Not applicable.

4.8.7. Notification of Certificate issuance by the CA to other entities
Not applicable.

4.9. Certificate revocation and suspension
CAs enabled for revocation operating under this policy SHALL issue CRLs, and MAY provide OCSP responses covering all unexpired Certificates issued under this policy except for OCSP responder. Some CAs operating under this policy MAY choose not to be enabled for revocation and in such case CRLs and OCSP responses will not be issued.

CAs with revocation enabled operating under this policy SHALL publish a description of how to obtain revocation information for the Certificates they issue, and an explanation of the consequences of using outdated revocation information. This information SHALL be given to Subscribers during Certificate request or issuance and SHALL be readily available to any potential relying party.

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 on all new publications of the Certificate status information until the Certificates expire.

Sectigo MAY revoke a Certificate if any of the following occur:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the Private Key associated with the Certificate;
- The Subscriber or Sectigo has breached a material obligation under this CP or the relevant Service Contract or Subscriber Agreement;
- Either the Subscriber's or Sectigo's obligations under this CP 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;
- There has been a modification of the information pertaining to the Subscriber that is contained within the Certificate;
- 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;
- A Subscriber's Digital Certificate has not been issued in accordance with the policies set out in this CP;
- The Subscriber has used the Subscription Service 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; or
- The Certificate, if not revoked, will compromise the trust status of Sectigo.

4.9.2. Who can request revocation

Revocation requests MAY be made by:

- The Subscriber of the Certificate or any authorized representative of the Subscriber
- The CA, or affiliated RA, for Certificates within its domain
- The Policy Authority

Other parties MAY report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, inappropriate conduct, or any other matter related to Certificates, in the first instance, by email to sslabuse@sectigo.com.

4.9.3. Procedure for revocation request

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 indicated in section 3 of this CP.

4.9.4. Revocation request grace period

There is no revocation grace period under this policy. Revocation requests SHOULD be submitted as promptly as possible within a reasonable time of becoming aware of a revocation circumstance listed in CP section 4.9.1.

4.9.5. Time within which CA MUST process the revocation request

Revocation request SHALL be processed within twenty-four (24) hours of receipt of request.

4.9.6. Revocation checking requirement for relying parties

Use of revoked Certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data SHOULD be obtained is a determination to be made by the Relying Party and the system accreditor. If it is not possible to obtain revocation information, whether due to a temporary outage or the CA not being enabled for revocation, the Relying Party MUST either reject use of the Certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a Certificate whose authenticity cannot be guaranteed to the standards of this CP. Such use MAY occasionally be necessary to meet urgent operational requirements.

4.9.7. CRL issuance frequency (if applicable)

CAs enabled for revocation operating under this policy SHALL issue CRLs periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information MAY be issued more frequently than the issuance frequency described below. A CA SHALL ensure that superseded Certificate status information is removed from the PKI repository upon posting of the latest Certificate status information.

Certificate status information SHALL be published no later than the next scheduled update. This will facilitate the local caching of Certificate status information for offline or remote operation.

PKI Participants SHALL coordinate with the PKI repositories to which they post Certificate status information to reduce latency between creation and availability.

The following table provides CRL issuance frequency requirements of CAs for which revocation is enabled.

Routine	At least once every 7 days
Loss/Compromise of Private Key	Within 24 hours of notification
CA Compromise	Immediately, but no later than 18 hours after notification

4.9.8. Maximum latency for CRLs (if applicable)

Sectigo does not employ a maximum latency for CRLs. However, generally CRLs will be published within one (1) hours of generation. Each CRL SHALL be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

4.9.9. On-line revocation/status checking availability

The latency of online Certificate status information distributed by the CA or its delegated status responders SHALL meet or exceed the requirements for CRL issuance stated in Section 4.9.7.

4.9.10. On-line revocation checking requirements

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

4.9.11. Other forms of revocation advertisements available

No stipulation.

4.9.12. Special requirements regarding key compromise

In the event of Compromise or suspected Compromise of the CA signing key, senior management of the CA Operator and any cross-certified CAs SHALL be immediately notified. A CRL MUST be issued within eighteen (18) hours of notification. The requirements of Section 4.9.7 also apply.

CA Compromise	Immediately, but no later than 18 hours after notification

4.9.13. Circumstances for suspension
Certificate suspension is not supported by this CP.

4.9.14. Who can request suspension
Certificate suspension is not supported by this CP.

4.9.15. Procedure for suspension request
Certificate suspension is not supported by this CP.

4.9.16. Limits on suspension period
Certificate suspension is not supported by this CP.

4.10. Certificate status services

4.10.1. Operational characteristics
For CAs enabled for revocation, Certificate status SHALL be available via CRL through a URL specified in the CPS or customer CP/CPS, and MAY be available via LDAP directory or OCSP responder.

4.10.2. Service availability
Certificate status services are available 24/7.

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 Service Contract or Subscriber Agreement terminates or expires without renewal.

4.12. Key escrow and recovery

4.12.1. Key escrow and recovery policy and practices

No stipulation. MAY be specified in customer CP/CPS.

4.12.2. Session key encapsulation and recovery policy and practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

All CA and RA equipment, SHALL be protected from theft, loss, and unauthorized access at all times. Unauthorized use of CA and RA equipment is prohibited. CA equipment SHALL be dedicated to performing CA functions. RA equipment SHALL be operated to ensure that the equipment meets all physical controls at all times.

5.1. Physical controls

All CA systems SHALL be protected from unauthorized access. The CA SHALL implement physical Access Controls to reduce the risk of equipment tampering even when the HSM is not installed and/or activated. All CA systems SHALL be protected against theft, loss, and unauthorized use.

All 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

All CA systems SHALL 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).

The CA SHALL construct the facilities housing their operational and standby CA functions with at least four physical security tiers. CAs SHALL perform all validation operations within Tier 2 or higher. CAs SHALL place 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.

Site Location and Construction SHALL be described in more detail in the CPS.

5.1.2. Physical access

5.1.2.1. Physical Access for CA Equipment

Access to each tier of physical security, constructed in accordance with CP section 5.1.1, SHALL be auditable and controlled so that only authorized personnel can access each tier.

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 Sectigo's entrances and exits are secured or monitored by security personnel, reception staff, or monitoring/control systems.

5.1.2.2. Physical Access for RA Equipment

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

The CA facilities SHALL be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these facilities SHALL be equipped with primary and backup heating/ventilation/air conditioning systems for temperature control.

The CA facilities SHALL 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

CA facilities SHALL be constructed, equipped and installed, and procedures SHALL be implemented, to prevent floods or other damaging exposure to water. Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5. Fire prevention and protection

CA facilities SHALL be constructed and equipped, and procedures SHALL be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures SHALL meet all local applicable safety regulations.

5.1.6. Media storage

CA media SHALL be stored to protect them from accidental damage (e.g., water, fire, or electromagnetic) and unauthorized physical access. Media that contains audit, Archive, or backup information SHALL be duplicated and stored in a location separate from the CA location.

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

CA and Operations Staff and RA Staff SHALL remove and destroy normal office waste in accordance with local policy. Media used to collect or transmit privacy information SHALL be destroyed, such that the information is unrecoverable, prior to disposal. 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 specified in the NIST Special Publication 800-88.

5.1.8. Off-site backup

Sectigo backs up its information to secure, off-site locations which are sufficiently distant from each other to escape potential damage from a disaster at the primary location effecting a backup 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 are appropriately labeled according to the sensitivity of the information.

Requirements for CA Private Key backup are specified in Section 6.2.4.

5.2. Procedural controls

5.2.1. Trusted roles

Trusted roles are assigned by senior members of the management team who assign 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.

Persons acting in trusted roles are only allowed to access a Certificate Management System (CMS) after they are authenticated using a method approved as being suitable for the control of PIV-I Hardware.

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 CP 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 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 CP and, where relevant, an RA's contract.

5.2.1.5. RA Staff

RA Staff are the individuals holding trusted roles that operate and manage RA components.

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 CA cryptographic modules SHALL be strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a CA is activated with operational keys, further Access Controls SHALL be invoked to maintain split control over both physical and logical access to the CA.

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.

No single person has the capability to issue a PIV-I credential.

5.2.3. Identification and authentication for each role

The CA 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.

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 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 person control.

An individual that performs any trusted role shall only have one identity when accessing CA equipment.

Role separation, when required as mentioned above, MAY be enforced by either the CA equipment, or procedurally, or by both means.

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

Consistent with this CP, 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. 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.

5.3.2. Background check procedures

All trusted personnel have background checks before access is granted to Sectigo's systems. 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 CP.

CA Administrators and 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.

5.3.4. Retraining frequency and requirements

The CA 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.

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. The CA SHOULD only use contractors or consultants as Trusted Persons if the CA does not have 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.

Contractors fulfilling trusted roles are subject to all personnel requirements stipulated in this policy and SHALL establish procedures to ensure that any subcontractors perform in accordance with this policy.

Once the independent contractor completes the work for which it was hired, or the independent contractor's employment is terminated, physical access rights assigned to that contractor are removed as soon as possible and within 24 hours 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.

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

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, 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
- Custody of keys and of devices and media holding keys
- Compromise of a Private Key

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 HSM events, such as usage, de-installation, service or repair and retirement
- Successful and unsuccessful Sectigo PKI access attempts
- Secure CA facility 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
- Method of entry
- Source of entry
- Identity of entity making log entry

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 at least 2 years and MUST be retained in the manner described below. For the RA, a system administrator other than the RA SHALL be responsible for managing the audit log.

5.4.4. Protection of audit log

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

Both current and 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.

5.4.6. Audit collection system (internal vs. external)

Automatic audit collection processes run from system startup to system shutdown. The failure of an automated audit 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.

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.

Sectigo employs external parties to perform regular vulnerability scans & penetration testing on our CA systems/infrastructure.

5.5. Records archival

Sectigo implements an archive standard for all business-critical systems located at its data centers. Sectigo retains records in electronic or paper-based formats in conformance with this subsection of this CP.

5.5.1. Types of records archived

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

- Audit data, as specified in section 5.4 of this CP;
- 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 the records of Sectigo Certificates and the associated documentation for a term of not less than 7 years, 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

CA 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. The CPS SHALL describe how system clocks used for time-stamping are 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 CP.

5.5.7. Procedures to obtain and verify archive information

Procedures, detailing how to create, verify, package, transmit, and store Archive information, SHALL be described in the applicable CPS.

5.6. Key changeover

Towards the end of each Private Key's lifetime, a new CA signing key pair is commissioned. 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 in the CPS.

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. 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.

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 co-location facilities run by independent commercial data center providers, 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 at 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 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 CP.
- 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

6.1. Key pair generation and installation

6.1.1. Key pair generation

CA Key pair generation SHALL be performed using FIPS 140-2 Level 3 validated cryptographic modules and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of Private Keys. Any pseudo-random numbers use and parameters for key generation material SHALL be generated by a FIPS-approved method.

CA keys SHALL be generated in a Key Generation Ceremony using multi-person control for CA key pair generation, as specified in Section 6.2.2.

CA key pair generation SHALL create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure SHALL be detailed enough to show that appropriate role separation was used. An independent third party SHALL validate the execution of the key generation procedures either by witnessing the key generation or by examining the video, signed and documented record of the key generation.

6.1.2. Private key delivery to Subscriber

Subscriber key pair generation SHALL be performed by the Subscriber or CA. If the Subscribers themselves generate Private Keys, then Private Key delivery to a Subscriber is unnecessary.

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, the CA SHALL NOT retain any copy of the key for more than two weeks after delivery of the Private Key to the Subscriber.
- CAs SHALL use FIPS certified systems and deliver Private Keys to Subscribers via SSL/TLS and SHALL secure such delivery through the use of a PKCS#8 package or, at the CAs sole discretion, any other comparably equivalent means (e.g., PKCS#12 package) in order to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys.
- 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.
    - For hardware modules, accountability for the location and state of the module SHALL be maintained until the Subscriber accepts possession of it.
    - For electronic delivery of Private Keys, the key material SHALL be encrypted using a cryptographic algorithm and key size at least as strong as the Private Key. Activation data SHALL be delivered using a separate secure channel.

6.1.3. Public key delivery to Certificate issuer

When a Public Key is transferred to the issuing CA to be certified, it SHALL be delivered through a mechanism validating the identity of the Subscriber and ensuring that the Public Key has not been altered during transit and that the Certificate Applicant possesses the Private Key corresponding to the transferred Public Key. The Certificate Applicant SHALL deliver the Public Key in a PKCS#10 CSR or an equivalent method ensuring that the Public Key has not been altered during transit; and the Certificate Applicant possesses the Private Key corresponding to the transferred Public Key. The Certificate Applicant will submit the CSR via their online account, which employs two-factor authentication, e.g., a USB token with the account administrator's Certificate and a PIN (this procedure is not applicable in the case of the automated issuance of end entity Certificates).

6.1.4. CA Public Key delivery to relying parties

The Public Key of a trust anchor SHALL be provided to the Device Sponsors acting as Relying Parties in a secure manner so that the trust anchor is not vulnerable to modification or substitution. Acceptable methods for delivery of a trust anchor include but are not limited to:

- Loading a trust anchor onto tokens delivered to Relying Parties via secure mechanisms;
- Secure distribution of trust anchor through secure out-of-band mechanisms;
- Comparison of Certificate hash (fingerprint) against the trust anchor hash made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the Certificate are not acceptable as an Authentication mechanism); and

- Downloading a trust anchor from trusted web sites (e.g., CA web site) secured with a currently valid Certificate of equal or greater assurance level than the Certificate being downloaded and the trust anchor is not in the Certificate Chain for the web site Certificate.

Systems using cryptographic hardware tokens SHALL store trusted Certificates such that unauthorized alteration or replacement is readily detectable.

6.1.5. Key sizes

This CP 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.

RSA signatures on CRLs that only provide status information for Certificates that were generated using SHA-1 MAY continue to be generated using SHA-1.

Where implemented, CSSs SHALL sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs.

6.1.6. Public key parameters generation and quality checking

Sectigo generates the Public Key parameters. Sectigo's CA keys are generated within a FIPS 140-2 Level 3 certified HSM.

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:

- Digital signature, for verifying digital signatures that is, for entity authentication and data origin authentication with integrity
- Non-repudiation, for verifying digital signatures used in providing a nonrepudiation service which protects against the signing entity falsely denying some action
- Key encipherment, for enciphering keys or other security information, e.g. for key transport
- Data encipherment, for enciphering user data, but not keys or other security information
- Key agreement, for use as a Public Key agreement key
- Key Certificate signing, for verifying a CA's signature on Certificates, used in CA Certificates only
- CRL signing, for verifying a CA's signature on CRLs
- Encipher only, Public Key agreement key for use only in enciphering data when used with key agreement
- 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 of the CPS does not indicate that Sectigo does or will issue a certificate with that key usage.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

CA Private keys within this PKI SHALL be protected using FIPS 140-2 Level 3 systems. Private key holders SHALL take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with this CP and any existing contractual obligations.

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules:

- Root CAs SHALL perform all CA cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-2 level 3.
- Sub-CAs SHALL use a FIPS 140-2 Level 3 or higher validated hardware cryptographic module.
- Subscribers SHOULD use a FIPS 140-2 Level 1 or higher validated cryptographic module for their cryptographic operations.

6.2.2. Private key (n out of m) multi-person control

Multi-person control is enforced to protect the activation data needed to activate CA Private Keys so that a single person SHALL NOT be permitted to activate or access any cryptographic module that contains the complete CA private signing key.

CA signature keys SHALL be backed up only under multi-person control. Access to CA signing keys backed up for disaster recovery SHALL be under multi-person control. The names of the parties used for multi-person control SHALL be maintained on a list that SHALL be made available for inspection during compliance audits.

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. Backup procedures SHALL be included in the CA's CPS.

For CA Root key recovery purposes, the Root CA signing keys are encrypted, split and stored within a secure environment under multi-person control.

End entity Private Keys MAY be backed up or copied but SHALL be held under the control of the Subscriber or other authorized administrator. Backed up end entity Private Keys SHALL NOT be stored in plaintext form and storage SHALL ensure security controls consistent with the security specifications the device is compliant with. Subscribers MAY have the option of using enhanced Private Key protection mechanisms available today including the use of smart cards, biometric access devices, and other hardware tokens to store Private Keys.

6.2.5. Private key archival

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 CP.

6.2.6. Private key transfer into or from a cryptographic module

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

6.2.7. Private key storage on cryptographic module

Private Keys are generated and stored inside Sectigo's Hardware Signing Modules (HSMs), which have been certified to at least FIPS 140-2 Level 3.

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

6.2.8. Method of activating Private Key

All CAs SHALL protect the activation data for their Private Keys against loss, theft, modification, disclosure, or unauthorized use.

CA administrators SHALL be authenticated to the cryptographic token before the activation of the associated Private Key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data SHALL be protected from disclosure (i.e., the data SHOULD NOT be displayed while it is entered).

For device Certificates, the device MAY be configured to activate its Private Key, provided that appropriate physical and logical access controls are implemented for the device. The strength of the security controls SHALL be commensurate with the level of threat in the device's environment, and SHALL protect the device's hardware, software, Private Keys and its activation data from compromise.

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.

6.2.8.4. Device Private Keys

A Device MAY be configured to activate its Private Key, provided that appropriate physical and logical Access Controls are implemented for the Device. The strength of the security controls SHALL be commensurate with the level of threat in the Device's environment, and SHALL protect the Device's hardware, software, Private Keys and its activation data from compromise. If the Private Key is stored in a protected form using password based encryption, then the password or pass-phrase activation data MUST be entered each time the Device and the security application are initialized in order to unlock the Private Key for operational use.

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, the CA 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 Ceremony, in which such Private Keys are used for Private Key operations, the CA SHALL remove the activation tokens from the HSM containing the Private Keys in order to deactivate them. Once the activation tokens have been removed from the reader, they SHALL be securely stored.

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 SHALL comprise of removing it from the HSM and removing it from the active backup set. Private Keys are destroyed in accordance with NIST SP 800-88.

6.2.11. Cryptographic Module Rating

See section 6.2.1.

6.3. Other aspects of key pair management

6.3.1. Public key archival

The Public Key is archived as part of the Certificate archival. The issuing CA SHALL retain all verification Public Keys for a minimum of seven (7) years or as further required by applicable law or industry regulation.

6.3.2. Certificate operational periods and key pair usage periods

Generally, the Certificate validity period will be set as follows, however, Sectigo reserves the right to offer validity periods outside of this standard. Additionally, a PKI Customer CP or CPS MAY specify other validity periods.

- Root CA Certificates MAY have a validity period of up to 25 years
- Sub-CA Certificates MAY have a validity period of up to 15 years
- End entity Certificates MAY have a validity period of up to 5 years

Validity periods SHALL be nested such that the validity periods of issued Certificates SHALL be contained within the validity period of the issuing CA.

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 is certified by FIPS 140-2.

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 online Root CA Systems in a high security zone;
- Maintaining offline Root CAs 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 Systems 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.

6.5.2. Computer security rating

No stipulation.

6.6. Life cycle 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 have any access to the production environment. 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. Life cycle security controls

No stipulation.

6.7. Network security controls

Sectigo develops, implements, and maintains a comprehensive security program designed to protect its networks. In this security program, general protections for the network include:

- 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.
- Default deny policy unless explicity authorized for all access.
- Any services that are not required for the correct functionality of the services provided by a system are either:
    - Not installed where the installation process allows.
    - Disabled where they are installed/enabled by default

6.8. Time-stamping

All CA and CSA 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 CSA responses.

Certificates, CRLs, and other revocation database entries SHALL contain time and date information. Asserted times SHALL be accurate to within three (3) minutes. Electronic or manual procedures MAY be used to maintain system time. Clock adjustments are auditable events (see Section 5.4.1).

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate profile

Certificates SHALL conform to RFC 5280 & 6818. Text fields are encoded using printableString encoding whenever possible and utf8String encoding if necessary.

Certificates SHALL contain the identity and attribute data of a subject using the base Certificate with applicable extensions. The base Certificate SHALL contain the version number of the Certificate, the Certificate's identifying serial number, the signature algorithm used to sign the Certificate, the issuer's distinguished name, the validity period of the Certificate, the subject's distinguished name, information about the subject's Public Key, and extensions as defined in the Sectigo IoT CPS or a customer CP/CPS.

7.1.1. Version number(s)

Sectigo Certificates SHALL be X.509 v3 Certificates. The Certificate version number SHALL be set to the integer value of "2" for Version 3 Certificates.

7.1.2. Certificate extensions

As described in the Sectigo IoT CPS or a customer CP/CPS.

7.1.3. Algorithm object identifiers

Sectigo Certificates are signed using algorithms including but not limited to RSA and ECDSA. Additional detail MAY be found in the Sectigo IoT CPS or a customer CP/CPS.

7.1.4. Name forms

As specified in Section 3.1.1.

7.1.5. Name constraints

No stipulation.

7.1.6. Certificate policy object identifier

As specified in the Sectigo IoT CPS or customer CP/CPS.

7.1.7. Usage of Policy Constraints extension

No stipulation.

7.1.8. Policy qualifiers syntax and semantics

A common use of policy qualifiers is to provide location information (e.g., URI) for a Certificate policy. If this is desirable usage will be specified in the Sectigo IoT CPS or a customer CP/CPS.

7.1.9. Processing semantics for the critical Certificate Policies extension

Processing semantics for the critical Certificate policy extension SHALL conform to X.509 certification path processing rules.

7.2. CRL profile

For CAs which have been enabled for revocation 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 every 24 hours or more frequently under special circumstances. 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.

As previously stated in this CP, some CAs operating under this policy MAY choose to not be enabled for revocation, and in such case CRLs and OCSP responses will not be issued.

The profile of the Sectigo IoT CRL MAY be as per the table below:

Version	[Value 1]	
Issuer Name	Issuer DN, for example: CountryName = [Root Certificate Country Name], OrganizationName=[Root Certificate Organization], CommonName=[Root Certificate Common Name] [PrintableString encoding] OR [UTF8String encoding]	
This Update	[Date of Issuance]	
Next Update	End Entity Certificates: [<= Date of Issuance + 10 days] Sub CA Certificates: [<= Date of Issuance + 12 months]	
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

7.3. OCSP profile

For CAs which are configured for revocation, Sectigo MAY publish 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 CP. If queried for a certificate which was not issued by Sectigo the responder will provide 'unauthorized'. The OCSP responders will give an 'unknown' response for expired Certificates.

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.

7.3.1. Version number(s)

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

7.3.2. OCSP extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices specified in this CP have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the WebTrust for Certification Authorities ("WebTrust for CAs") and other industry standards related to the operation of CAs.

A regular audit is performed by an independent external auditor to assess Sectigo's compliancy with the WebTrust for CAs.

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

This audit is 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:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in a WebTrust for Certification Authorities v2.0;
- 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;
- licensed by WebTrust;
- Bound by law, government regulation, or professional code of ethics; and
- 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 WebTrust for CAs annual audit MAY include but are not limited to the following:

- Business Practices Disclosure, meaning
    - the CA discloses its business practices, and
    - the CA provides its services in accordance with its CPS.
- Key Lifecycle Management, meaning
    - 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
    - The CA maintains effective controls to provide reasonable assurance that Subscriber information was properly authenticated for specific registration activities, and
    - The CA maintains effective controls to provide reasonable assurance that subordinate CA Certificate requests are accurate, authenticated, and approved.
- CA Environmental Control, meaning that
    - 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.

8.5. 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 about Certificates already issued.

8.6. Communication of results

The audit requires that Sectigo make the Audit Report available to the public. Sectigo is not required to make publicly available any general audit finding that does not impact the overall audit opinion.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

Sectigo charges Subscriber fees for some of the Certificate services it offers. Sectigo retains its right to make changes to such fees. Sectigo partners will be advised of price amendments as detailed in their respective 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 SHALL not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties, but 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 the 30-day period, beginning when a Certificate is first issued, the Subscriber MAY request a full refund for their Certificate. Under such circumstances, Sectigo MAY revoke the original Certificate and MAY provide a refund to the Subscriber. Sectigo is not obliged to refund a Certificate after the 30-day refund period has expired.

9.2. Financial responsibility

9.2.1. Insurance coverage

Sectigo maintains insurance coverage from reputable, financially sound insurers with appropriate limits that equal or exceed industry norms.

9.2.2. Other assets

No stipulation.

9.2.3. Insurance or extended warranty coverage

No stipulation.

9.3. Confidentiality of business information

Sectigo observes applicable rules on the protection of personal data deemed by law or by Sectigo's privacy policy (see section 9.4.1 of this CP) 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.

- Executed 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 WebTrust audit reports that MAY be published at the discretion of Sectigo.
- Private Keys.
- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of Sectigo infrastructure, Certificate management and enrolment services and data.

9.3.2. Information not within the scope of confidential information

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

9.3.3. Responsibility to protect confidential information

All personnel in trusted positions handle all confidential information in strict confidence. Personnel of RA/LRAs especially MUST comply with the requirements of English law on the protection of personal data.

9.4. Privacy of personal information

9.4.1. Privacy plan

Sectigo has implemented adequate privacy safeguards and protections, and follows its published Privacy Policy, which complies with this CP and applicable law.

9.4.2. Information treated as private

See 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 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 obtain an Applicant's, or Subscriber's, consent to use private information as required by applicable laws or regulations.

9.4.6. Disclosure pursuant to judicial or administrative process

Sectigo's disclosure of information pursuant to judicial or administrative process is stated in the Privacy Policy. Sectigo reserves the right to disclose 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

No stipulation.

9.5. Intellectual property rights

Sectigo, or its subsidiaries, affiliates, licensors, or associates, own all intellectual property rights in Sectigo's services, including databases, web sites, Sectigo Certificates and any other publication originating from Sectigo, including this CP.

9.6. Representations and warranties

9.6.1. CA representations and warranties

Sectigo makes certain representations regarding Certificate services performed pursuant to this CP, 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 CP, or in a separate agreement with Subscriber, to the extent specified in the relevant sections of the CP, Sectigo represents to:

- Comply with this CP 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 available.
- Issue Certificates in accordance with this CP and fulfill its obligations presented herein.
- Upon receipt of a request from an RA operating within the Sectigo network, act promptly to issue a Certificate in accordance with this CP.

- 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 CP.
- Publish accepted Certificates in accordance with this CP.
- Revoke Certificates in accordance with this CP.
- Provide for the expiration and renewal of Certificates in accordance with this CP.

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 policies and in accordance with this CP.

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

9.6.2. RA representations and warranties

Sectigo's RAs operate under the policies and practices detailed in this CP and also the associated agreement. In addition to the representations and warranties made in the applicable agreement between Sectigo and an RA, an RA represents and warrants to:

- Receive applications for Sectigo Certificates in accordance with this CP.
- Maintain its operations in conformance to the stipulations of this CP
- Perform all verification actions prescribed by the Sectigo validation procedures and this CP.
- Receive, verify, and relay to Sectigo all requests for revocation of a Sectigo Certificate in accordance with the Sectigo revocation procedures and this CP.
- Act in compliance with all applicable laws and regulations.

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, warrants, and covenants to Sectigo and to Relying Parties that at the time of acceptance and until further notice, to do each of the following:

- provide accurate and complete information at all times to Sectigo in the Certificate request and as otherwise requested in connection with the issuance of Certificates;
- install and use each Certificate 1) only on domains owned or controlled by Subscriber and 2) only on the server(s) accessible at the domain name listed in the Certificate if the Certificate is a server Certificate;
- use the Certificates only for the purposes listed in this CP;
- review and verify the accuracy of the data in each Certificate prior to installing and using the Certificate, and immediately inform Sectigo if any data listed in a Certificate changes or ceases to be accurate;
- be responsible, at Subscriber's expense, for 1) all computers, telecommunication equipment, software, access to the Internet, and communications networks (if any) required to use the Certificates, 2) Subscriber's conduct and its website maintenance, operation, development, and content;
- promptly inform Sectigo if Subscriber becomes aware of any misuse of the Certificates and assist Sectigo in preventing, curing, and rectifying any misuse;
- take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in a Certificate;
- immediately cease using a Certificate and the related Private Key and request revocation of the Certificate if 1) any information in the Certificate is or becomes incorrect or inaccurate, or 2) there is any actual or suspected misuse or compromise of the Private Key associated with the Certificate;
- cease all use of the Certificate and its Private Key upon expiration or revocation of the Certificate;
- comply with all regulations, policies, and procedures of its networks while using Certificates;

- obtain and keep in force any consent, authorization, permission or license that MAY be required for Subscriber's lawful use of the Certificates;
- abide by all applicable laws, rules, regulations, and guidelines when using a Certificate;
- The Subscriber retains control of the Private Key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use; and
- 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.

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 and acknowledges that in order to reasonably rely on a Sectigo Certificate, such party 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 Certificates and PKI.
- Not use a Certificate, or rely upon a Certificate, as control equipment in hazardous circumstances or circumstances requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, weapon control systems, or where failure could lead directly to death, personal injury, or severe environment damage, each of which is an unauthorized use of a Certificate and for which a Certificate is neither designed nor intended.
- Study the limitations to the usage of Certificates and be aware through the Relying Party agreement the maximum value of the transactions that can be made using a Sectigo Certificate.
- Read and agree with the terms of the Sectigo CP 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 Certificate only if it is valid and has not been revoked or has expired.
- Rely on a Certificate, only as MAY be reasonable under the circumstances listed in this section and other relevant sections of this CP.

9.6.5. Representations and warranties of other participants

No Stipulation.

9.7. Disclaimers of warranties

9.7.1. Fitness for a Particular Purpose

EXCEPT AS STATED IN THIS CP, AND TO THE EXTENT PROHIBITED BY LAW, SECTIGO DISCLAIMS ALL IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE IN THE CERTIFICATES AND RELATED SERVICES, INCLUDING ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY OF THE ACCURACY OF UNVERIFIED INFORMATION PROVIDED.

THE CERTIFICATES AND RELATED SERVICES ARE NOT TO BE USED FOR, OR RELIED UPON AS, CONTROL EQUIPMENT IN HAZARDOUS CIRCUMSTANCES OR CIRCUMSTANCES REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL SYSTEMS, WEAPONS CONTROL SYSTEMS, OR WHERE FAILURE COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE ENVIRONMENTAL DAMAGE, EACH OF WHICH IS AN UNAUTHORIZED USE OF A CERTIFICATE AND FOR WHICH A CERTIFICATE IS NEITHER DESIGNED NOR INTENDED.

9.7.2. Other Warranties

EXCEPT AS STATED OTHERWISE IN THIS CP, SECTIGO EXPRESSLY DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES IN THE CERTIFICATES AND RELATED SERVICES. THIS DISCLAIMER IS EFFECTIVE TO THE MAXIMUM EXTENT ALLOWED BY LAW AND INCLUDES ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

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 CP.

- The accuracy, authenticity, completeness or fitness of any information contained in Sectigo Personal Certificates class 1, free, trial or demo Certificates.
- 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 CP.
- 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 or during a force majeure event.
- 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 CP. 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:

- An organizational unit attribute.
- 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 CP.

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, consequential, or special 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 CP.
- 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 CP.
- 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 CP.
- 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 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, a Subscriber 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.

9.10. Term and termination

9.10.1. Term

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

9.10.2. Termination

This CP, 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 CP for Certificates issued under this CP:

- All unpaid fees incurred under section 9.1 of this CP;

- All responsibilities and obligations related to confidential information, including those stated in section 9.3 of this CP;
- All responsibilities and obligations to protect private information, including those stated in section 9.4.4 of this CP;
- All representations and warranties, including those stated in section 9.6 of this CP;
- All warranties disclaimed in section 9.7 of this CP for Certificates issued during the term of this CP;
- All limitations of liability provided for in section 9.8 of this CP; and
- All indemnities provided for in section 9.9 of this CP.

Termination of this CP SHALL NOT affect any Subscriber Agreements executed during the term of this CP. Upon termination of this CP, all PKI participants are bound by the terms of this CP for Certificates issued during the term of this CP 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 CP 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
3rd Floor, 26 Exchange Quay, Trafford Road,
Salford, Greater Manchester, M5 3EQ, United Kingdom
Attention: Legal Practices
Email: legalnotices@sectigo.com

9.12. Amendments

Upon the Sectigo Certificate Policy Authority accepting such changes it deems to have significant impact on the users of this CP, Sectigo will, with seven (7) days' notice given of upcoming changes, communicate the updated version of this CP to applicable users via registered mail, email, publishing in the Sectigo repository, or otherwise. An updated version of

this CP will be denoted by a suitable incremental version numbering used to identify new version.

Revisions not denoted "significant" are those deemed by the Sectigo Certificate 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 of the CP and without changing the version number of this CP.

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

9.12.1. Procedure for amendment

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

9.12.2. Notification mechanism and period

Sectigo provides notice of an amendment to the CP 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 CP, 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 Certificate Policy Authority has the sole authority to determine whether an amendment to the CP 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, Interpretation, and Jurisdiction

9.14.1. Governing Law

This CP is governed by, and construed in accordance with, English law. This choice of law is made to ensure uniform interpretation of this CP, regardless of the place of residence or place of use of Sectigo Certificates or other products and services. English law applies in all Sectigo commercial or contractual relationships in which this CP 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 CP 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 CP, 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 CP are intended for convenience and reference only and SHALL NOT be used in interpreting, construing, or enforcing any of the provisions of this CP.

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

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 CP or the provision of Sectigo PKI services.

9.15. Compliance with applicable law

This CP 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. In delivering its PKI services Sectigo complies in all material respects with high-level international standards and all other relevant legislation and regulation.

9.16. Miscellaneous provisions

9.16.1. Entire agreement

This CP 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 CP 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 CP 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 this CP articles 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 provision of this CP or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CP (and the application of the invalid or unenforceable provision to other persons or circumstances) SHALL be interpreted in such manner as to affect the original intention of the parties.

Each and every provision of this CP that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

This CP SHALL be enforced as a whole, whilst failure by any person to enforce any provision of this CP 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 Sectigo, 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 the Sectigo CP, 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 CP conflicts with other rules, guidelines, or contracts, this CP 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 CP.
- Expressly superseding this CP 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 CP, 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 CP 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 CP, 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 Sectigo CP and associated policies published in the Sectigo Repository at https://www.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 CP.
- 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 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: ChangeLog

Version	Change Description	Date
1.0	Create new CP	29-May-2019
1.1	• Add ChangeLog • Fix various minor errors throughout document • Updated 5.2.4 regarding separation of roles • Slight modification to HSM requirements • Change physical requirement from 5 tier to 4 tier in Section 5.1 and clarified application to HSM mode. • Certificate Policy Authority has been renamed to Policy Authority • Section titles changed: 6.2.2 and 9.2.3 • Added section 4.2.4 for CAA • Updates in sections 1.6.1 and 1.6.2 • Change log retention to 2 years in section 5.4.3	25-February-2022
1.2	• Minor update in section 2.2 • Update section 3.2.2 to point to section 3.1 • Clarification on section 4.8 about revocation	24-February-2023