Sectigo Certification Practice Statement

Sectigo Limited
Version 5.1.2
Effective: May 6, 2019
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

Copyright Notice

Contents

1. INTRODUCTION

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

1.1. Overview

For issuance of Server Certificates Sectigo conforms to the current version of the Baseline Requirements (BR) and EV Guidelines (EVG). For the issuance of Code Signing Certificates Sectigo conforms to the EVG for Code Signing and the Code Signing BR. In the event of any inconsistency between this CPS and the other documents specified in this paragraph, those documents take precedence over this CPS.

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

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

Document Status Location	Status	Location
Sectigo Certification Practice Statement	Public	Sectigo Repository
Sectigo Relying Party Agreement	Public	Sectigo Repository
Certificate Subscriber Agreement	Public	Sectigo Repository
Code Signing Certificate Subscriber Agreement	Public	Sectigo Repository
Enterprise Public Key Infrastructure Manager Agreement	Confidential	Presented to partners accordingly
Enterprise Public Key Infrastructure Manager Guide	Confidential	Presented to partners accordingly
Powered SSL Partner Agreement	Confidential	Presented to partners accordingly
Powered SSL Partner Guide	Confidential	Presented to partners accordingly
Reseller Agreement	Confidential	Presented to partners accordingly
Reseller Agreement	Confidential	Presented to partners accordingly

This CPS, related agreements and Certificate policies referenced within this document are available online at www.sectigo.com/legal.

1.2. Document Name and Identification

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

The Sectigo CPS 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 PKI. Sectigo conforms to this CPS and other obligations it undertakes through adjacent contracts when it provides its services.

1.3.1. Certification Authorities

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

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

1.3.2. Registration Authorities

Sectigo has established the necessary secure infrastructure to fully manage the lifecycle of digital Certificates within its PKI. Through a network of RAs, Sectigo also makes its certification authority services available to its Subscribers. Sectigo RAs:

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

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

Sectigo MAY extend the use of RAs for its Web Host Reseller, Enterprise Public Key Infrastructure (EPKI) Manager and, optionally, Powered SSL programs. Upon successful approval to join the respective programs the Web Host Reseller Subscriber, EPKI Manager Subscriber or Powered SSL Subscriber MAY be permitted to act as an RA on behalf of Sectigo. RAs are required to conform to this CPS, the BR and/or the EVG. Certificates issued through an RA contain an amended Certificate Profile within an issued Certificate to represent the involvement of the RA in the issuance process to the Relying Party.

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

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

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

1.3.2.1. Internal Registration Authority

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

For the issuance of Secure Server Certificates this RA is also equipped with automated systems that validate domain control. For that minority of Secure Server Certificates for which the validation of domain control is not possible by completely automated means, the specially trained and vetted staff that Sectigo employs in its RA have the ability to cause the issuance of Certificates – but only when they are authenticated to Sectigo's issuance systems using two-factor authentication.

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

1.3.2.2. External Registration Authority

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

External RAs do not validate domain control for Secure Server Certificates. This element of the validation of Secure Server Certificates is always performed by Sectigo's internal RA as described in this CPS.

1.3.3. Subscribers (End Entities)

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

1.3.4. Relying Parties

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

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

location is detailed within the Certificate. OCSP responses are sent through the OCSP responder.

1.3.5. Other Participants

Sectigo has several categories of partner which assist in the provision of certification services.

1.3.5.1. Reseller Partners

Sectigo operates a Reseller Partner network that allows authorized partners to integrate Sectigo digital Certificates into their own product portfolios. Reseller Partners are responsible for referring digital Certificate customers to Sectigo, who maintain full control over the Certificate lifecycle process, including application, issuance, renewal and revocation. Due to the nature of the reseller program, the Reseller Partner must authorize a pending customer order made through its Reseller Partner account prior to Sectigo instigating the validation of such Certificate orders. All Reseller Partners are required to provide proof of organizational status (refer to section 3.2.2 of this CPS for examples of documentation required) and must enter into a Sectigo Reseller Partner agreement prior to being provided with Reseller Partner facilities.

1.3.5.2. Web Host Resellers

The Web Host Reseller program allows organizations providing hosting facilities to manage the Certificate lifecycle on behalf of their hosted customers. Such Web Host Resellers are permitted to apply for Secure Server Certificates on behalf of their hosted customers.

All Web Host Resellers are required to provide proof of organizational status (refer to section 3.2.2 of this CPS for examples of documentation required) and must enter into a Sectigo Web Host Reseller agreement prior to being provided with Web Host Reseller facilities.

Some Web Host Resellers MAY be designated as external RAs.

1.3.5.3. EPKI Manager Accounts

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

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

EPKI account holders do not perform the initial validation of domain control for Secure Server Certificates. This element of the validation of Secure Server Certificates is always performed by Sectigo's internal RA as described in this CPS.

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

1.3.5.4. Powered SSL Partners

Sectigo operates the Powered SSL service that includes an international network of approved organizations sharing the Sectigo practices and policies and using a suitable brand name to issue privately labeled Secure Server Certificates to individuals and companies. Sectigo controls all aspects of the Certificate lifecycle, including but not limited to the validation, issuance, renewal and revocation of Powered Secure Server Certificates, however issued Certificates contain an amended Certificate profile to reflect the Powered SSL status to Relying Parties (ultimately customers).

All Powered SSL Partners are required to provide proof of organizational status (refer to section 3.2.2 of this CPS for examples of documentation required) and must enter into a Sectigo Powered SSL Partner agreement prior to being provided with Powered SSL Partner facilities.

Some Powered SSL Partners MAY be designated as external RAs.

1.4. Certificate Usage

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

Sectigo currently offers a portfolio of digital Certificates and related products that can be used to address the needs of users for secure personal and business communications, 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.

1.4.1. Appropriate Certificate Uses

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

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

1.4.1.1. Secure Server Certificates

Secure Server Certificates, also known as SSL or TLS certificates, facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a Web site. There are typically three levels of validation for Secure Server Certificates.

Domain Validated (DV) Certificates: The appropriate use of DV Certificates is to keep information encrypted when sent between a client and a server where there are low risks and consequences of data compromise and where the identity of the server operator is of little consequence. DV Certificates are appropriate for entities needing low cost Certificates issued at a fast pace. DVs do not provide authentication or validation, and are the lowest cost means of securing a website.

Organization Validated (OV) Certificates: OV Certificates are used to keep information encrypted that is sent between a client and a server where there are moderate risks and consequences of data compromise, and therefore the end user desires to have reasonable assurance of the identity of the server operator. OV Certificates include business and company validation. Additionally, OV Certificates provide higher levels of trust and security than DV certificates, but provide lower levels of trust and security than EV Certificates.

Extended Validated (EV) Certificates: Clearly identify the legal entity that controls a web site. EV certificates provide a greater level of assurance to the user of an Internet browser that the web site the user is accessing is controlled by a specific legal entity identified in the Certificate Subject by name, address of place of business, jurisdiction of incorporation or registration, and the entities registration number or other disambiguating information.

Multidomain Certificates (MDC) are Certificates that may contain multiple FQDNs or IP addresses in the subjectAlternativeName field.

Wildcard Certificates are Certificates that cover sub-domains of any single domain.

Wildcard Domain Names MUST NOT be issued in EV Certificates.

1.4.1.2. S/MIME Certificates

Secure/Multipurpose Internet Mail Extension(s) (S/MIME) Certificates are used for cryptographically signing and encrypting email. They are issued to a specific email address and MAY also contain Subject information verifying the identity of the individual/natural person and/or the organization which owns the email address.

1.4.1.3. Code Signing Certificates

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

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

1.4.2. Prohibited Certificate Uses

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

DV Certificates are not for use as a means of providing identity assurance.

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 CPS.

1.5.1. Organization Administering the Document

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

1.5.2. Contact Person

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

Sectigo Certificate Policy Authority
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
Attention: Legal Practices
URL: https://www.sectigo.com
Email: legalnotices@sectigo.com

To report abuse, fraudulent, or malicious use of Certificates issued by Sectigo, please send email to:

- For SSL/TLS Certificates: sslabuse@sectigo.com
- For Code Signing Certificates: signedmalwarealert@sectigo.com

1.5.3. Person Determining CPS Suitability for the Policy

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

1.5.4. CPS approval procedures

This CPS and any subsequent changes, amendments, or addenda, shall be approved by the Sectigo Certificate Policy Authority.

1.6. Definitions and Acronyms

The list of definitions and acronyms located in this section are for use within the Sectigo CPS.

1.6.1. Acronyms

Acronyms and abbreviations used throughout this CPS shall stand for the phrases or words set forth in Appendix A to this CPS.

1.6.2. Definitions

Capitalized terms used throughout this CPS shall have the meanings set forth in Appendix B to this CPS.

1.6.3. Conventions

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

Sectigo publishes this CPS, Certificate terms and conditions, the Relying Party Agreement and copies of all Subscriber Agreements in the Repository. The Sectigo Certificate 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 CPS.

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

2.1. Repositories

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

  Sectigo Ltd.
  Attention: Legal Practices,
  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

In addition to the repository, Sectigo hosts test web pages that allow Application Software Suppliers to test their software with Subscriber Certificates which chain up to Sectigo's publicly trusted Root Certificates.

Root Certificate	Valid	Expired	Revoked
AAA Certificate Services	https://aaacertificateservices.comodoca.com/	https://aaacertificateservices.comodoca.com:442/	https://aaacertificateservices.comodoca.com:444/
AddTrust External CA Root	https://addtrustexternalcaroot-ev.comodoca.com/	https://addtrustexternalcaroot-ev.comodoca.com:442/	https://addtrustexternalcaroot-ev.comodoca.com:444/
COMODO Certification Authority	https://comodocertificationauthority-ev.comodoca.com/	https://comodocertificationauthority-ev.comodoca.com:442/	https://comodocertificationauthority-ev.comodoca.com:444/
COMODO Certification Authority	https://comodocertificationauthority-ev.comodoca.com/	https://comodocertificationauthority-ev.comodoca.com:442/	https://comodocertificationauthority-ev.comodoca.com:444/

COMODO ECC Certification Authority	https://comodoecccertificationauthority-ev.comodoca.com/	https://comodoecccertificationauthority-ev.comodoca.com:442/	https://comodoecccertificationauthority-ev.comodoca.com:444/
COMODO RSA Certification Authority	https://comodorsacertificationauthority-ev.comodoca.com/	https://comodorsacertificationauthority-ev.comodoca.com:442/	https://comodorsacertificationauthority-ev.comodoca.com:444/
USERTrust ECC Certification Authority	https://usertrustecccertificationauthority-ev.comodoca.com/	https://usertrustecccertificationauthority-ev.comodoca.com:442/	https://usertrustecccertificationauthority-ev.comodoca.com:444/
USERTrust RSA Certification Authority	https://usertrustrsacertificationauthority-ev.comodoca.com/	https://usertrustrsacertificationauthority-ev.comodoca.com:442/	https://usertrustrsacertificationauthority-ev.comodoca.com:444/

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. The Sectigo CPS is reviewed and updated or modified versions are published at least once per year and in accordance with section 9.12 of this CPS. For CRL issuance frequency, see section 4.9.7 of this CPS.

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 CPS and the Sectigo insurance policy.

3. IDENTIFICATION AND AUTHENTICATION

Sectigo offers different Certificate types to make use of TLS and S/MIME technology for secure online transactions and secure email respectively. Prior to the issuance of a Certificate, Sectigo will validate an application in accordance with this CPS that may involve the request by Sectigo to the Applicant for relevant official documentation supporting the application.

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

3.1. Naming

3.1.1. Types of Names

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

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

Server authentication Certificates in general include entries in the subjectAlternateName (SAN) extension which are intended to be relied upon by relying parties.

3.1.2. Need for Names to be Meaningful

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

3.1.3. Anonymity or Pseudonymity of Subscribers

Sectigo does not issue pseudonymous Certificates for server authentication, code-signing, or email use, but does issue some Certificates solely for client authentication where the names in the subject of the Certificate are meaningful only within the scope of the application with which they are issued to be used and are not generally meaningful outside that scope.

3.1.4. Rules for Interpreting Various Name Forms

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

3.1.5. Uniqueness of Names

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

For secure server Certificates, domain name uniqueness is controlled by ICANN.

3.1.6. Recognition, Authentication, and Role of Trademarks

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

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

3.2. Initial Identity Validation

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

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

3.2.1. Method to Prove Possession of Private Key

Verification of a digital signature is used to determine that:

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

The usual means by which Sectigo accepts signed data from an Applicant to prove possession of a Private Key is in the receipt of a PKCS#10 Certificate Signing Request (CSR).

3.2.2. Authentication of Organization and Domain Identity

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

The following elements are critical information elements for a Sectigo Certificate issued to an Organization. Those elements marked with PUBLIC are present within an issued Certificate and are therefore within the public domain. Those elements not marked with PUBLIC remain confidential in line with the privacy and protection of data provisions outlined in this CPS.

- Legal Name of the Organization (PUBLIC)
- Organizational unit (PUBLIC)
- Street, city, postal/zip code, country (PUBLIC)
- VAT-number (if applicable)
- Company / DUNS number (if available)
- Server Software Identification
- Payment Information

- Administrator contact full name, email address and telephone
- Billing contact persons and organizational representative
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organizational status of the Organization
- Subscriber Agreement, signed (if applying out of bands)

3.2.2.1. Domain and IP Address Verification

For each domain name to be included in the Secure Server Certificate Subject, Sectigo verifies the Applicant's control of the domain name in accordance with the Baseline Requirements, section 3.2.2.4, using one of the following methods for each FQDN;

1. Communicating directly with the Domain Name Registrant using a postal address, email address, or telephone number provided by the Domain Name Registrar;

   a. Email, Fax, SMS, or Postal Mail to Domain Contact
   (in accordance with section 3.2.2.4.2 of the Baseline Requirements)
   Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail to a recipient identified as a Domain Contact and then receiving a confirming response utilizing the Random Value.
   The Random Value is generated by Sectigo and remains valid for use in a confirming response for no more than 30 days from its generation;

2. Communicating directly with the Domain Contact confirming the Applicant's control over the requested FQDN using a constructed email address (as defined in section 3.2.2.4.4 of the Baseline Requirements) by:

   a. sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name,

   b. including a Random Value in the email, and

   c. having the Applicant submit (by clicking or otherwise) the Random Value to Sectigo's servers to confirm receipt and authorization.

   The Random Value is generated by Sectigo and remains valid for use in a confirming response for no more than 30 days from its generation;

3. Confirming the Applicant's control over the requested FQDN by having the Applicant make an agreed-upon change to the website (in accordance with section 3.2.2.4.6 of the Baseline Requirements).
   Confirming that the Request Token or Random Value appear in the content of a file or on a webpage in the form of a meta tag, the file or webpage being accessed via the URL HTTP[S]://<Authorization Domain>/.well-known/pki-validation/FileName over port

80 (HTTP) or 443 (HTTPS).
The Random Value is generated by Sectigo and remains valid for use for no more than 30 days from its generation;

4. Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token in a DNS CNAME record for an Authorization Domain Name or an Authorization Domain Name that is prefixed with a label that begins with an underscore character (as defined in section 3.2.2.4.7 of the Baseline Requirements).
The Random Value is generated by Sectigo and remains valid for no more than 30 days from its generation;

5. Confirming the Applicant's control over the requested FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN (as defined in section 3.2.2.4.8 of the Baseline Requirements).

6. Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 (Appendix A) (as defined in section 3.2.2.4.13 of the Baseline Requirements).

7. Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address identified as a DNS TXT record email contact for the Authorization Domain Name selected to validate the FQDN (as defined in Section 3.2.2.4.14 and Appendix B of the Baseline Requirements).

8. For each IP Address listed in a Certificate, Sectigo confirms that, as of the date the Certificate was issued, the Applicant has control over the IP Address by obtaining documentation of IP address assignment from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC.

3.2.2.2. Authentication of Organization Identity for OV TLS Secure Server, Object Signing, Adobe Document Signing, and Device Certificates

In addition to the verification of domain control using the procedures listed above in section 3.2.2.1, Sectigo verifies the identity and address of the Applicant in accordance with the *CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* (commonly referred to as the Baseline Requirements), using documentation that is provided by, or through communication with at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence or recognition;

2. A third party database that is periodically updated and considered a Reliable Data Source;

3. A site visit by the CA or a third party who is acting as an agent for the CA; or,

4. An attestation letter;

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

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

1. Communication directly with a government agency responsible for the management of such DBAs or trade names, or;

2. A utility bill, bank statement, credit card statement, government issued tax document, or other form of identification that Sectigo determines to be reliable.

3.2.2.3. Authentication of Organization Identity for EV TLS Secure Server and EV Code Signing Certificates

Before issuing an EV Certificate, Sectigo ensures that all Subject organization information to be included in the EV Secure Server, or Code Signing Certificate conforms to the requirements of, and is verified in accordance with the *CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates* (commonly referred to as the EV Guidelines) and/or the *Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates* as applicable.

Sectigo will verify:

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

3.2.3. Authentication of Individual Identity

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

The following elements are critical information elements for a Sectigo Certificate issued to an individual:

- Legal Name of the Individual (PUBLIC)
- Organizational unit (PUBLIC)
- Street, city, postal/zip code, country (PUBLIC)
- VAT-number (if applicable)
- Server Software Identification
- Payment Information
- Administrator contact full name, email address and telephone
- Billing contact persons and organizational representative
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organizational status of the Organization
- Subscriber Agreement, signed (if applying out of bands)

3.2.3.1. Domain and IP Address Verification

Same as section 3.2.2.1 for Organizational Applicants.

3.2.3.2. Individual Identity Verification for OV TLS Secure Server, Object Signing, Adobe Document Signing, and Device Certificates

In addition to the verification of domain control using the procedures listed above in section 3.2.2.1 of this CPS, if the Applicant is a natural person, Sectigo verifies the identity and address of the Applicant in accordance with the Baseline Requirements, using:

1. Verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government issued photo ID (passport, drivers license, military ID, national ID or equivalent document type)

2. Verify the Applicant's address using a form of identification that Sectigo determines to be reliable such as a government ID, utility bill, or bank or credit card statement. Sectigo MAY rely on the same government issued ID that was used to verify the Applicant's name.

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

notary, a notary public or equivalent. Such face to face verification SHALL be required prior to issuance of an Adobe Document Signing Certificate.

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

3.2.3.3. Individual Identity Verification for EV TLS Secure Server or EV Code Signing Certificate

Sectigo does not issue EV TLS Secure Server or EV Code Signing Certificates to Individual Applicants.

3.2.4. Non-Verified Subscriber Information

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

For server authentication Certificates, Sectigo verifies the subject elements as defined in section 9.2 of the Baseline Requirements.

3.2.5. Validation of Authority

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

3.2.5.1. S/MIME / Client Certificates

The request is verified via email sent to the email address to be contained in the Certificate Subject

3.2.5.2. Domain Registrant Authorization of TLS Server Certificates

Authorization by the Domain Name Registrant is verified as documented in section 3.2.2.1 of this CPS.

3.2.5.3. OV TLS Server, Code Signing, and Adobe Document Signing Certificates

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

Sectigo MAY use the sources listed in section 3.2.2.2 to verify the Reliable Method of Communication. Provided that a Reliable Method of Communication is used, Sectigo MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that Sectigo deems appropriate.

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

3.2.5.4. EV TLS Server and Code Signing Certificates

The request is verified in accordance with the *CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates* section 11.5.

3.2.6. Criteria for Interoperation

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

3.2.7. Application Validation

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

3.2.7.1. Personal Secure Email Certificate

The only identifying information in the subject DN is the email address of the Subscriber. Sectigo validates the right for the Applicant to use the submitted email address. This is achieved through the delivery via a challenge and response made to the email address submitted during the Certificate application.

Sectigo validates that the Applicant holds the Private Key corresponding with a Public Key to be included in the Certificate by utilizing an online enrollment process whereby Sectigo facilitates the Subscriber generating its key-pair using a specially crafted web page. The key pair is generated in the Subscriber's computer. The Private Key is not exported or transferred from the Subscriber's computer as part of the application process.

3.2.7.2. Corporate Secure Email Certificate

Corporate Secure Email Certificates are only available through the EPKI Manager and will only be issued to email addresses within approved domain names. The EPKI Manager Account Holder must first submit a domain name to Sectigo and appropriate domain name ownership, or right to use a domain name, validation takes place in accordance with section 3.2.7.1 of this CPS except that a domain authorization letter may be used in substitution of any domain ownership validation. Upon successful validation of a submitted

domain name or receipt of domain authorization letter, Sectigo allows the EPKI Manager Account Holder to utilize email addresses within the domain name.

The EPKI Manager nominated administrator applies for Corporate Secure Email Certificates. The administrator will submit the secure email Certificate end-entity information on behalf of the end-entity. An email is then delivered to the end-entity containing unique login details to online Certificate generation and collection facilities hosted by Sectigo. Once logged into the online Certificate generation and collection facilities, the end-entity's browser creates a public and private key pair. The Public Key is submitted to Sectigo who will issue a Corporate Secure Email Certificate containing the Public Key. Sectigo then validates using an automated cryptographic challenge that the Applicant holds the Private Key associated with the Public Key submitted during this automated application process. If the automated challenge is successful, Sectigo will release the digital Certificate to the end-entity Subscriber.

3.2.7.3. Custom Client Certificates

Custom client Certificates are a means for Certificates to be requested which have the structure and purpose of Personal Secure Email Certificates (3.2.7.1) and Corporate Secure Email Certificates (3.2.7.2), but with which the key usage or extended key usage fields may be varied to suit specific applications.

Custom Client Certificates are a deprecated product which are being phased out in favor of the Sectigo Personal Authentication Certificate (3.2.7.5).

3.2.7.4. Personal Authentication Certificates

Personal Authentication Certificates are issued to Natural Persons.

Personal Authentication Certificates always contain an email address. Sectigo validates the right for the Applicant to use the submitted email address. This is achieved through the delivery of a challenge and response made to the email address submitted during the Certificate application.

When ordered for an Enterprise account through the EPKI Manager for email addresses within approved domain names, the EPKI Manager Account Holder may first submit a domain name to Sectigo and prove appropriate domain name ownership or control, or the right to use the domain name for which validation takes place in accordance with section 3.2.2.1 of this CPS except that a domain authorization letter may be used in substitution of any domain ownership validation. Upon successful validation of a submitted domain name or receipt of domain authorization letter, Sectigo allows the EPKI Manager Account Holder to utilize email addresses within the domain name.

Sectigo validates that the Applicant holds the Private Key corresponding with a Public Key to be included in the Certificate by utilizing an online enrollment process whereby Sectigo facilitates the Subscriber generating its key-pair using a specially crafted web page. The key pair is generated in the Subscriber's computer. The Private Key is not exported or transferred from the Subscriber's computer as part of the application process.

Alternatively, the subscriber may demonstrate to Sectigo ownership of the Private Key associated with the Public Key to be included in the Certificate through the submission of a valid PKCS#10 Certificate Signing Request (CSR) or SPKAC request.

Where other subject details are present they are validated in the same manner as would be the case for a Natural Person Applicant for an OV TLS Server, Object Signing or Device Certificate as documented in section 3.2.3.2.

3.3. Identification and Authentication for Re-Key Requests

Sectigo supports rekeys on:

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

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

3.3.1. Identification and Authentication for Routine Re-Key

As stated above - in both cases, Sectigo requires the Subscriber to use the same authentication details (typically username and password) which they used in the original purchase of the Certificate.

3.3.2. Identification and Authentication for Re-Key after Revocation

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

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

3.4. Identification and Authentication for Revocation Request

Revocation at the Subscriber's request:

The Subscriber must either be in possession of the authentication details (typically username and password) which were used to purchase the Certificate originally OR the

Subscriber must be able to send an S/MIME email signed with the Private Key associated with the Certificate.

Revocation at the RA's request:

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

Revocation at the CA's request:
Sectigo does not revoke Certificates at the request of other CAs. Sectigo can and does revoke Subscriber Certificates for cause as set out in section 4.9 of this CPS, but identification and authentication is not required in these cases.

Sectigo employs the following procedure for authenticating a revocation request:

- The revocation request must be sent by the administrator contact associated with the Certificate application. Sectigo may, if necessary, also request that the revocation request be made by either / or the organizational contact and billing contact.
- Upon receipt of the revocation request Sectigo will request confirmation from the known administrator out of bands contact details, either by telephone or by fax.
- Sectigo validation personnel will then command the revocation of the Certificate and logging of the identity of validation personnel and reason for revocation will be maintained in accordance with the logging procedures covered in this CPS.

4. CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS

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

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

The following steps describe the milestones to issue a Secure Server Certificate:

1. The Applicant fills out the online request on Sectigo's web site and the Applicant submits the required information: Certificate Signing Request (CSR), e-mail address, common name, organizational information, country code, verification method and billing information.
2. The Applicant accepts the online Subscriber Agreement.
3. The Applicant submits the required information to Sectigo.
4. The Applicant pays the Certificate fees.

5. Sectigo verifies the submitted information using third party databases and Government records

6. Upon successful validation of the application information, Sectigo may issue the Certificate to the Applicant or should the application be rejected, Sectigo will alert the Applicant that the application has been unsuccessful.

7. Renewal is conducted as per the procedures outlined in this CPS and the official Sectigo websites.

8. Revocation is conducted as per the procedures outlined in this CPS.

4.1. Certificate Application

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

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

Sectigo may at its discretion, accept applications via email.

4.1.1. Who can Submit a Certificate Application

Generally, Applicants will complete the online forms made available by Sectigo or by approved RAs at the respective official websites. Under special circumstances, the Applicant may submit an application via email; however, this process is available at the discretion of Sectigo or its RAs.

EPKI Manager Account Holder applications are made through the EPKI Manager Management Console – a web-based console hosted and supported by Sectigo.

4.1.1.1. EPKI Manager Account Holder Certificate Applications

EPKI Manager Account Holders make the application for a secure server Certificate to be used by a named server, or a secure email Certificate to be used by a named employee, partner or extranet user under a domain name that Sectigo has validated either belongs to, or may legally be used by the EPKI Manager Account holding organization. Validation for adding domains to the EPKI Manager account may occur solely using a domain authorization letter.

4.1.1.2. Web Host Reseller Partner Certificate Applications

Web Host Reseller Partners may act as RAs under the practices and policies stated within this CPS. The RA may make the application on behalf of the Applicant pursuant to the Web Host Reseller program.

Under such circumstances, the RA is responsible for all the functions on behalf of the Applicant detailed in section 4.1.2 of this CPS. Such responsibilities are detailed and maintained within the Web Host Reseller agreement and guidelines.

4.1.2. Enrollment Process and Responsibilities

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

- Generate an RSA or ECC key pair and demonstrate to Sectigo ownership of the Private Key associated with the Public Key to be included in the Certificate through the submission of a valid PKCS#10 Certificate Signing Request (CSR) (or SPKAC request for certain client authentication or email Certificates).
- Make all reasonable efforts to protect the integrity and confidentiality of the Private Key.
- Submit to Sectigo a Certificate application, including application information as detailed in this CPS, a Public Key corresponding to the Private Key of which they are in possession, and agree to the terms of the relevant Subscriber Agreement.
- Provide proof of identity through the submission of official documentation as requested by Sectigo during the enrolment process.

4.2. Certificate Application Processing

Certificate applications are submitted to either Sectigo or a Sectigo approved RA. The following table details the entity(s) involved in the processing of Certificate applications. Sectigo issues all Certificates regardless of the processing entity.

Certificate Type	Enrolment Entity	Processing Entity	Issuing Authority
Secure Server Certificate - *all types as per section 2.4.1 of this CPS*	End Entity Subscriber	Sectigo	Sectigo
Secure Server Certificate - *all types as per section 2.4.1 of this CPS*	Web Host Reseller on behalf of End Entity Subscriber	Web Host Reseller	Sectigo
Personal Secure Email Certificate	End Entity Subscriber	Sectigo	Sectigo
Corporate Secure Email Certificate	End Entity Subscriber	EPKI Manager Account Holder	Sectigo
Code Signing Certificate	End Entity Subscriber	Sectigo	Sectigo
Sectigo Personal Authentication Certificate	End User Subscriber	Sectigo	Sectigo

4.2.1. Performing Identification and Authentication Functions

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

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

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

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

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

4.2.2. Approval or Rejection of Certificate Applications

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

If the validation of a Certificate application fails, Sectigo rejects the Certificate application. Sectigo reserves its right to reject applications to issue a Certificate to Applicants if, on its own assessment, by issuing a Certificate to such parties the good and trusted name of Sectigo might get tarnished, diminished or have its value reduced and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal.

Applicants whose applications have been rejected may subsequently reapply.

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

4.2.3. Time to Process Certificate Applications

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

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

4.2.4. Certificate Authority Authorization

Where an application is for a Certificate which includes a domain-name and is to be used for server authentication, Sectigo examines the Certification Authority Authorization (CAA) DNS Resource Records as specified in RFC 6844 as amended by Errata 5065 (Appendix A) and, if such CAA Records are present and do not grant Sectigo the authority to issue the Certificate, the application is rejected.

Where the 'issue' and 'issuewild' tags are present within a CAA record, Sectigo recognizes the following domain names within those tags as granting authorization for issuance by Sectigo.

- sectigo.com
- usertrust.com
- trust-provider.com

For a transitional period we also recognize the following domain names as granting authorization although these are deprecated and should be replaced with a domain name from the above list at the earliest opportunity.

- comodo.com
- comodoca.com

4.3. Certificate Issuance

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

Sectigo Certificates are issued to organizations or individuals.

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

4.3.1. CA Actions during Certificate Issuance

Sectigo's automated systems receive and collate:

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

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

Sectigo's 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

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

Secure Server Certificates

> Secure server Certificates are delivered via email to the Subscriber using the administrator contact email address provided during the application process.

Code Signing Certificates

> Notification of issuance of Code Signing Certificates are delivered via email to the Subscriber using the administrator contact email address provided during the application process. The certificate is then retrieved by the Subscriber via secure connection to Sectigo servers.

Secure Email Certificate: Personal Secure Email, Corporate Secure Email Certificates, Sectigo Personal Authentication Certificates

> Upon issuance of a Personal Secure Email Certificate, Corporate Secure Email Certificate, or Sectigo Personal Authentication Certificates the Subscriber is emailed a collection link using the email provided during the application. The Subscriber must visit the collection link using the same computer from which the original Certificate request was made. The Subscriber's cryptographic service provider software is initiated to ensure the Subscriber holds the Private Key corresponding to the Public Key submitted during application. Pending a successful challenge, the issued Certificate is installed automatically onto the Subscriber's computer.

Sectigo Dual Use Certificates

Sectigo Dual Use Certificates are downloaded by the Subscribers from the Sectigo Certificate Manager software.

4.3.3. Refusal to Issue a Certificate

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

4.4. Certificate Acceptance

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

4.4.1. Conduct Constituting Certificate Acceptance

An issued Certificate is either delivered via email or installed on a Subscriber's computer / hardware security module through an online collection method. A Subscriber is deemed to have accepted a Certificate when:

- the Subscriber uses the Certificate, or
- 30 days pass from the date of the issuance of a Certificate

4.4.2. Publication of the Certificate by the CA

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

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

Sectigo provides notification of Certificate issuance to the following entities by the following means:

Web Host Reseller Partner:

Issued Subscriber Secure Server Certificates applied for through a Web Host Reseller Partner on behalf of the Subscriber are emailed to the administrator contact of the Web Host Reseller Partner account. For Web Host Reseller Partners using the "auto-apply" interface, Web Host Resellers have the added option of collecting an issued Certificate from a Web Host Reseller account specific URL.

EPKI Manager Account Holder:

Issued Subscriber Secure Server Certificates applied for through an EPKI Manager Account are emailed to the administrator contact of the account.

4.5. Key Pair and Certificate Usage

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

4.5.1. Subscriber Private Key and Certificate Usage

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

4.5.2. Relying Party Public Key and Certificate Usage

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

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

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

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

4.6. Certificate Renewal

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

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

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

4.6.1. Circumstance for Certificate Renewal

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

4.6.2. Who May Request Renewal

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

4.6.3. Processing Certificate Renewal Requests

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

4.6.4. Notification of New Certificate Issuance to Subscriber

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

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

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

4.6.6. Publication of the Renewal Certificate by the CA

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

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

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

4.7. Certificate Rekey

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

4.7.1. Circumstances for Certificate Re-Key

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

4.7.2. Who May Request Certificate Rekey

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

4.7.3. Processing Certificate Rekey Requests

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

4.7.4. Notification of Rekey to Subscriber

Sectigo will notify Subscriber of a Certificate rekey by the means delineated in section 4.3.2 of this CPS.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

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

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

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

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

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

4.8. Certificate Modification

Sectigo does not offer Certificate modification. Instead, Sectigo will 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

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

Sectigo does not utilize Certificate suspension.

4.9.1. Circumstances for Revocation

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

- The Subscriber requests in writing that the CA revoke the Certificate;
- The Subscriber notifies Sectigo that the original Certificate request was not authorized and does not retroactively grant authorization;
- Sectigo reasonably believes there has been loss, theft, modification, unauthorized disclosure, or other compromise of the Private Key associated with the Certificate;
- Sectigo reasonably believes that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon;

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

- The Subscriber or Sectigo has breached a material obligation under this CPS or the relevant Subscriber Agreement;

- The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the Baseline Requirements;
- Sectigo is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- Sectigo is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- Either the Subscriber's or Sectigo's obligations under this CPS 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;
- Sectigo is made aware of a material change in the information contained in the Certificate, or the information contained in the Certificate is inaccurate;
- A personal identification number, Private Key or password has, or is likely to become known to someone not authorized to use it, or is being or is likely to be used in an unauthorized way
- The Certificate has not been issued in accordance with the policies set out in this CPS;
- The Subscriber has used the Certificate contrary to law, rule or regulation, or Sectigo reasonably believes that the Subscriber is using the Certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The Certificate was issued as a result of fraud or negligence;
- Sectigo is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key, or if there is clear evidence that the specific method used to generate the Private Key was flawed;
- Sectigo right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless Sectigo has made arrangements to continue maintaining the CRL/OCSP Repository; or
- The Certificate, if not revoked, will compromise the trust status of Sectigo.

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

- The Subordinate CA requests revocation in writing;
- The Subordinate CA notifies Sectigo that the original certificate request was not authorized and does not retroactively grant authorization;

- Sectigo obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the Baseline Requirements;
- Sectigo obtains evidence that the Subordinate CA Certificate was misused;
- Sectigo is made aware that the Subordinate CA Certificate was not issued in accordance with, or that Subordinate CA has not complied with, the Baseline Requirements or this CPS;
- Sectigo determines that any of the information appearing in the Subordinate CA Certificate is inaccurate or misleading;
- Sectigo or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- Sectigo's, or Subordinate CA's, right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless Sectigo has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by this CPS;
- The Subordinate CA has used the Certificate contrary to law, rule or regulation, or Sectigo reasonably believes that the Subordinate CA is using the Certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The Subordinate CA Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The Subordinate CA Certificate was issued as a result of fraud or negligence;
- The Subordinate CA Certificate, if not revoked, will compromise the trust status of Sectigo.

4.9.2. Who can Request Revocation

A Subscriber or another appropriately authorized party can request revocation of a Certificate. An authorized party includes an RA, regardless of whether on behalf of the Subscriber may request revocation through their account. Other parties may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, in the first instance, by email to sslabuse@sectigo.com.

4.9.3. Procedure for Revocation Request

Sectigo accepts and responds to revocation requests and problem reports on a 24/7 basis. Prior to the revocation of a Certificate, Sectigo will verify that the revocation request has been:

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

4.9.4. Revocation Request Grace Period

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

4.9.5. Time Within which Sectigo Will Process the Revocation Request

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

4.9.6. Revocation Checking Requirement for Relying Parties

Parties relying on a digital Certificate must verify a digital signature at all times by checking the validity of a digital Certificate against the relevant CRL published by Sectigo or using the Sectigo OCSP responder. Note that CRL MAY lag behind OCSP creating a situation where a revoked certificate MAY show as Revoked on OCSP yet MAY NOT show as revoked in the most recent CRL available. Therefore it is recommended to obtain revocation information from Sectigo's OCSP responder whenever possible. Relying parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the Subscriber.

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

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

4.9.7. CRL Issuance Frequency

Sectigo publishes CRLs to allow relying parties to verify a digital signature made using a Sectigo issued digital Certificate. Each CRL contains entries for all revoked un-expired Certificates issued and is valid for 24 hours. Sectigo issues a new CRL every 24 hours and includes a monotonically increasing sequence number for each CRL issued. Under special circumstances, Sectigo may publish new CRLs prior to the expiry of the current CRL. All expired CRLs are archived (as described in section 3.4 of this CPS) for a period of 7 years or longer if applicable. For Code Signing Certificates revoked due to key compromise or that have been issued to unauthorized persons, Sectigo will maintain Certificate information on CRLs for at least 20 years.

4.9.8. Maximum Latency for CRLs

The maximum latency for CRLs means the maximum time between the generation of CRLs and posting of the CRLs to the repository (i.e., the maximum amount of processing- and

communication-related delays in posting CRLs to the repository after the CRLs are generated). Sectigo does not employ a maximum latency for CRLs. Generally, however, CRLs are published within 1 hour.

4.9.9. On-Line Revocation/Status Checking Availability

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

4.9.10. On-Line Revocation Checking Requirements

Sectigo's OCSP responses are either:

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

All Sectigo's OCSP responses are updated at least every 3.5 days and have a maximum expiration of 7 days.

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

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements for Key Compromise

No stipulation.

4.9.13. Circumstances for Suspension

Not applicable.

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

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

4.10.1. Operational Characteristics

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

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 Subscriber Agreement terminates or expires without renewal.

4.12. Key Escrow and Recovery

Sectigo does not create or store the Subscriber's private key for publicly trusted TLS Server Certificates. In general, Sectigo does not provide key escrow or key backup services. In general, Sectigo expects an Applicant to generate key-pairs in its own environment and to pass only the Public Key to Sectigo for inclusion in the Certificates issued.

In certain enterprise scenarios, where specifically provided for by contract between Sectigo and the Subscriber enterprise, Sectigo provides key backup for Certificates to be used for document signing and provides key escrow for Certificates to be used for (typically email) encryption. In order to effectuate backup and escrow where contracted, Sectigo generates the key-pairs for the relevant Certificates and passes the encrypted Private Key to the Subscriber along with the original delivery of the public Certificate.

4.12.1. Key Escrow and Recovery Policy and Practices

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

Escrowed Private Keys are kept for three years after the corresponding Certificate's expiry prior to their destruction. Private Keys are destroyed by deleting the key from the storage material immediately, and from all related back up material within a further 12-month period.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

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

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

5.1. Physical Controls

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

5.1.1. Site Location and Construction

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

5.1.2. Physical Access

Card access systems are in place to control and monitor access to all areas of the facility. Access to the Sectigo physical machinery within the secure facility is protected with locked

cabinets and logical access controls. Security perimeters are clearly defined for all Sectigo locations. All of Sectigo's entrances and exits are secured or monitored by security personnel, reception staff, or monitoring/control systems.

5.1.3. Power and Air Conditioning

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

5.1.4. Water Exposures

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

5.1.5. Fire Prevention and Protection

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

5.1.6. Media Storage

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

5.1.7. Waste Disposal

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

5.1.8. Off-Site Backup

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

5.2. Procedural Controls

5.2.1. Trusted Roles

Trusted roles are assigned by senior members of the management team who decide permissions with signed 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 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 CPS and recording the details of approval and issuance steps taken identity vetting tasks are completed.

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

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

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

5.2.1.4. Internal Auditors

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

5.2.2. Number of Persons Required per Task

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

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

5.2.3. Identification and Authentication for Each Role

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

5.2.4. Roles Requiring Separation of Duties

No Trusted Roles can assume any other role, except Operator

5.3. Personnel Controls

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

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

5.3.1. Qualifications, Experience, and Clearance Requirements

Consistent with this CPS, 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.

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

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

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. CA Administrators are trained in the operation and installation of CA software. Operators are trained in the maintenance, configuration, and use of the specific software, operating systems, and hardware systems used by Sectigo. Internal Auditors are trained to proficiency in the general principles of systems and process audit as well as familiarity with Sectigo's policies and procedures. CA Officers are trained in Sectigo's validation and verification policies and procedures.

5.3.4. Retraining Frequency and Requirements

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

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

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

5.3.7. Independent Contractor Requirements

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

5.3.8. Documentation Supplied to Personnel

The selection of documentation supplied to Sectigo personnel is based on the role(s) they are to fill. Such documentation may include a copy of this CPS, the CA/B Forum Baseline Requirements, EV Guidelines, and the EVG for Code Signing, as well as the Code Signing BR and other technical and operational documentation necessary to maintain Sectigo's CA operations.

5.4. Audit Logging Procedures

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

5.4.1. Types of Events Recorded

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 hardware security module events, such as usage, de-installation, service or repair and retirement
- Successful and unsuccessful Sectigo PKI access attempts
- Secure CA facility visitor entry and exit

Certificate Application Information:

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

All logs include the following elements:

- Date and time of entry
- Serial or sequence number 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

When the removable media reaches the end of its life it is wiped by a third party secure data destruction facility and the Certificates of destruction are archived.

5.4.4. Protection of Audit Log

These media are only removed by Sectigo staff on a visit to the data center, and when not in the data center are held either in a safe in a locked office within the development site, or off-site in a secure storage facility.

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 separate local servers/HDDs and transferred off-site over encrypted VPN to remote servers/HDDs.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.

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

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

5.5. Records Archival

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

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 CPS;
- 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 digital 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

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

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 CPS.

5.5.7. Procedures to Obtain and Verify Archive Information

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

5.6. Key Changeover

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

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

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

The UTN-USERFirst-Hardware Certificate is present in Explorer 5.01 and above, Netscape 8.1 and above, Opera 8.0 and above, Mozilla 1.76 and above, Konqueror 3.5.2 and above, Safari 1.2 and above, FireFox 1.02 and above, Camino and SeaMonkey and is made available through these browsers.

The AddTrustExternalCARoot Certificate is present in Netscape 4.x and above, Opera 8.00 and above, Mozilla .06 and above, Konqueror, Safari 1.0 and above, Camino and SeaMonkey and is made available to Relying Parties through these browsers.

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

5.7. Compromise and Disaster Recovery

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

5.7.1. Incident and Compromise Handling Procedures

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

These procedures are in place to ensure that:

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

To maintain the integrity of its services Sectigo implements, documents, and periodically tests appropriate contingency and disaster recovery plans and procedures. These procedures define and contain a formal incident management reporting process, incident response, and incident escalation procedures to ensure professional incident management and the return to normal operations within a timely manner. 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 a co-location facility run by a commercial data-center, and all of the critical computer equipment is duplicated within the facility. Incoming power and connectivity feeds are duplicated. The duplicate equipment is ready to take over the role of providing the implementation of the CA, and allows Sectigo to specify a maximum system outage time (in case of critical systems failure) of 1 hour. Sectigo operations are distributed across several sites worldwide. All sites offer facilities to manage the lifecycle of a Certificate, including but not limited to the application, issuance, revocation and renewal of such Certificates. As well as a fully redundant CA system, Sectigo maintains provisions for the activation of a backup CA and a secondary site should the primary site suffer a total loss of systems. This disaster recovery plan states that Sectigo will endeavor to minimize interruptions to its CA operations.

5.8. CA or RA Termination

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

- Providing Subscribers of valid Certificates, Relying Parties, and other affected parties with ninety (90) days' notice of its intention to cease acting as a CA.

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

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

6. TECHNICAL SECURITY CONTROLS

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

Sectigo is not involved in functions associated with the generation, issuance, decommissioning or destruction of a Subscriber key pair, other than from suitably enabled enterprise accounts operated through the Sectigo Certificate Manager service which provide key pair generation, and optionally backup and escrow for client and email (Dual Use) certificates.

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

In general, unless otherwise noted in this CPS, Subscriber is solely responsible for the generation of an asymmetric cryptographic key pair (RSA or ECDSA) appropriate to the Certificate type being applied for. During application, the Subscriber will generally be required to submit a Public Key and other personal / corporate details in the form of a Certificate Signing Request (CSR) or SPKAC.

Secure Server Certificate requests are usually generated using the key generation facilities available in the Subscriber's webserver software.

Client Certificate requests are usually generated using the cryptographic service provider module software present in popular browsers, although they may also be submitted as a PKCS#10 or SPKAC.

Sectigo Dual Use Certificate requests are generated by Sectigo on Sectigo's servers. The Sectigo Certificate Manager software generates the Private Key on behalf of the end user and delivers the Private Key and Certificate to the end user.

Key pairs for EV Code Signing Certificates and End Entity Certificates issued pursuant to Adobe Approved Trust List requirements SHALL be generated, stored and used in a crypto

module that meets or exceeds the requirements of FIPS 140-2 level 2. Acceptable methods of satisfying this requirement include (but are not limited to) the following:

- Sectigo ships a suitable hardware crypto module, with a preinstalled key pair, in the form of a smartcard or USB device or similar
- The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate indicating that the key is managed in a suitable hardware module,
- The Subscriber provides a suitable IT audit indicating that its operating environment achieves a level of security at least equivalent to that of FIPS 140-2 level 2.

For Root CA Key Pairs created under this CPS Sectigo:

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

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

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

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

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

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

Access to the cryptographic operation software on the HSM is controlled, at a minimum, through the use of multi person Smart Cards & PINs, which must be entered/presented before any key operations may be performed. Access to the Smart Cards & PINs is restricted to authorised Sectigo Officers under multi person control (Sectigo settings require N from M cards to be present). Authorised Sectigo personnel with access to Smart Cards & PINs is logged.

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

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

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

6.1.2. Private Key Delivery to Subscriber

Where Subscriber keys are generated on Sectigo's servers, they are delivered to the Subscriber over an encrypted communication. Sectigo does not generate keys for SSL/TLS end entity server certificates.

Where key pairs for EV Code Signing Certificates or end entity certificates issued pursuant to Adobe Approved Trust List requirements are generated by Sectigo, Sectigo authorized personnel will provide the FIPS-140 L2 crypto module's random, unguessable PIN to the subscriber named in the subscriber certificate after validating that their identity matches the subscriber certificate. The cryptographic device will be configured to not allow the export of the private key.

6.1.3. Public Key Delivery to Certificate Issuer

Secure Server Certificate requests are generated using the Subscriber's webserver software and the request is submitted to Sectigo in the form of a PKCS #10 Certificate Signing Request (CSR). Submission is made electronically via the Sectigo website or through a Sectigo approved RA.

Secure Email Certificate requests are generated using the Subscriber's cryptographic service provider software present in the Subscriber's browser and submitted to Sectigo in the form of a PKCS#10 Certificate Signing Request (CSR). The Subscriber's browser generally makes submission automatically.

Code Signing Certificate requests are typically generated using the cryptographic service provider software present in the Subscriber's browser and submitted automatically to Sectigo in the form of a PKCS#10 Certificate Signing Request (CSR). The Private Key may

either be allowed to remain in the cryptographic service provider, or may be exported to the Subscriber's hard drive.

6.1.4. CA Public Key Delivery to Relying Parties

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

6.1.5. Key Sizes

COMMON_NAME	KEY_SIZE
AAA Certificate Services	RSA 2048
Secure Certificate Services	RSA 2048
Trusted Certificate Services	RSA 2048
UTN-USERFirst-Client Authentication and Email	RSA 2048
UTN - DATACorp SGC	RSA 2048
UTN-USERFirst-Hardware	RSA 2048
UTN-USERFirst-Object	RSA 2048
AddTrust Class 1 CA Root	RSA 2048
AddTrust External CA Root	RSA 2048
AddTrust Public CA Root	RSA 2048
AddTrust Qualified CA Root	RSA 2048
COMODO Certification Authority	RSA 2048
COMODO RSA Certification Authority	RSA 4096
USERTrust RSA Certification Authority	RSA 4096
COMODO ECC Certification Authority	ECC 384
USERTrust ECC Certification Authority	ECC 384

EV Code Signing and Adobe Document Signing certificate key sizes SHALL be governed by NIST key management guidelines. SSL/TLS end entity certificates SHALL have minimum RSA modulus size of 2048.

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.

RSA: Sectigo confirms that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 216+1 and 2256-1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89]

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

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

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

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

1. Digital signature, for verifying digital signatures that have purposes other than those identified in b), f) or g), that is, for entity authentication and data origin authentication with integrity
2. Non-repudiation, for verifying digital signatures used in providing a nonrepudiation service which protects against the signing entity falsely denying some action (excluding Certificate or CRL signing, as in f) or g) below)
3. Key encipherment, for enciphering keys or other security information, e.g. for key transport
4. Data encipherment, for enciphering user data, but not keys or other security information as in c) above
5. Key agreement, for use as a Public Key agreement key
6. Key Certificate signing, for verifying a CA's signature on Certificates, used in CA Certificates only
7. CRL signing, for verifying a CA's signature on CRLs
8. Encipher only, Public Key agreement key for use only in enciphering data when used with key agreement
9. Decipher only, Public Key agreement key for use only in deciphering data when used with key agreement

The appearance of a key usage in this section 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

The Sectigo Infrastructure uses trustworthy systems to provide Certificate services. A trustworthy system is computer hardware, software and procedures that provide an

acceptable resilience against security risks, provide a reasonable level of availability, reliability and correct operation, and enforce a security policy.

Sectigo strongly urges Subscribers to use a password or equivalent authentication method to prevent unauthorized access and usage of the Subscriber Private Key.

6.2.1. Cryptographic Module Standards and Controls

Sectigo securely generates and protects its own Private Key(s), using a trustworthy system certified to FIPS 140-2 Level 3 or higher, and takes necessary precautions to prevent the compromise or unauthorized usage of it.

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

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

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

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

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

6.2.5. Private Key Archival

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 CPS.

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 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

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

6.2.9. Method of Deactivating Private Key

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

6.2.10. Method of Destroying Private Key

Destroying a Private Key means the destruction of all active keys, both backed-up and stored. Destroying a Private Key may comprise of removing it from the HSM or removing it from the active backup set. Private Keys are destroyed in accordance with FIPS PUB 140-2.

6.2.11. Cryptographic Module Rating

See section 6.2.1 of this CPS.

6.3. Other Aspects of Key Pair Management

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

6.3.1. Public Key Archival

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

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Certificates are valid upon issuance by Sectigo and acceptance by the Subscriber. Generally, the Certificate validity period will be from 1 to 10 years, however, Sectigo reserves the right to offer validity periods outside of this standard validity period. The maximum duration of a SSL/TLS end entity server certificate is 825 days and Sectigo verifies all information that is included in SSL/TLS Certificates at time intervals of 825 days or less.

The expiration of Sectigo's Root CA keys is set out in Table 6.3.2. Subordinate CA key lifetimes are either the same or shorter than those of the CA by which they are signed.

Table 6.3.2

COMMON_NAME	VALID_TO	KEY_SIZE	SIGNATURE
AAA Certificate Services	31/Dec/2028	RSA 2048	sha1WithRSA
Secure Certificate Services	31/Dec/2028	RSA 2048	sha1WithRSA
Trusted Certificate Services	31/Dec/2028	RSA 2048	sha1WithRSA
UTN-USERFirst-Client Authentication and Email	09/Jul/2019 17:36:58	RSA 2048	sha1WithRSA
UTN - DATACorp SGC	24/Jun/2019 19:06:30	RSA 2048	sha1WithRSA
UTN-USERFirst-Hardware	09/Jul/2019 18:19:22	RSA 2048	sha1WithRSA
UTN-USERFirst-Object	09/Jul/2019 18:40:36	RSA 2048	sha1WithRSA
AddTrust Class 1 CA Root	30/May/2020 10:38:31	RSA 2048	sha1WithRSA
AddTrust External CA Root	30/May/2020 10:48:38	RSA 2048	sha1WithRSA
AddTrust Public CA Root	30/May/2020 10:41:50	RSA 2048	sha1WithRSA
AddTrust Qualified CA Root	30/May/2020 10:44:50	RSA 2048	sha1WithRSA
COMODO Certification Authority	31/Dec/2030 10:48:38	RSA 2048	sha1WithRSA
COMODO RSA Certification Authority	18/Jan/2038 23:59:59	RSA 4096	sha384WithRSA
USERTrust RSA Certification Authority	18/Jan/2038 23:59:59	RSA 4096	sha384WithRSA
COMODO ECC Certification Authority	18/Jan/2038 23:59:59	ECDSA 384	ecdsa-with-SHA384
USERTrust ECC Certification Authority	18/Jan/2038 23:59:59	ECDSA 384	ecdsa-with-SHA384

Sectigo protects its CA Root key pairs in accordance with its AICPA/CICA WebTrust program compliant infrastructure and CPS. Details of Sectigo's WebTrust compliancy are available at its official website (www.sectigo.com).

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 Root CA Systems in a high security zone and in an offline state or air-gapped from other networks;
- Maintaining and protecting Issuing Systems, Certificate Management Systems, and Security Support systems;
- Configuring Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End/Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in Sectigo's operations and allowing only those that are approved by Sectigo;
- Reviewing configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End/Internal-Support Systems on a weekly basis;
- Undergoing penetration tests on a periodic basis and after significant infrastructure or application upgrades;
- Granting administration access to Certificate 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. Lifecycle Technical Controls

6.6.1. System Development Controls

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

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

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

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

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

Development and QA team members do not 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. Lifecycle 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.

6.8. Time-Stamping

Sectigo operates two Time-Stamping Authorities (TSA). The Sectigo TSAs are intended only for use in signing software when used in conjunction with a Sectigo Code-signing Certificate. No warranty is offered, and no liability will be accepted for any use of the Sectigo TSAs which is made other than signing software in conjunction with a Sectigo Code-signing Certificate.

The Sectigo Authenticode time-stamping service is available at the URL http://timestamp.comodoca.com/authenticode.

Sectigo also offers a RFC3161 TSA, whose URL is:

http://timestamp.comodoca.com/rfc3161.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Sectigo uses version 3 of the X.509 standard to construct digital Certificates for use within the Sectigo PKI. X.509v3 allows a CA to add certain Certificate extensions to the basic

Certificate structure. Sectigo uses a number of Certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. X.509v3 is a standard of the International Telecommunications Union for digital Certificates.

7.1. Certificate Profile

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

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

A Certificate profile contains fields as specified below:

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

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

- Secure Server Certificates, Secure Email Certificates, and Code-signing Certificates
    - Applicant's name or organizational name.
    - Code of Applicant's country.
    - Organizational unit name, street address, city, state.
    - Issuing certification authority (Sectigo).
    - Applicant's Public Key.
    - Sectigo digital signature.
    - Signing algorithm.
    - Validity period of the digital Certificate.
    - Serial number of the digital Certificate.
- Secure Server Certificates additionally have:
    - Applicant's fully qualified domain name(s).
- Secure Email Certificates additionally have:
    - Applicant's e-mail address(es).

7.1.1. Version Number(s)

Certificate versions are all X.509 version 3

7.1.2. Certificate Extensions

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

Enhanced naming is the usage of an extended organization field in an X.509v3 Certificate. Information contained in the organizational unit field is also included in the Certificate Policy extension that Sectigo may use.

7.1.2.1. Root CAs

Sectigo Root CA certificates contain a basicConstraints extension marked critical. The cA field is set true. The pathLenConstraint is not present.

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

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

Sectigo Root CA certificates do not contain a certificatePolicies extension.

7.1.2.2. Subordinate CAs

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

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

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

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

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

7.1.2.3. Subscriber Certificates

Sectigo Subscriber Certificates contain a certificatePolicies extension that includes one or more policyIdentifiers and usually contains a policyQualifier referring to the CPS URI but not including a userNotice.

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

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

Sectigo Subscriber certificates contain a basicConstraints extension marked critical. The cA field is not set.

Sectigo Subscriber certificates contain a keyUsage extension marked critical. Bit positions for keyCertSign and cRLSign are NOT set.

Sectigo Subscriber certificates contain a non-critical extKeyUsage extension.
codeSigning certificates contain id-kp-codeSigning.
serverAuthentication certificates contain both id-kp-serverAuth and id-kp-clientAuth.
emailProtection certificates contain id-kp-emailProtection. Other values are not typically present in serverAuthentication and emailProtection certificates.

7.1.2.4. All Certificates

All other fields and extensions are in accordance with RFC5280.

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

Sectigo does not issue certificates containing Extensions that do not apply in the context of the public Internet unless:
i. such value falls within an OID arc for which the Applicant demonstrates ownership, or
ii. the Applicant can otherwise demonstrate the right to assert the data in a public context;

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

7.1.3. Algorithm Object Identifiers

Sectigo Certificates are signed using algorithms with these identifiers:

From RFC3279:

(not used for SSL/TLS Server Certificates, EV Code Signing, Adobe Document Signing, or OCSP Certificates)

```
sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {
iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
pkcs-1(1) 5 }
```

From RFC5754:

```
sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1)
member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }

sha384WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1)
member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 }
```

From RFC5758:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }

ecdsa-with-SHA384 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
```

Sectigo does not sign Certificates using RSA with PSS padding.

For ECDSA, Sectigo uses and accepts only the NIST Suite B curves.

7.1.4. Name Forms

Name forms are as stipulated in 3.1.1 of this CPS.

7.1.4.1. Issuer Information

The content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, section 4.1.2.4.

7.1.4.2. Subject Information – Subscriber Certificates

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

Sectigo does not include Domain Names or IP Addresses in a Subject attribute except as specified in Section 3.2.2. of this CPS.

7.1.4.2.1. Subject Alternative Name Extension

For serverAuthentication certificates, this extension will be present and will contain at least one entry. Each entry is either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server. Sectigo confirms that the Applicant controls the Fully-Qualified Domain Name or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate. Wildcard FQDNs are permitted.

For emailProtection certificates, this extension may be present, in which case it will contain at least one entry. Each entry is an rfc822Name. Sectigo confirms that the Applicant controls the email account associated with the email address referenced in the certificate or has been authorized by the email account holder to act on the account holder's behalf.

7.1.4.2.2. Subject Distinguished Name Fields

1. commonName
   If present in serverAuthentication certificates, this field contains a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension (see above).

2. organizationName
   If present in serverAuthentication certificates, this field contains the Subject's name and/or DBA as verified under Section 3.2.2.2 or 3.2.2.3.

   Sectigo may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", we may use "Company Name Inc." or "Company Name".

   Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, we may use the subject:organizationName field to convey a natural person Subject's name or DBA.

3. (omitted)

4. streetAddress
   If present in serverAuthentication certificates, this field contains the Subject's street address information as verified under Section 3.2.2.2 or 3.2.2.3.

5. localityName
   If present in serverAuthentication certificates, this field contains the Subject's locality information as verified under Section 3.2.2.2 or 3.2.2.3.

   Where the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(h), the localityName field may contain the Subject's locality and/or state or province information as verified under Section 3.2.2.2 or 3.2.2.3.

6. stateOrProvinceName
   If present in serverAuthentication certificates, this field contains the Subject's state or province information as verified under Section 3.2.2.2 or 3.2.2.3.

   If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(h), the subject:stateOrProvinceName field may contain the full name of the Subject's country information as verified under Section 3.2.2.2 or 3.2.2.3.

7. postalCode
   If present in serverAuthentication certificates, this field contains the Subject's zip or postal code information as verified under Section 3.2.2.2 or 3.2.2.3.

8. countryName
   If present in serverAuthentication certificates, this field contains the Subject's two-letter ISO 3166-1 country code information as verified under Section 3.2.2.2 or 3.2.2.3.

   If a Country is not represented by an official ISO 3166-1 country code, Sectigo will specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

9. organizationalUnitName
   Sectigo implements processes that prevent an organizationalUnitName attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the we have verified this information in accordance with Section 3.2.2.2 or 3.2.2.3 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in under Section 3.2.2.2 or 3.2.2.3.

10. EV and EV Codesigning Certificates SHALL also include the following fields as per Section 9.2 of the EVG:

    a. Subject Business Category

       i. subject:businessCategory (OID: 2.5.4.15)

    b. Subject Jurisdiction of Incorporation or Registration

       i. subject:jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1) (if required)

       ii. subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2) (if required)

       iii. subject:jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)

    c. Subject Registration Number

       i. Subject:serialNumber (OID: 2.5.4.5)

11. Other Subject Attributes
    If present in serverAuthentication certificates, all other optional attributes, will contain information that has been verified by Sectigo. Optional attributes will not contain metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.3. Subject Information – Root Certificates and Subordinate CA Certificates

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

7.1.4.3.1. Subject Distinguished Name Fields

1. commonName

   This field will be present and may be used as an identifier for the CA certificate. Across all CA certificates issued by Sectigo, each unique subject:commonName will be paired with only one CA keypair.

2. organizationName

   This field will be present and contains the Subject CA's name or DBA as verified under Section 3.2.2.2.

   Sectigo may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", we may use "Company Name Inc." or "Company Name".

3. countryName

   This field will be present and contains the Subject's two-letter ISO 3166-1 country code information as verified under Section 3.2.2.2 or 3.2.2.3.

7.1.5. Name Constraints

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

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

7.1.5.1. TLS Web Server Authentication

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

1. For each dNSName in permittedSubtrees, Sectigo confirms that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of section 3.2.2.1 of this CPS.

2. For each iPAddress range in permittedSubtrees, Sectigo confirms that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf.

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

If the Subordinate CA Certificate is not allowed to issue certificates with an iPAddress, then the Subordinate CA Certificate will specify the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate will include within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate will also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0).
Otherwise, the Subordinate CA Certificate will include at least one iPAddress in permittedSubtrees.

7.1.5.2. E-mail Protection

For Name Constrained CAs that include the id-kp-emailProtection extended key usage, the CA certificate includes the Name Constraints X.509v3 extension with constraints on rfc822Name, with at least one name in permittedSubtrees, each such name having its ownership validated according to section 3.2.2.4 of the Baseline Requirements.

7.1.5.3. Code Signing

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

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

7.1.6. Certificate Policy Object Identifier

Sectigo uses policy OIDs under the arcs:

iso(1)
identified-organization(3)
dod(6)
internet(1)
private(4)
enterprise(1)
6449
certificates(1)
policies(2),

and also

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

End entity certificate policies	
1.3.6.1.4.1.6449.1.2.1.1.1	Personal Secure Email
1.3.6.1.4.1.6449.1.2.1.3.1	Secure Server

1.3.6.1.4.1.6449.1.2.1.3.2	Software Publisher
1.3.6.1.4.1.6449.1.2.1.3.4	InstantSSL
1.3.6.1.4.1.6449.1.2.1.3.5	Corporate Secure Email
1.3.6.1.4.1.6449.1.2.1.3.6	Enterprise-Wide Secure Email
1.3.6.1.4.1.6449.1.2.1.3.8	Timestamping Certificate
1.3.6.1.4.1.6449.1.2.1.5.1	Sectigo EV TLS Server Certificates
1.3.6.1.4.1.6449.1.2.1.6.1	Sectigo EV Code-signing Certificates
1.3.6.1.4.1.6449.1.2.1.6.6	Sectigo AATL Certified Document Services
2.23.140.1.2.1	DV TLS Server Certificates
2.23.140.1.2.2	OV TLS Organization Server Certificates
2.23.140.1.2.3	OV TLS Individual Server Certificates
2.23.140.1.1	EV TLS Server Certificate
2.23.140.1.4.1	Code Signing Certificates
1.2.840.113583.1.1.5	Adobe AuthenticDocumentsTrust
Arc for intermediate CA policy identifiers	
1.3.6.1.4.1.6449.1.2.2	Intermediate CA policies
Other Policy OIDs	
1.3.6.1.4.1.6449.2.1.1	Default Time-stamping Policy

7.1.7. Usage of Policy Constraints Extension

No stipulation

7.1.8. Policy Qualifiers Syntax and Semantics

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

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL Profile

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

The profile of the Sectigo CRL is as per the table below:

Version	[Version 1]	
Issuer Name	CountryName = [Root Certificate Country Name], OrganizationName=[Root Certificate Organization], CommonName=[Root Certificate Common Name]	

	[UTF8String encoding]	
This Update	[Date of Issuance]	
Next Update	[Date of Issuance + no more than 10 days]	
Revoked Certificates	CRL Entries	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]

7.2.1. Version Number(s)

Sectigo issues version 2 CRLs.

7.2.2. CRL and CRL Entry Extensions

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

7.3. OCSP Profile

Sectigo also publishes Certificate status information using Online Certificate Status Protocol (OCSP). Sectigo's OCSP responders are capable of providing a 'good' or 'revoked' status for all Certificates issued under the terms of this CPS. If queried for a certificate which was not issued by Sectigo the responder will provide 'unauthorized'. In the case of Code Signing Certificates only, the OCSP responders will continue to give a 'good' status for unrevoked Certificates even after their expiry – for at least 20 years from issuance. In the case of all other Certificate types 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 6960 and 5019.

7.3.2. OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust for Certification Authorities ("WebTrust for CAs"), ANS X9.79:2001 PKI Practices and Policy Framework, 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 AICPA/CICA WebTrust for CAs.

8.1. Frequency or Circumstances of Assessment

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

8.2. Identity/Qualifications of Assessor

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

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.1);
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
5. Bound by law, government regulation, or professional code of ethics; and
6. 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

WebTrust for CAs audit: 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

As per current version of *WebTrust for Certification Authorities*, *WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security*, *WebTrust for Certification Authorities –Extended Validation – SSL*, and *WebTrust for Certification Authorities –Extended Validation – Code Signing* which can be found at http://www.webtrust.org

8.5. Actions Taken as a Result of Deficiency

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

8.6. Communication of Results

WebTrust for CAs audit: 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.

8.7. Self-Audits

Sectigo performs regular self audits and audits of Registration Authorities in accordance with Section 8.7 of the Baseline Requirements.

9. OTHER BUSINESS AND LEGAL MATTERS

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

9.1. Fees

Sectigo charges Subscriber fees for some of the Certificate services it offers, including issuance, renewal and reissues (in accordance with the Sectigo Reissue Policy stated in 9.1.6 of this CPS). Such fees are detailed on the official Sectigo websites (www.sectigo.com, www.comodoca.com, www.instantssl.com,and www.enterprisessl.com).

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

9.1.1. Certificate Issuance or Renewal Fees

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

9.1.2. Certificate Access Fees

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

9.1.3. Revocation or Status Information Access Fees

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

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

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

9.1.6. Reissue Policy

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

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

9.2. Financial Responsibility

9.2.1. Insurance Coverage

Sectigo maintains professional Errors and Omissions Insurance.

9.2.2. Other Assets

No stipulation.

9.2.3. Warranty Coverage

If Sectigo was negligent in issuing a Certificate that resulted in a Covered Loss to a Relying Party, the Relying Party may be eligible under Sectigo's Relying Party Warranty to receive up to the Maximum Certificate Coverage per Incident, subject to the Total Payment Limit,

for all claims related to that Certificate. For complete terms and conditions, see the Relying Party Agreement and the Relying Party Warranty located in the Repository.

9.3. Confidentiality of Business Information

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

9.3.1. Scope of Confidential Information

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

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

9.3.2. Information Not Within the Scope of Confidential Information

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

9.3.3. Responsibility to Protect Confidential Information

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

9.3.4. Publication of Certificate Revocation Data

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

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

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

9.4.2. Information Treated as Private

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

9.4.3. Information not Deemed Private

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

9.4.4. Responsibility to Protect Private Information

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

9.4.5. Notice and Consent to Use Private Information

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

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

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

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

9.4.7. Other Information Disclosure Circumstances

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

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

9.5. Intellectual Property Rights

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

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

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

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

- Comply with this CPS and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certification services, including but not limited to the establishment and operation of the Sectigo Repository and web site for the operation of PKI services.
- Provide trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its Private Key(s).
- Provide and validate application procedures for the various types of Certificates that it may make publicly available.
- Issue digital Certificates in accordance with this CPS and fulfill its obligations presented herein.
- Upon receipt of a request from an RA operating within the Sectigo network; act promptly to issue a Sectigo Certificate in accordance with this CPS.
- 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 Sectigo CPS.
- Publish accepted Certificates in accordance with this CPS.
- Provide support to Subscribers and relying parties as described in this CPS.
- Revoke Certificates according to this CPS.
- Provide for the expiration and renewal of Certificates according to this CPS.
- Make available a copy of this CPS and applicable policies to requesting parties.

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

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

9.6.2. RA Representations and Warranties

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

- Receive applications for Sectigo Certificates in accordance with this CPS.
- Perform all verification actions prescribed by the Sectigo validation procedures and this CPS.
- Receive, verify and relay to Sectigo all requests for revocation of a Sectigo Certificate in accordance with the Sectigo revocation procedures and the CPS.
- Act according to relevant 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 to Sectigo and to relying parties that at the time of acceptance and until further notice:

- Digital signatures created using the Private Key corresponding to the Public Key included in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is properly operational at the time the digital signature is created.
- No unauthorized person has ever had access to the Subscriber's Private Key.
- All representations made by the Subscriber to Sectigo regarding the information contained in the Certificate are accurate and true.
- All information contained in the Certificate is accurate and true to the best of the Subscriber's knowledge or to the extent that the Subscriber had notice of such information whilst the Subscriber shall act promptly to notify Sectigo of any material inaccuracies in such information.
- The Certificate is used exclusively for authorized and legal purposes, consistent with this CPS.
- It will use a Sectigo Certificate only in conjunction with the entity named in the organization field of a digital Certificate (if applicable).
- The Subscriber retains control of her Private Key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.
- The Subscriber is an end-user Subscriber and not a CA, and will not use the Private Key corresponding to any Public Key listed in the Certificate for purposes of signing any Certificate (or any other format of certified Public Key) or CRL, as a CA or otherwise, unless expressly agreed in writing between Subscriber and Sectigo.
- The Subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of Sectigo.

- The Subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.
- The Subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

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

9.6.4. Relying Party Representations and Warranties

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

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

9.6.5. Representations and Warranties of other Participants

No stipulation.

9.7. Disclaimers of Warranties

9.7.1. Fitness for a Particular Purpose

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

9.7.2. Other Warranties

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

- The accuracy, authenticity, completeness or fitness of any unverified information contained in Certificates or otherwise compiled, published, or disseminated by or on

behalf of Sectigo except as it may be stated in the relevant product description below in this CPS and in the Sectigo insurance policy.
- 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 CPS.
- Does not warrant the quality, functions or performance of any software or hardware device.
- Although Sectigo is responsible for the revocation of a Certificate, it cannot be held liable if it cannot execute it for reasons outside its own control.
- The validity, completeness or availability of directories of Certificates issued by a third party (including an agent) unless specifically stated by Sectigo.

Sectigo assumes that user software that is claimed to be compliant with X.509v3 and other applicable standards enforces the requirements set out in this CPS. 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 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 CPS.

9.8.2. Exclusion of Certain Elements of Damages

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

- Any indirect, incidental or consequential damages.
- Any loss of profits.
- Any loss of data.

- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of Certificates or digital signatures.
- Any other transactions or services offered within the framework of this CPS.
- 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 CPS.
- 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 CPS.
- 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, Certificate Subscribers shall defend, indemnify, and hold Sectigo harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions on behalf of Sectigo.

9.10. Term and Termination

9.10.1. Term

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

9.10.2. Termination

This CPS, 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 CPS for Certificates issued under this CPS:

- All unpaid fees incurred under section 9.1 of this CPS;
- All responsibilities and obligations related to confidential information, including those stated in section 9.3 of this CPS;
- All responsibilities and obligations to protect private information, including those stated in section 9.4.4 of this CPS;
- All representations and warranties, including those stated in section 9.6 of this CPS;
- All warranties disclaimed in section 9.7 of this CPS for Certificates issued during the term of this CPS;
- All limitations of liability provided for in section 9.8 of this CPS; and
- All indemnities provided for in section 9.9 of this CPS.

Upon termination of this CPS, all PKI participants are bound by the terms of this CPS for Certificates issued during the term of this CPS 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 CPS 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 Certificate Policy Authority
3rd Floor, Building 26 Exchange Quay, Trafford Road
Salford, Greater Manchester, M5 3EQ, United Kingdom
Attention: Legal Practices
Email: legalnotices@sectigo.com

This CPS, related agreements and Certificate policies referenced within this document are available online in the Repository.

9.12. Amendments

Upon the Sectigo Certificate Policy Authority accepting such changes it deems to have significant impact on the users of this CPS, an updated edition of the CPS will be published at the Sectigo repository (available at https://www.sectigo.com/legal), with seven (7) days' notice given of upcoming changes and suitable incremental version numbering used to identify new editions. This CPS SHALL be updated at least once per year.

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 CPS and without changing the version number of this CPS.

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

9.12.2. Notification Mechanism and Period

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

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

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 CPS or the provision of Sectigo PKI services.

9.15. Compliance with Applicable Law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders, including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. Sectigo complies with all applicable laws, rules, regulations, ordinances, decrees, and orders when providing services pursuant to this CPS.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

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

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

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

9.16.5. Force Majeure

Neither Sectigo nor any independent third-party RA operating under a Sectigo Certification Authority, nor any Resellers, Co-marketers, nor any subcontractors, distributors, agents, suppliers, employees, or directors of any of the forgoing shall be in default hereunder or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or related to delays in performance or from failure to perform or comply with the terms of the Sectigo CPS, 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 CPS conflicts with other rules, guidelines, or contracts, this CPS 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 CPS.
- Expressly superseding this CPS 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 CPS, 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. Financial Limitations on Certificate Usage

Sectigo Certificates may only be used in connection with data transfer and transactions completed using a credit card and having a US dollar (US$) value no greater than the max transaction value associated with the Certificate detailed in section 9.2.3 of this CPS.

9.17.4. 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.

9.17.5. 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 CPS 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.

9.17.6. 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.

9.17.7. 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.

9.17.8. Subscriber Obligations

Unless otherwise stated in this CPS, 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 CPS 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 CPS.

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

Appendix A: Table of Acronyms

Acronym	Full Name
AICPA	American Institute of Certified Public Accountants
BR	Baseline Requirements (see Definitions
CA	Certificate Authority
CA/B (or CAB)	Certificate Authority/Browser (Forum)
CICA	Canadian Institute of Chartered Accountants
CMS	Certificate Management System
CPS	Certification Practice Statement
CRL(s)	Certificate Revocation List(s)
CSR	Certificate Signing Request
DN	Distinguished Name
DSA	Digital Signature Algorithm
EPKI	Enterprise Public Key Infrastructure Manager
ECDSA	Elliptic Curve Digital Signature Algorithm
EVG	EV Guidelines (see Definitions)

FIPS PUB	Federal Information Processing Standards Publication
FQDN	fully qualified domain name
FTP	File Transfer Protocol
HSM	Hardware Signing Module
HTTP	Hypertext Transfer Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
MDC	Multiple Domain Certificate
NIST	National Institute for Standards and Technology
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
RA(s)	Registration Authority(ies)
RFC	Request for Comments
RSA	Rivest Shamir Adleman
SAN	Subject Alternate Name
SHA	Secure Hash Algorithm
SGC	Server Gated Cryptography
S/MIME	Secure/Multipurpose Internet Mail Extension(s)
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TSA	Time Stamping Authority
UTC	Coordinated Universal Time

URL	Uniform Resource Locator

Appendix B: Table of Definitions

Term	Definition
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 mandatory provisions of the Baseline Requirements.
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
Baseline Requirements (BR)	Means the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, published at https://www.cabforum.org.
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.
Code Signing BR	*Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates* currently published at https://www.casecurity.org
Demand Deposit Account	a deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as: a checking account, a share draft account, or a current account
Domain Contact	Means the Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.
Domain Name	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).
EV Guidelines (EVG)	CA/Browser Forum *Guidelines for the Issuance and Management of Extended Validation Certificates* published at https://www.cabforum.org
EVG for Code Signing	CA/Browser Forum *Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates* published at https://www.cabforum.org
Front End/Internal Support System	Means a system with a public IP address, including a web server, mail server, DNS server, jump host, or authentication server.
Grace Period	Means the period during which the Subscriber must make a revocation request.
IP Address Registration Authority	The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).
Issuing System	Means a system used to sign Certificates or validity status information.
Legal Entity	Means an association, corporation, partnership, proprietorship, trust, government entity, or other entity with legal standing in a country's legal system.
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.
Random Value	Means a value specified by Sectigo to the Applicant that exhibits at least 112 bits of entropy.
Reliable Method of Communication	Means a method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.
Relying Party	Means an entity that relies upon the information contained within the Certificate.
Relying Party Agreement	means an agreement between Sectigo and a Relying Party that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference in the Repository.
Repository	Means Sectigo's repository, available at www.sectigo.com/legal.
Request Token	Means a value derived in a method specified by Sectigo which binds a demonstration of control to the certificate request.
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.
Sectigo Certificate Policy Authority	Means the entity charged with the maintenance and publication of this CPS.
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 is an entity that has been issued a Certificate.
Subscriber Agreement	Means an agreement that must be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the digital Certificate product type as presented during the product online order process and is available for reference in the Repository.
Verified Method of	Method of communication as defined and verified in

Communication	conformance with Section 11.5 of the EVG
WebTrust for Certification Authorities	Means the current program for CAs located at http://www.webtrust.org/homepage-documents/item27839.aspx.
Wildcard Certificate	A Certificate containing an asterisk (*) in the left-most position of any of the FQDNs contained in the Certificate Subject
Wildcard Domain Name	A Domain Name consisting of a single asterisk character followed by a single full stop character (*.) followed by a FQDN
X.509	Means the ITU-T standard for Certificates and their corresponding authentication framework

Appendix C: Certificate Profiles

Showing the outline profiles of Sectigo Certificates.

Root certificate

Version:	3 (0x2)	
Serial Number:	containing at least 64 bits of output from a CSPRNG	
Signature Algorithm:	sha384WithRSAEncryption or ecdsa-with-SHA384	
Issuer:	commonName	USERTrust RSA Certification Authority
	organizationName	The USERTRUST Network
	locality	Jersey City
	stateOrProvince	New Jersey
	countryName	US
Validity:	Not Before:	Jan 19 00:00:00 2010 GMT
	Not After:	Jan 18 23:59:59 2038 GMT
Subject:	commonName	USERTrust RSA Certification Authority
	organizationName	The USERTRUST Network
	locality	Jersey City
	stateOrProvince	New Jersey
	countryName	US
Subject Public Key Info:	rsaEncryption and RSAPublicKey, or	
	id-ecPublicKey and EcpkParameters	
X509v3 Subject Key Identifier:	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of	

	unused bits)	
X509v3 Key Usage: critical	Certificate Sign, CRL Sign	
X509v3 Basic Constraints: critical	CA:TRUE	

ISSUING CA certificate

E.g DV TLS Issuing CA

Version:	3 (0x2)	
Serial Number:	containing at least 64 bits of output from a CSPRNG	
Signature Algorithm:	sha384WithRSAEncryption or ecdsa-with-SHA384	
Issuer:	commonName	USERTrust RSA Certification Authority
	organizationName	The USERTRUST Network
	locality	Jersey City
	stateOrProvince	New Jersey
	countryName	US
Validity:	Not Before:	Jan 19 00:00:00 2010 GMT
	Not After:	Jan 18 23:59:59 2038 GMT
Subject:	commonName	Sectigo RSA Domain Validation Secure Server CA
	organizationName	Sectigo Limited
	locality	Salford
	stateOrProvince	Greater Manchester
	countryName	GB
Subject Public Key Info:	rsaEncryption and RSAPublicKey, or	
	id-ecPublicKey and EcpkParameters	
X509v3 Authority Key Identifier:	keyID: based on the subject key identifier in the issuer's certificate	
X509v3 Subject Key Identifier:	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)	
X509v3 Key Usage: critical	Digital Signature, Certificate Sign, CRL Sign	
X509v3 Basic Constraints: critical	CA:TRUE, pathlen:0	
X509v3 Extended Key Usage:	TLS Web Server Authentication,	
	TLS Web Client Authentication	
X509v3 Certificate Policies:	X509v3 Any Policy, 2.23.140.1.2.1	
X509v3 CRL Distribution	http://crl.usertrust.com/USERTrustRSACertificationAuth	

Points:	ority.crl	
Authority Information Access:	CA Issuers - http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt OCSP - http://ocsp.usertrust.com	

E.g EV TLS Issuing CA. As DV issuing CA, except:

Subject:	commonName	Sectigo RSA **Extended** Validation Secure Server CA
X509v3 Certificate Policies:	X509v3 Any Policy **CPS: https://cps.usertrust.com**	

E.g. EV Code Signing CA. As DV issuing CA, except:

Subject:	commonName	Sectigo RSA **Extended Validation Code Signing** CA
X509v3 Extended Key Usage:	**Code Signing, Time Stamping**	
X509v3 Certificate Policies:	X509v3 Any Policy	

END ENTITY certificate

E.g DV Secure Server Certificate

Version:	3 (0x2)	
Serial Number:	containing at least 64 bits of output from a CSPRNG	
Signature Algorithm:	sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer:	commonName	Sectigo ECC Domain Validation Secure Server CA
	organizationName	Sectigo Limited
	locality	Salford
	stateOrProvince	Greater Manchester
	countryName	GB
Validity:	Not Before:	Feb 19 00:00:00 2019 GMT
	Not After:	Feb 19 23:59:59 2020 GMT
Subject:	commonName	*.example.com
	organizationalUnit	PositiveSSL
	organizationalUnit	Hosted by WeHost WebHosting, Inc.
	organizationName	Customer Example Inc.
	organizationName	Domain Control Validated
Subject Public Key Info:	id-ecPublicKey and EcpkParameters or	

	rsaEncryption and RSAPublicKey	
X509v3 Authority Key Identifier:	keyID: based on the subject key identifier in the issuer's certificate	
X509v3 Subject Key Identifier:	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)	
X509v3 Key Usage: critical	Digital Signature	
X509v3 Basic Constraints: critical	CA:FALSE	
X509v3 Extended Key Usage:	TLS Web Server Authentication,	
	TLS Web Client Authentication	
X509v3 Certificate Policies:	1.3.6.1.4.1.6449.1.2.2.7, CPS: https://sectigo.com/CPS, 2.23.140.1.2.1	
X509v3 CRL Distribution Points:	http://crl.sectigo.com/SectigoECCOrganizationValidationSecureServerCA.crl	
Authority Information Access:	CA Issuers - http://crt.sectigo.com/SectigoECCDomainValidationSecureServerCA.crt OCSP - http://ocsp.sectigo.com	
X509v3 Subject Alternative Name:	DNS:*.example.com, DNS:example.com	
CT Precertificate SCTs:	2 or more SCTs as per RFC6962	

E.g OV Secure Server Certificate. As DV Secure Server Certificate, except:

Issuer:	commonName	Sectigo ECC **Organization** Validation Secure Server CA
Subject:	commonName	*.example.com
	organizationalUnit	PremiumSSL Wildcard
	organizationalUnit	IT Department
	organizationName	Customer Example Inc.
	street	18 Main Street
	locality	Springfield
	stateOrProvince	New Jersey
	postalCode	10100
	countryName	US
X509v3 Certificate Policies:	1.3.6.1.4.1.6449.1.2.1.3.4, CPS: https://sectigo.com/CPS, 2.23.140.1.2.2	

E.g EV Secure Server Certificate. As OV Secure Server Certificate, except:

Issuer:	commonName	Sectigo ECC **Extended** Validation Secure Server CA
Subject: (additional subject fields)	businessCategory	Private Organization
	jurisdictionST	New jersey
	jurisdictionC	US
	serialNumber	1234567
X509v3 Certificate Policies:	1.3.6.1.4.1.6449.1.2.1.**5.1**, CPS: https://sectigo.com/CPS, 2.23.140.**1.1**	

E.g codeSigning certificate

Version:	3 (0x2)	
Serial Number:	containing at least 64 bits of output from a CSPRNG	
Signature Algorithm:	sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer:	commonName	Sectigo RSA Code Signing CA
	organizationName	Sectigo Limited
	locality	Salford
	stateOrProvince	Greater Manchester
	countryName	GB
Validity:	Not Before:	Feb 19 00:00:00 2019 GMT
	Not After:	Feb 19 23:59:59 2020 GMT
Subject:	commonName	Customer Example Inc.
	organizationName	Customer Example Inc.
	street	18 Main Street
	locality	Springfield
	stateOrProvince	New Jersey
	postalCode	10100
	countryName	US
Subject Public Key Info:	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	
X509v3 Authority Key Identifier:	keyID: based on the subject key identifier in the issuer's certificate	
X509v3 Subject Key Identifier:	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)	
X509v3 Key Usage: critical	Digital Signature, Key Encipherment	
X509v3 Basic Constraints: critical	CA:FALSE	
X509v3 Extended Key Usage:	Code Signing	
X509v3 Certificate	1.3.6.1.4.1.6449.1.2.1.3.2	

Policies:	, CPS: https://sectigo.com/CPS	
X509v3 CRL Distribution Points:	http://crl.sectigo.com/SectigoRSACodeSigningCA.crl	
Authority Information Access:	CA Issuers - http://crt.sectigo.com/SectigoRSACodeSigningCA.crt OCSP - http://ocsp.sectigo.com	
X509v3 Subject Alternative Name:	email: user@example.com	

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

Issuer:	commonName	Sectigo ECC **Extended Validation Code Signing CA**
Subject: (additional subject fields)	businessCategory	Private Organization
	jurisdictionST	New jersey
	jurisdictionC	US
	serialNumber	1234567
X509v3 Certificate Policies:	1.3.6.1.4.1.6449.1.2.1.**6.1** , CPS: https://sectigo.com/CPS	

E.g Adobe Document Signing certificate

Version:	3 (0x2)	
Serial Number:	containing at least 64 bits of output from a CSPRNG	
Signature Algorithm:	Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer:	commonName	Sectigo RSA Document Signing CA
	organizationName	Sectigo Limited
	locality	Salford
	stateOrProvince	Greater Manchester
	countryName	GB
Validity:	Not Before:	May 6 00:00:00 2019 GMT
	Not After:	May 6 23:59:59 2020 GMT
Subject:	commonName	Customer Example Inc.
	emailAddress	user@example.com
	organizationName	Customer Example Inc.
	street	18 Main Street
	locality	Springfield
	stateOrProvince	New Jersey
	postalCode	10100
	countryName	US
Subject Public Key Info:	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	

X509v3 Authority Key Identifier:	keyID: based on the subject key identifier in the issuer's certificate	
X509v3 Subject Key Identifier:	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)	
X509v3 Key Usage: critical	Digital Signature, Key Encipherment	
X509v3 Basic Constraints: critical	CA:FALSE	
X509v3 Extended Key Usage:	Document Signing, Client Authentication, Adobe Authentic Documents Trust, and up to one of Code Signing or Secure Email	
X509v3 Certificate Policies:	1.3.6.1.4.1.6449.1.2.1.6.6 , CPS: https://sectigo.com/CPS	
X509v3 CRL Distribution Points:	http://crl.sectigo.com/SectigoRSADocumentSigningCA.crl	
Authority Information Access:	CA Issuers - http://crt.sectigo.com/SectigoRSADocumentSigningCA.crt OCSP - http://ocsp.sectigo.com	
X509v3 Subject Alternative Name:	email: user@example.com	

E.g secureEmail certificate

Version:	3 (0x2)	
Serial Number:	containing at least 64 bits of output from a CSPRNG	
Signature Algorithm:	sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer:	commonName	Sectigo RSA Client Authentication and Secure Email CA
	organizationName	Sectigo Limited
	locality	Salford
	stateOrProvince	Greater Manchester
	countryName	GB
Validity:	Not Before:	Feb 19 00:00:00 2019 GMT
	Not After:	Feb 19 23:59:59 2020 GMT
Subject:	emailAddress	user@example.com
	commonName	Wendy Zheng
	organizationalUnit	Personal Authentication Enterprise

	organizationalUnit	IT Department
	organizationName	Customer Example Inc.
	street	18 Main Street
	locality	Springfield
	stateOrProvince	New Jersey
	postalCode	10100
	countryName	US
Subject Public Key Info:	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	
X509v3 Authority Key Identifier:	keyID: based on the subject key identifier in the issuer's certificate	
X509v3 Subject Key Identifier:	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)	
X509v3 Key Usage: critical	Digital Signature, Key Encipherment	
X509v3 Basic Constraints: critical	CA:FALSE	
X509v3 Extended Key Usage:	E-mail Protection,	
	TLS Web Client Authentication	
X509v3 Certificate Policies:	1.3.6.1.4.1.6449.1.2.1.1.1 , CPS: https://sectigo.com/CPS	
X509v3 CRL Distribution Points:	http://crl.sectigo.com/SectigoRSAClientAuthenticationandSecureEmailCA.crl	
Authority Information Access:	CA Issuers - http://crt.sectigo.com/SectigoRSAClientAuthenticationandSecureEmailCA.crt OCSP - http://ocsp.sectigo.com	
X509v3 Subject Alternative Name:	email: user@example.com	

Appendix D: Types of Sectigo Certificates

Sectigo TLS Secure Server Certificates

Trial SSL Certificate

InstantSSL Certificate

InstantSSL Pro Certificate

PremiumSSL Certificate

PremiumSSL Wildcard Certificate

PremiumSSL Legacy Certificate

PremiumSSL Legacy Wildcard Certificate

SGC SSL Certificate

SGC SSL Wildcard Certificate

EliteSSL Certificate

Enterprise SSL Certificate

Enterprise SSL Pro Certificate

Enterprise SSL Pro Wildcard Certificate

PlatinumSSL Legacy Certificate

PlatinumSSL Legacy Wildcard Certificate

PlatinumSSL SGC Certificate

PlatinumSSL SGC Wildcard Certificate

Unified Communications Certificate

Multi-Domain SSL Certificate

eScience TLS Server Certificate

LiteSSL e-commerce Certificate

LiteSSL e-commerce Wildcard Certificate

DV eScience TLS Server Certificate

COMODO AMT SSL Certificate

COMODO AMT SSL Wildcard Certificate

COMODO AMT SSL Multi-Domain Certificate

COMODO SSL Certificate

COMODO SSL Wildcard Certificate

COMODO SSL Unified Communications Certificate

PositiveSSL Trial Certificate

PositiveSSL Certificate

PositiveSSL Wildcard Certificate

PositiveSSL Multi-Domain Certificate

Free SSL Certificate

EssentialSSL Certificate

EssentialSSL Wildcard Certificate

OptimumSSL Trial Certificate

Optimum SSL Premium with DV Certificate

Optimum SSL Premium with DV Multi-Domain Certificate

Optimum SSL Premium Wildcard Certificate

Legacy Multi-Domain SSL Certificate

Free TLS Certificate

Educational Certificates and IGTF Certificates

Sectigo Client / Secure Email Certificates

Personal Secure Email Certificate

Corporate Secure Email Certificate

Custom Client Certificates

Sectigo Dual Use Certificates

Personal Authentication Certificates

Software Publishing Certificates

Code Signing Certificate

Legacy Code Signing Certificate

Time Stamping Certificate

Appendix E: ChangeLog

Version	Change Description	Date
5.0	Update all sections of document to rebrand as well as to bring up to date with BR and Mozilla policies	22-Feb-2019
5.1	Add and update EV requirements	19-Mar-2019
5.1.1	Add ChangeLog	23-Apr-2019
5.1.2	Additions related to Adobe Approved Trust List requirements	06-May-2019