Sectigo WebPKI Certificate Policy

Sectigo Limited
Version 1.4.0
Effective: 11 March, 2025
Unit 7, Campus Road, Listerhills Science Park, Bradford, BD7 1HR, United Kingdom
Tel: +44 (0) 161 874 7070
www.sectigo.com

Copyright Notice

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

SECTIGO

Contents

1. INTRODUCTION

1.1. Overview

This document defines the Sectigo Web PKI Certificate Policy which governs issuance of digital certificates intended to be trusted on the public internet.

This Certificate Policy conforms to the current version of the TLS Baseline Requirements (BR) and EV Guidelines (EVG), the Code Signing BR and the S/MIME BR of the CA/Browser Forum. In the event of any inconsistency between this CP and the other documents specified in this paragraph, those documents take precedence over this CP.

1.2. Document name and identification

This document is the *Sectigo Web PKI Certificate Policy (CP)*. It outlines the legal, commercial and technical principles and practices to provide certification services for Web PKI 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 (PKI). This CP is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the Sectigo Web PKI.

The Sectigo Web PKI CP is a public statement of the conditions of issuance, revocation and renewal of a Certificate.

This CP is structured in accordance with and includes all material required by the Internet Engineering Task Force (IETF) standard RFC 3647.

1.3. PKI participants

This section identifies and describes some of the entities that participate within the Sectigo Web PKI.

1.3.1. Certification Authorities

Entities that provide Certificate services within the Sectigo Web PKI.

1.3.1.1. Policy Authority

This entity 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 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 accordingly.

1.3.2. Registration authorities

The registration authorities (RAs) collect and verify each Subscriber's identity and information that is to be entered into the Subscriber's Public Key Certificate. The RA performs its function in accordance with a CPS approved by the Policy Authority. The RA is responsible for:

- The registration process
- The identification and authentication process.

RAs do not issue or cause the issuance of Certificates. Some RAs may be enabled to perform validation of some or all of the subject identity information but for example, are not able to undertake domain control validation.

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

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

1.3.3. Subscribers

Subscribers are individuals or companies that use PKI.

1.3.4. Relying parties

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

1.3.5. 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.

1.4. Certificate usage

1.4.1. Appropriate Certificate uses

The different Certificate types have differing intended usages and differing policies.

Specific Certificate usage will be defined in the CPS.

1.4.2. Prohibited Certificate uses

Certificates are prohibited from being used to the extent that the use is inconsistent with applicable law. Certificates are prohibited from being used as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe damage to persons or property.

1.5. Policy administration

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

1.5.1. Organization administering the document

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

1.5.2. Contact person

The Policy Authority MAY be contacted at the following address:

Policy Authority
Unit 7, Campus Road, Listerhills Science Park, Bradford, BD7 1HR, United Kingdom
Tel: +44 (0) 161 874 7070
Attention: Legal Practices
URL: http://www.sectigo.com
Email: legalnotices@sectigo.com

1.5.3. Person determining CP suitability for the policy

The Policy Authority is responsible for determining the suitability of Certificate policies illustrated within this CP. The 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

The Policy Authority SHALL approve this CP and any subsequent changes, amendments, or addenda.

1.6. Definitions and acronyms

1.6.1. Definitions

As defined in the correspondent CPS.

1.6.2. Acronyms

As defined in the correspondent CPS.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

Sectigo publishes this CP and associated documents in the Repository. The Policy Authority maintains the Repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in section 5.4 of this CP.

2.1. Repositories

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

Sectigo Ltd.
Attention: Legal Practices,
Unit 7, Campus Road, Listerhills Science Park, Bradford, BD7 1HR, United Kingdom
Tel: + 44(0) 161 874 7070

2.3. Time or frequency of publication

Updated or modified versions of the Sectigo Web PKI CP are published at least once per year and in accordance with section 9.12 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 and physical access 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

3.1. Naming

3.1.1. Types of names

The constituent elements of the subject DN conform with ITU X.500.

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 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

No stipulation.

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

Assigned serial numbers are unique.

3.2. Initial identity validation

3.2.1. Method to prove possession of Private Key

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

In the case where key generation is performed under the CA or RA's direct control, proof of possession is not required.

The CA MAY approve other methods to prove possession of the Private Key by an Applicant. If other methods are approved, they SHALL be stipulated in the CPS.

3.2.2. Authentication of Organization Identity

Verification practices are detailed in the CPS.

3.2.3. Authentication of Individual Identity

If the Applicant is a natural person, the CA SHALL verify the Applicant's name, Applicant's address, and the authenticity of the certificate request.

3.2.4. Non-verified Subscriber Information

Information that is not verified is not included in certificates.

3.2.5. Validation of authority

Before issuing certificates that assert organizational authority, the CA SHALL validate the subscriber's authority to act in the name of the organization.

3.2.6. Criteria for interoperation

The Policy Authority SHALL determine criteria for interoperation with this PKI.

3.3. Identification and authentication for re-key requests

Rekeys are supported on Replacement and Renewal.

3.3.1. 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 through the use of the device's current valid signature key.

3.3.2. Identification and authentication for re-key after revocation

In the event of Certificate revocation, issuance of a new Certificate generally requires that the party go through the initial registration process per CP Section 3.2.

3.4. Identification and authentication for revocation request

Requests to revoke a Certificate have different options, for example, MAY be authenticated using that Certificate's Public Key, regardless of whether the associated Private Key has been compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The validity period of a Certificate varies depending on the Certificate type, but typically, a Certificate will be valid for either 1 year, 2 years, or 3 years.

4.1. Certificate Application

The Certificate application process MUST provide sufficient information to:

- Establish the applicant's authorization (by the employing or sponsoring organization) to obtain a Certificate. (per Section 3.2.3)
- Establish and record identity of the applicant. (per Section 3.2.3)
- Obtain the applicant's Public Key and verify the applicant's possession of the Private Key for each Certificate required. (per Section 3.2.1)
- Verify any role, authorization, or other subject information requested for inclusion in the Certificate.

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

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 authorized representative of the applicant CA shall submit an application for a CA Certificate.

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

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 as specified in Sections 3.2 and 3.3. 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 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 (e.g., internal name), or when the CA has cause to lack confidence in the application or certification process.

4.2.3. Time to process Certificate applications

The time frame is greatly dependent on the type of Certificate and the verification requirements as stated in the CPS.

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 3.2.
- 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.

Certificate issuance by the Root CA SHALL require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation. 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.

4.3.3. Refusal to Issue a Certificate

No stipulation.

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:

- Using the Certificate
- Failure to object to the Certificate or its content within 30 days of issuance

4.4.2. Publication of the Certificate by the CA

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

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 operating under this policy SHOULD issue CRLs 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.

4.6. Certificate renewal

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 or RA 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 3.2.

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.

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

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 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

Those who may request a Certificate rekey include, but are not limited to, the Subscriber, the RA on behalf of the Subscriber, or the CA at its discretion.

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 3.2 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

4.8.1. Circumstance for Certificate modification

No stipulation.

4.8.2. Who MAY request Certificate modification

No stipulation.

4.8.3. Processing Certificate modification requests

No stipulation.

4.8.4. Notification of new Certificate issuance to Subscriber

No stipulation.

4.8.5. Conduct constituting acceptance of modified Certificate

No stipulation.

4.8.6. Publication of the modified Certificate by the CA

No stipulation.

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

No stipulation.

4.9. Certificate revocation and suspension

CAs operating under this policy MAY issue CRLs and MUST provide OCSP responses covering all unexpired Certificates issued under this policy except for OCSP responder.

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

See section 4.9.1 of the correspondent CPS for more information.

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

4.9.3. Procedure for revocation request

The CA SHALL accept and respond to revocation requests and problem reports on a 24/7 basis.

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

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

4.9.4. Revocation request grace period

There is no Grace Period under this policy, but a Grace Period MAY be specified in the CPS or in the Subscriber Agreement. 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

Once a certificate has been revoked the revocation will be reflected in the OCSP responses issued within 1 hour, and in the CRLs within 24 hours.

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. If it is temporarily infeasible to obtain revocation information, then 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.

4.9.7. CRL issuance frequency (if applicable)

See CPS for additional information.

4.9.8. Maximum latency for CRLs (if applicable)

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

OCSP responses MUST conform to RFC6960 and/or RFC5019. OCSP responses MUST either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10. On-line revocation checking requirements

See CPS for additional information.

4.9.11. Other forms of revocation advertisements available

CAs operating under this policy MAY rely on stapling, in accordance with RFC4366, to distribute its OCSP responses. In this case, the CA SHALL ensure that the Subscriber "staples" the OCSP response for the Certificate. The CA SHALL enforce this requirement on the Subscriber either contractually, through the Subscriber Agreement or Terms of Use, or by technical review measures.

4.9.12. Special requirements related to key compromise

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

4.9.13. Circumstances for suspension

Certificate suspension is not supported by this CP. The Repository SHALL NOT include entries that indicate that a Certificate is suspended.

4.9.14. Who can request suspension

Not applicable.

4.9.15. Procedure for suspension request

Not applicable.

4.9.16. Limits on suspension period

Not applicable.

4.10. Certificate status services

4.10.1. Operational characteristics

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

4.10.2. Service availability

Certificate status services are available 24/7.

4.10.3. Optional features

No stipulation.

4.11. End of subscription

No stipulation. It SHALL be specified in the correspondent CPS and/or Subscriber Agreement.

4.12. Key escrow and recovery

4.12.1. Key escrow and recovery policy and practices

No stipulation. It MAY be specified in the correspondent 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 of the physical control requirements specified below apply equally to the Root and Sub-CAs, and any remote workstations used to administer the CAs, except where specifically noted.

5.1.1. Site location and construction

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 controlled.

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 in NIST Special Publication 800-88.

5.1.8. Off-site backup

The CA SHALL back 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 back up location.

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 on the “principle of least privilege” basis through a formal authorization process with authorizations being archived.

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

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

The CA SHALL require 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 a CA 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.

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 MAY NOT assume more than one role, except Operator.

No individual in a Trusted Role SHALL be assigned more than one identity.

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

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 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 IT systems & policies and that they have reached a suitable skill level satisfactory to the Server Systems Manager/Administrator or CEO. New administrators are closely monitored by the Server Systems Manager/Administrator for the first three months. Where systems allow, administrator access authentication is via a public/Private Key specifically issued for this purpose. This provides accountability of individual administrators and permits their activities to be monitored.

5.3.2. Background check procedures

All trusted personnel have background checks before access is granted to Certificate Systems.

5.3.3. Training requirements

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.

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 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.

5.3.7. Independent contractor requirements

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.

5.3.8. Documentation supplied to personnel

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

5.4. Audit logging procedures

5.4.1. Types of events recorded

See CPS for additional information.

5.4.2. Frequency of processing log

No stipulation.

5.4.3. Retention period for audit log

Audit logs SHALL be retained for at least two (2) years. 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)

No stipulation.

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. There´s a specific treatment for critical vulnerabilities.

5.5. Records archival

5.5.1. Types of records archived

See CPS for additional 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.

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.

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.

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,
- Subscriber Agreements,
- Certificate issuance, and
- Certificate revocation.

5.5.6. Archive collection system (internal or external)

No stipulation.

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

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.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

See CPS for additional information.

5.7.2. Computing resources, software, and/or data are corrupted

No stipulation.

5.7.3. Entity Private Key compromise procedures

Due to the nature of the CA Private Keys, these are classified as highly critical to business operations and continuity.

5.7.4. Business continuity capabilities after a disaster

See CPS for additional information.

5.8. CA or RA termination

See CPS for additional information.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

6.1.1. Key pair generation

Subscriber key pair generation is described in the CPS.

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 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

The Subscriber or the CA SHALL perform subscriber key pair generation. 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 the 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.

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

CA keys SHALL be generated within a FIPS 140-2 Level 3 certified HSM.

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

The use of a specific key is constrained by the keyUsage extension in the X.509 Certificate.

Public keys that are bound into CA Certificates SHALL be used for signing Certificates and status information (e.g., CRLs). The following table shows the specific keyUsage extension settings for CA Certificates and specifies that all CA Certificates (i.e., Root CAs, Sub-CAs):

- Shall include a keyUsage extension
- Shall set the criticality of the keyUsage extension to TRUE
- Shall assert the digitalSignature bit, keyCertSign bit and the cRLSign bit in the key usage extension

Table: keyUsage Extension for all CA Certificates

Field	Format	Criticality	Value	Comment
keyUsage	BIT STRING	TRUE	{ id-ce 15 }	Included in all CA Certificates
digitalSignature	(0)		0	Set
nonRepudiation	(1)		0	Not Set
keyEncipherment	(2)		0	Not Set

dataEnciphermen t	(3)		0	Not Set
keyAgreement	(4)		0	Not Set
keyCertSign	(5)		1	Set
cRLSign	(6)		1	Set
encipherOnly	(7)		0	Not Set
decipherOnly	(8)		0	Not Set

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 FIPS 140-2.

- Root CAs SHALL perform all CA cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-2 level 3 or higher.
- 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.

6.2.3. Private key escrow

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.

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

No stipulation.

6.2.6. Private key transfer into or from a cryptographic module

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

6.2.7. Private key storage on cryptographic module

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

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 CA Administrator's workstation to prevent use of the workstation and its associated Private Key without the CA Administrator's authorization.

6.2.8.2. Offline CAs Private Key

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

6.2.8.3. Online CAs Private Keys

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

6.2.9. Method of deactivating Private Key

Cryptographic modules that have been activated SHALL NOT be available to unauthorized access. After use, the cryptographic module SHALL be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity. CA cryptographic modules SHALL be stored securely when not in use.

When an online CA is taken offline, 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 Generation Ceremony, in which such Private Keys are used for Private Key operations, the CA SHALL remove the token containing the Private Keys from the reader in order to deactivate them. Once removed from the reader, tokens SHALL be securely stored.

When deactivated, Private Keys SHALL be kept in encrypted form only. They SHALL be cleared from memory before the memory is de-allocated. Any disk space where Private Keys were stored SHALL be overwritten before the space is released to the operating system.

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

The Certificate validity period MAY be set as follows:

- 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 3 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 at least.

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

See CPS for additional information.

6.5.2. Computer security rating

No stipulation.

6.6. Life cycle technical controls

6.6.1. System development controls

See CPS for additional information.

6.6.2. Security management controls

No stipulation.

6.6.3. Life cycle security controls

No stipulation.

6.7. Network security controls

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.

6.8. Time-stamping

All CA components SHALL regularly synchronize with a time service such as National Institute of Standards and Technology (NIST) Atomic Clock or NIST Network Time Protocol Service. Time derived from the time service SHALL be used for establishing the time of:

- Initial validity type of a Device's Certificate;
- Revocation of a Device's Certificate;
- Posting of CRL updates; and
- OCSP or other responses.

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

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 CPS.

7.1.1. Version number(s)

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

They SHALL conform to the different BRs and MAY be described in the CPS.

7.1.3. Algorithm object identifiers

Certificates are signed using algorithms including but not limited to RSA and ECDSA. Additional detail MAY be found in the CPS.

7.1.4. Name forms

As specified in Section 3.1.1.

7.1.5. Name constraints

No stipulation. It MAY be specified in the correspondent CPS.

7.1.6. Certificate policy object identifier

As specified in the correspondent 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.

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

The profile of the CRL is 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)

These are 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

OCSP responders are capable of providing a 'good' or 'revoked' status for all Certificates issued under the terms of this CP. The OCSP responders will give an 'unknown' response for expired Certificates.

7.3.1. Version number(s)

OCSP responders conform 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.

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

A Qualified Auditor performs this audit. 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;
- 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;
- (For audits conducted in accordance with the WebTrust standard) 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 and does not have a financial interest, business relationship, or course of dealing that would create a conflict of interest.

8.4. Topics covered by assessment

Topics covered by the annual audit 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 the CA of the findings. Depending on the nature and extent of the deficiency, the CA would develop a plan to correct the deficiency, which could involve changing its policies or practices, or both.

8.6. Communication of results

The audit requires the CA making the Audit Report available to the public no later than 3 months after of the audit period.

8.7. Self Audits

No stipulation.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

No stipulation.

9.1.1. Certificate issuance or renewal fees

No stipulation.

9.1.2. Certificate access fees

No stipulation.

9.1.3. Revocation or status information access fees

No stipulation.

9.1.4. Fees for other services

No stipulation.

9.1.5. Refund policy

No stipulation. It MAY be specified in the CPS.

9.2. Financial responsibility

9.2.1. Insurance coverage

The CA SHALL maintain professional Errors and Omissions Insurance.

9.2.2. Other assets

No stipulation.

9.2.3. Insurance or warranty coverage for end-entities

No stipulation. It MAY be specified in the CPS.

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

No stipulation.

9.3.2. Information not within the scope of confidential information

No stipulation.

9.3.3. Responsibility to protect confidential information

No stipulation.

9.4. Privacy of personal information

9.4.1. Privacy plan

The CA SHALL implement 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

No stipulation.

9.4.5. Notice and consent to use private information

The CA SHALL provide notices to Applicants and Subscribers about use of private information through its Privacy Policy.

9.4.6. Disclosure pursuant to judicial or administrative process

The CA disclosure of information pursuant to judicial or administrative process is stated in the Privacy Policy.

9.4.7. Other information disclosure circumstances

No stipulation.

9.5. Intellectual property rights

No stipulation.

9.6. Representations and warranties

9.6.1. CA representations and warranties

The CA SHALL make certain representations regarding Certificate services performed pursuant to this CP.

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, the CA 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, act promptly to issue a Certificate in accordance with this CP.
- Upon receipt of a request for revocation from an RA, act promptly to revoke a 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.

9.6.2. RA representations and warranties

The RA is bound under contract to:

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

9.6.3. Subscriber representations and warranties

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

- provide accurate and complete information at all times in the Certificate request and as otherwise requested in connection with the issuance of Certificates;
- 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 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 if Subscriber becomes aware of any misuse of the Certificates;

- 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; and
- 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.
- 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.

9.6.4. Relying party representations and warranties

A party relying accepts and acknowledges that in order to reasonably rely on a 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.
- 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

No stipulation.

9.7.2. Other Warranties

No stipulation.

9.8. Limitations of liability

Subscribers MUST agree to the Terms & Conditions, or a Subscriber Agreement, before signing-up for a Certificate.

9.8.1. Damage and Loss Limitations

No stipulation.

9.8.2. Exclusion of Certain Elements of Damages

No stipulation.

9.9. Indemnities

No stipulation.

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 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:

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 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.

9.12.1. Procedure for amendment

An amendment to this CP is made by the Policy Authority. The 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

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.

9.12.3. Circumstances under which OID MUST be changed

The 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

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 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.

9.14.3. Jurisdiction

Each party, 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.

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.

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.

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

No stipulation.

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 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

Private and Public Keys are property of the Subscribers who rightfully issue and hold them.

9.17.4. 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
- Ensure that the Public Key corresponds with the Private Key used.
- Ensure that the Public Key is the correct one.
- Provide correct and accurate information
- Read, understand and agree with all terms and conditions in this CP and associated policies published in the Repository
- Use Certificates for legal and authorized purposes in accordance with the suggested usages and practices in this CP.
- Cease using a Certificate if any information in it becomes misleading obsolete or invalid.
- Cease using a Certificate if such Certificate is expired and remove it from any applications and/or devices it has been installed on.
- 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 Certificate.
- Request the revocation of a Certificate in case of an occurrence that materially affects the integrity of a 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 Slight modification to HSM requirements in 6.1.1 and 6.1.6 Change physical requirement from 5 tier to 4 tier in Section 5.1 and clarified application to HSM mode. Fixed an error in 6.2.10 Certificate Policy Authority has been renamed to Policy Authority	22-May-2020
1.2	Some clarifications and typos throughout the document Update of sections 1.6.1 and 1.6.2 pointing to the CPS Specify the 398 days for reuse of domain or IP validation Update the CRL and OCSP frequency issuance Update the publication of the audit report timeframe Update the audit logging storage	6-July-2021
1.3	Update some incorrect links in sections 3.4, 6.2.5 and 9.8.1 Removed section 9.17.3 entirely Updated some section titles: 3.2.2, 4.9.12, 6.2.2 and 9.2.3 Clarifying in section 4.9.7 the CRL issuance frequency	15-November-2021
1.3.1	Updated sections 2.1 and 2.4 with minor changes Update section 3.4 pointing to the updated CPS Clarification on section 4.8 regarding the revocation of the replaced certificate Updated section 4.9.1 regarding weak keys Updated section 4.9.7 adding the 10 days for subscriber certs Updated section 4.9.10 for OCSP Updated section 5.3.3 with the training records Updated section 5.4.1 and 5.5.2 More detail in section 6.2.6 Updated section 6.5.1 with the MFA Updated section 9.9.1 adding Sectigo and third parties	5-April-2022
1.3.2	Updated section 4.9.1 pointing to the CPS revocation information Updated section 9.6.2	11-November-2022
1.3.3	Updated links Removed fax Updated section 5.3.2 adding certificate systems	23-March-2023
1.3.4	Update titles of sections 9.2.3 and 9.14	7-February-2024
1.3.5	Adding SMIME BRs into section 1.1 for clarification Removal of section 4.2.4 related to CAA records Changed the PA contact address	4-December-2024
1.4.0	Create an agnostic CP for external PKIs	11-March-2025