Sectigo eIDAS Certification Practice Statement

Sectigo
Version 1.0.9
Effective: October 22, 2020
Rambla Catalunya, 86 3 1,
08008 Barcelona, Spain
www.sectigo.com

Copyright Notice

Sectigo
Rambla Catalunya, 86 3 1,
08008 Barcelona, Spain

SECTIGO

Contents

1. INTRODUCTION

Sectigo is a Trust Service Provider (TSP) that issues trusted digital certificates to entities including private and public companies and individuals in accordance with this Certification Practice Statement (CPS).

This document defines the different practices for the Sectigo Qualified PKI, which governs the issuance and management of qualified certificates.

In its role as a CA (Certification Authority), Sectigo performs functions associated with public key operations that include receiving requests, issuing, revoking and renewing digital certificates and the maintenance, issuance and publication of Certificate Revocation Lists (CRLs) for users within the Sectigo Public Key Infrastructure (PKI).

1.1. Overview

Sectigo follows the EU Regulation 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the European Single Market, repealing the directive 1999/93/EC from 13 December 1999, commonly named eIDAS.

For issuance of specific qualified secure server certificates for websites, also named QWACs, Sectigo also conforms to the current version of the CA/B Forum Baseline Requirements (BR) and EV Guidelines (EVG). 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 qualified 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.

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) for qualified certificates. It outlines the legal, commercial and technical principles and practices that Sectigo employ in providing certification services that include, but are not limited to, approving, issuing, using and managing of digital certificates and in maintaining a X.509 certificate based public key infrastructure (PKI) in accordance with the certificate policies determined by Sectigo. It also defines the underlying certification processes for subscribers and describes Sectigo's repository operations. This CPS is also a means of notification of roles and responsibilities for parties involved in certificate based practices within the Sectigo Qualified PKI.

This 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.

In order to individually identify each type of a qualified certificate issued by Sectigo in accordance with this Certification Practice Statement, an object identifier (OID) is assigned to each type.

They can be found in the profiles document available at *www.sectigo.com*.

Also according to the definition of ETSI EN 319 412-5, Sectigo includes some of the QcStatements identifiers.

1.3. PKI participants

This section identifies and describes some of the entities that participate within the Sectigo Qualified 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 Qualified PKI. See annex A to check out Sectigo Qualified PKI. Sectigo will:

- Conform its operations to this CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the repository,
- Issue and publish certificates in a timely manner in accordance with the issuance times set out in this CPS,
- Upon receipt of a valid request to revoke the certificate from a person authorized to request revocation using the revocation methods detailed in this CPS, revoke a certificate issued for use within the Sectigo Qualified 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 qualified 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, following the eIDAS regulation and ETSI standards for qualified certificates and seals and in additional documentation such the BR and the EVG for QWACs.
- 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 EVG and the ETSI standards and eIDAS regulation.

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. Upon successful approval to join the respective program may be permitted to act as an RA on behalf of Sectigo. RAs are required to conform to this CPS, the BR and the EVG and the eIDAS regulation.

RAs may only undertake their validation duties from pre-approved systems that 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 qualified certificates for which a Registration Authority has performed some part of the validation. Some of the intermediate CAs are dedicated to the work of a single RA, whilst others are dedicated to the work of multiple related RAs.

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 QWACs this RA is also equipped with automated systems that validate domain control. For that minority of QWACs 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 audit requirements.

1.3.2.2. External Registration Authority

Some resellers or enterprise customers may be authorized by Sectigo to act as external RAs. As such they may be granted RA functionality which may include the validation of some or all of the subject identity information. The external RA is obliged to conduct validation in accordance with this CPS, the CAB Forum´s BRs and the EVG and the ETSI standards and eIDAS regulation 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 or via any other method that proves the identity of the applicant/subscriber.

External RAs do not validate domain control for QWACs. Sectigo's internal RA as described in this CPS always performs this element of the validation of QWACs.

1.3.3. Subscribers (End Entities)

Subscribers of Sectigo services are natural or legal persons 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.

See Annex B for additional information on the different qualified certificates issued by Sectigo

1.3.4. Relying Parties

Relying Parties use PKI services in relation with various Sectigo qualified 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.

To verify the validity of a qualified 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.

Furthermore, all qualified certificates shall be checked against the correspondent TSL.

1.3.5. Other participants

Sectigo has several categories of partner, which assist in the provision of certification services, such as reseller partners and Web Host resellers. All these partners help in sales services but are not related to the lifecycle of the certificates.

1.3.5.1. Reseller partners

Sectigo operates a reseller partner network that allows authorized partners to integrate Sectigo qualified certificates into their own product portfolios. Reseller partners are responsible for referring 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 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 qualified certificates, usually QWACs, on behalf of their hosted customers.

All Web Host resellers are required to provide proof of organizational status and must enter into a Sectigo Web Host reseller agreement prior to being provided with Web Host reseller facilities.

1.4. Certificate usage

A digital Certificate is formatted data that cryptographically binds an identified Subscriber with a Public Key. A digital Certificate allows a natural or legal person taking part in an electronic transaction to prove its identity to other participants in such transaction.

Sectigo currently offers a portfolio of digital certificates, with the consideration of qualified, 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/natural, 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 qualified certificate types. The different qualified certificate types have differing intended usages and differing policies. Pricing and Subscriber fees for these 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 qualified 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. QWACs

Usually, QWACs, 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.

The eIDAS regulation defines the EU qualified website certificates used in support of websites authentication. These certificates can be issued to natural and legal persons. When this type of certificate is issued to a legal person all requirements of EV certificates are incorporated plus additional provisions as specified in eIDAS. Also can be issued to legal persons according to the EU payment services directive 2015/2366, named PSD2.

QWACs may contain multiple FQDNs or IP addresses in the subjectAlternativeName field.

1.4.1.2. Qualified certificates for electronic signatures/seals

These certificates are issued in accordance to the eIDAS regulation offering the level of qualified as per the regulation. These certificates can be issued to natural person to be used for signing or can be issued to legal persons to be used for sealing. Depending on the device used, QSCDs or not, for these actions, the signature or the seal can be qualified or not.

As indicated in 1.4.1.1 there´s a specific type of qualified certificates for website authentication, commonly named QWAC.

Seals can be also issued to entities according to the EU payment services directive 2015/2366

1.4.2. Prohibited certificate uses

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

1.5. Policy administration

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

1.5.1. Organization administering the document

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

The Policy Authority (PA):

- Establishes and maintains this CPS.

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

1.5.2. Contact person

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

Sectigo 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
URL: *https://www.sectigo.com*
Email: *legalnotices@sectigo.com*

To report abuse, fraudulent, or malicious use of qualified certificates issued by Sectigo, please send email to *qcabuse@sectigo.com*

Sectigo also operates an automated revocation portal at https://secure.sectigo.com/products/RevocationPortal where Subscribers/Domain owners may revoke their certificates, or the public may report and revoke certificates for which the private key has been compromised.

1.5.3. Person determining CPS suitability for the policy

The Sectigo Policy Authority is responsible for determining the suitability of certificate policies illustrated within this CPS. The Sectigo Policy Authority is also responsible for determining the suitability of proposed changes to this 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 Policy Authority as specified in the *Sectigo Policy Authority (PA) Membership and Procedures* document.

1.6. Definitions and Acronyms

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

1.6.1. Acronyms

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

Acronym	Full Name
BR	Baseline Requirements
CA	Certification Authority
CAB	Conformity Assessment Body
CA/B	Certificate Authority/Browser (Forum)
CMS	Certificate Management System
CP	Certificate Policy
PA	Policy Authority
CPS	Certification Practice Statement
CRL(s)	Certificate Revocation List(s)
CSR	Certificate Signing Request
CT	Certificate Transparency
DBA	Doing Business As
DN	Distinguished Name
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
eIDAS	electronic IDentification, Authentication and trust Services
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications and Standards Institute
EV	Extended Validation
EVG	EV Guidelines
FIPS PUB	Federal Information Processing Standards Publication

FQDN	fully qualified domain name
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
LDAP	Lightweight Directory Access Protocol
LRA	Local RA
MDC	Multiple Domain Certificate
NIST	National Institute for Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
PSD2	Payment Services Directive 2
QSCD	Qualified Signature/Seal Creation Device
QTSP	Qualified Trust Service Provider
QWAC	Qualified Website Authentication Certificate

RA(s)	Registration Authority(ies)
RFC	Request for Comments
RSA	Rivest Shamir Adleman
SAN	Subject Alternative Name
SHA	Secure Hash Algorithm
SB	Supervisory Body
S/MIME	Secure/Multipurpose Internet Mail Extension(s)
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TSA	Time Stamping Authority
TSL	Trusted Services List
TSP	Trust Service Provider
UTC	Coordinated Universal Time
URL	Uniform Resource Locator

1.6.2. Definitions

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

Term	Definition
Advance electronic signature	means an electronic signature which meets the requirements set out in Article 26 of the eIDAS regulation
Advance electronic seal	means an electronic seal, which meets the requirements set out in Article 36 of the eIDAS regulation
Applicant	Means the natural or legal person 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 natural or legal person 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 CAB stating the CAB's opinion on whether a TSP's processes and controls comply with the mandatory provisions of the eIDAS regulation and ETSI standards.
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	public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it
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; 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.
Certificate Transparency	Means the protocol described in RFC 6962 for publicly logging the existence of Transport Layer Security (TLS) certificates as they are issued or observed.
Certification Authority	Authority trusted by one or more users to create and assign certificates. A CA can be: 1) a trust service provider that creates and assigns public key certificates; or 2) a technical certificate generation service that is used by a certification service provider that creates and assign public key certificates.
Conformity Assessment Body	body that performs conformity assessment services which is accredited as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides
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 natural or legal person(s) registered with a Domain Name Registrar as having the right to control how a

	Domain Name is used, such as the natural or legal person 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 natural or legal person 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).
Electronic signature	means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
Electronic seal	means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;
ETSI Standards	mean, individually or collectively, the documents developed by the Technical Committee ESI of ETSI with requirements applicable to a Certificate.
EU Payment Services Directive 2015/2366	This directive provides the legal foundation for the further development of a better integrated internal market for electronic payments within the EU. It also provides the necessary legal platform for the Single Euro Payments Area (SEPA). It repeals 2007/64/EC directive.
EU Regulation 910/2014	This regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted on 23 July 2014 provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. This regulation simplifies and standardises the systems for electronic interactions all over Europe to help create a "unique digital market"
EU Regulation 2016/679	This regulation on protection of natural persons with regard to the processing of personal data and of the free movement of such data (GDPR) provides a regulatory environment to protect fundamental rights and freedoms of natural persons for the protection of their personal data.

EV Guidelines (EVG)	CA/Browser Forum *Guidelines for the Issuance and Management of Extended Validation 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.
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 Person	Means an association, corporation, partnership, proprietorship, trust, government entity, or other entity with legal standing in a country's legal system.
Object Identifier	Refers to the unique identification numbers organized hierarchically, which particularly enable referencing the conditions applicable to the trust service provided.
Precertificate	Means a certificate that is constructed from the certificate to be issued by adding a special critical poison extension for the purpose of submission to a CT log in accordance with RFC 6962
Privacy Policy	Means the latest version of Sectigo's published document titled as such, which describes Sectigo's policies and practices in collecting, using, and safeguarding personal information, and which is accessible at the following website: *https://www.sectigo.com/privacy-policy/*.
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.

Qualified certificate	Under the context of Regulation (EU) 910/2014 (eIDAS), means a certificate that meets the requirements set in this regulation
Qualified certificate for electronic signature	Under the context of Regulation (EU) 910/2014 (eIDAS), means a certificate for an electronic signature issued by a qualified trust service provider
Qualified certificate for electronic seal	Under the context of Regulation (EU) 910/2014 (eIDAS), means a certificate for an electronic seal issued by a qualified trust service provider
Qualified electronic seal	means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;
Qualified electronic signature	means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;
Qualified electronic Signature/Seal Creation Device (QSCD)	Under the context of Regulation (EU) 910/2014 (eIDAS), means an electronic signature or seal creation device that meets the requirements as stipulated in the Annex II of the eIDAS Regulation.
Qualified Trust Service Provider (QTSP)	A natural or legal person that is recognized by a European Union member state national supervisory body to provide (a subset of) qualified trust services as defined within the eIDAS Regulation.
Qualified Website Authentication Certificate (QWAC)	Under the context of Regulation (EU) 910/2014 (eIDAS), means a certificate for identification a website issued by a qualified trust service provider. This certificate creates a secure link between a website and a browser. By ensuring that all data passed between the two remains private and secure
Random Value	Means a value specified by Sectigo to the applicant that exhibits at least 112 bits of entropy.
Registration Authority	Entity that is responsible for identification and authentication of subjects of certificates mainly. An RA can assist in the certificate application process or revocation process or both.

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 Policy Authority	Means the entity charged with the maintenance and publication of the policy and practice statements.
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.
Subject	entity identified in a certificate as the holder of the private key associated with the public key given in the certificate
Subscriber	legal or natural person bound by agreement with a trust service provider to any subscriber obligations
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.
Supervisory Body	A body responsible for supervisory tasks in the designating EU member state as defined in eIDAS article 17

Trust Service	electronic service for: • creation, verification, and validation of digital signatures and related certificates; • creation, verification, and validation of time-stamps and related certificates; • registered delivery and related certificates; • creation, verification and validation of certificates for website authentication; or • preservation of digital signatures or certificates related to those services.
Trust Service Provider	entity which provides one or more trust services
Verified Method of Communication	Method of communication as defined and verified in conformance with Section 11.5 of the EVG
X.509	Means the ITU-T standard for certificates and their corresponding authentication framework

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

Sectigo publishes this CPS, the terms and conditions, the Relying Party Agreement and copies of all Subscriber Agreements in the Repository. The Sectigo Policy Authority maintains the Sectigo Repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in section 5.4 of this 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
  Rambla Catalunya, 86 3 1,
  08008 Barcelona, Spain

In addition to the repository, Sectigo hosts test web pages for QWACs that allow third party Application Software Suppliers to test their software which chain up to Sectigo's Root certificates. Sectigo also includes in the repository test certificates for signatures and seals.

2.3. Time or frequency of publication

Issuance and revocation information regarding certificates will be published as soon as possible. Updated or modified versions of Subscriber Agreements and Relying Party Agreements are usually published within seven days after approval. This 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 4.9.6 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 qualified certificate types. Prior to the issuance of a qualified 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 Qualified 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.

For QWACs in general include entries in the subjectAlternateName (SAN) extension which are intended to be relied upon by relying parties, e.g., browsers.

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.

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 re-assign a subject distinguishName that has been used in a certificate to another subject.

Sectigo includes in the subject serial number field the semantics identifiers as per ETSI EN 319 412-1 for natural person certificates and the organizationIdentifier for legal persons.

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. Sectigo has a separate uniqueness check that verifies that certificate serial numbers are never re-used.

3.1.6. Recognition, authentication and role of trademarks

Subscribers and applicants may not request certificates with content that infringes the intellectual property rights of another entity. Unless otherwise specifically stated in this 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

Sectigo performs the identification and authentication of the applicants using any legal means of communication or investigation to validate the identity of these natural or legal persons. Procedures as well as descriptions of fields are described below for each type of certificate issued.

Sectigo does not issue certificates for itself except those needed for the correct management of the services provided.

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. Authentication of a natural person identity

The purpose of these EU Qualified Certificates are to identify the subscriber with a high level of assurance, for the purpose of:

- Creating Qualified Electronic Signatures meeting the qualification requirements defined by the eIDAS Regulation. These certificates use a QSCD for the protection of the private key. These certificates meet the relevant ETSI "Policy for EU Qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD" (QCP-n-qscd).
- Creating Advanced Electronic Signatures meeting the qualification requirements defined by the eIDAS Regulation. These certificates do not use a QSCD for the protection of the private key. These certificates meet the relevant ETSI "Policy for EU qualified certificate issued to a natural person" (QCP-n).

The content of these certificates meet the relevant requirements of:

- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements

3.2.1.1. Identity verification process

Identity validation procedures for these certificates meet the relevant requirements of ETSI EN 319 411-2.

Sectigo recommends that QCP-n-qcsd and QCP-n certificates are used only for electronic signatures.

The identity of the natural person and, if applicable, any specific attributes of the person, shall be verified:

- by the physical presence of the natural person; or
- using methods which provide equivalent assurance in terms of reliability to the physical presence and for which Sectigo can prove the equivalence. The proof of equivalence can be done according to the eIDAS Regulation.

Evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a nationally recognised identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

Evidence may be provided on behalf of the subject by the RA. However, the subject remains responsible for the content of the certificate.

If the subscriber is a physical person who is identified in association with an organizational entity, legal person, additional evidence shall be provided of:

- Full name and legal status of the associated organizational entity;
- Any relevant existing registration information (e.g. company registration) of the organisational entity; and
- Evidence that the subscriber is associated with the organisational entity.

The certificates that require a QSCD meet the requirements laid down in Annex II of the eIDAS Regulation.

The subscriber's obligations (or respectively the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or respectively is used) under the subject's sole control.

3.2.2. Authentication of a legal person identity

The purpose of these EU Qualified Certificates are to identify the subscriber with a high level of assurance, for the purpose of:

- Creating Qualified Electronic Seals meeting the qualification requirements defined by the eIDAS Regulation. These certificates use a QSCD for the protection of the private

key. These certificates meet the relevant ETSI “Policy for EU Qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD” (QCP-l-qscd).
- Creating Advanced Electronic Seals meeting the qualification requirements defined by the eIDAS Regulation. These certificates meet the relevant ETSI “Policy for EU Qualified certificate issued to a legal person” (QCP-l).

The content of these certificates meet the relevant requirements of:

- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-3: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements
- ETSI TS 119 495: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366 for PSD2 certificates type

3.2.2.1. Identity verification process

Identity validation procedures for these certificates meet the relevant requirements of ETSI EN 319 411-2.

Sectigo recommends that QCP-l-qcsd and QCP-l certificates are used only for electronic seals.

The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:

- by the physical presence by an authorised representative of the legal person; or
- using methods which provide equivalent assurance in terms of reliability to the physical presence and for which Sectigo can prove the equivalence. The proof of equivalence can be done according to the eIDAS Regulation.

Evidence shall be provided of:

- Full name of the legal person consistent with the national or other applicable identification practices; and
- When applicable, the association between the legal person and the other organisational entity identified in association with this legal person that would appear in the organisation attribute of the certificate, consistent with the national or other applicable identification practices.

For the authorized representative of the legal person, evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a nationally recognised identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

The certificates that require a QSCD meet the requirements laid down in Annex II of the eIDAS Regulation.

The subscriber's obligations (or respectively the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or respectively is used) under the subject's sole control.

3.2.3. QWACs

QWACs certificates can be issued either to natural or legal persons.

The purpose of these EU Qualified Certificates are to identify the subscriber with a high level of assurance of a website, meeting the qualification requirements defined by the eIDAS Regulation.

These certificates meet the relevant ETSI “Policy for EU Qualified certificate issued to natural or legal person websites” (QCP-w).

The content of these Certificates meet the relevant requirements of:

- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-4: Certificate Profiles; Part 4: Certificate profile for web site certificates
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements

Identity validation procedures for these certificates meet the relevant requirements of ETSI EN 319 411-2 for “Policy for EU qualified certificate issued to natural or legal person websites” (QCP-w) and CA/B Forum EV guidelines, which is specifically for legal persons.

3.2.3.1. Identity verification process

Sectigo ensures that all information to be included in the QWAC 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) in the case of QWACs issued to legal persons and the ETSI EN 319 411-2.

Independently of the natural or legal person identification process, Sectigo shall verify the content of every domain name or IP address included in a Qualified Website Authentication Certificate.

3.2.3.1.1. Domain verification

For each domain name to be included in a QWAC, Sectigo verifies the applicant's control of the domain name in accordance with the CAB Forum 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).

3.2.3.1.2. IP address verification

For each IP Address to be included in a QWAC, Sectigo verifies the applicant's control of the IP in accordance with the CAB Forum Baseline Requirements, section 3.2.2.5, using one of the following methods for each IP

1. Confirming the applicant's control over the requested IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of validating control of IP Addresses, on the IP Address that is accessible by the CA via HTTP/HTTPS over an Authorized Port. The Request Token or Random Value shall not appear in the request. (In accordance with BR 3.2.2.5.1).

2. Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value shall be sent to an email address, fax/SMS number, or postal mail address identified as an IP Address Contact. The Random Value is unique in each email, fax, SMS, or postal mail. The Random Value remains valid for use in a confirming response for no more than 30 days from its creation. (In accordance with BR 3.2.2.5.2).

3. Confirming the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under Section 3.2.2.1.1 above. (In accordance with BR 3.2.2.5.3).

3.2.4. PSD2

PSD2 certificates are legal person certificates that can be issued as QWACs or as Seals and when in Seals, these can be issued in QSCDs or not.

These certificates meet the relevant ETSI "Policy for EU Qualified certificate issued to legal persons" (QCP-l-qscd), (QCP-l), (QCP-w), (QCP-w-psd2).

3.2.4.1. Identity verification process

Additional steps to verify PSD2 specific attributes including name of the National Competent Authority (NCA), the PSD2 Authorisation Number or other recognized identifier, and PSD2 roles.

These details are provided by the Certificate Applicant and confirmed by Sectigo using authentic information from the NCA (e.g, using a national public register, EBA PSD2 Register, EBA Credit Institution Register or authenticated letter).

Sectigo also confirms the PSD2 role(s) of the Certificate Applicant (RolesOfPSP) in accordance with the rules for validation provided by the NCA, if applicable:

- account servicing (PSP_AS) OID: id-psd2-role-psp-as { 0.4.0.19495.1.1 }
- payment initiation (PSP_PI) OID: id-psd2-role-psp-pi { 0.4.0.19495.1.2 }
- account information (PSP_AI) OID: id-psd2-role-psp-ai { 0.4.0.19495.1.3 }
- issuing of card-based payment instruments (PSP_IC) OID: id-psd2-role-psp-ic { 0.4.0.19495.1.4 }

The certificates that require a QSCD meet the requirements laid down in Annex II of the eIDAS Regulation.

The subscriber's obligations (or respectively the obligations on the TSP managing the key on their behalf) require that the Private Key is maintained (or respectively is used) under the subject's sole control.

3.2.5. Method to prove possession of Private Key

When Sectigo does not generate the private key (i.e., QWACs), 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).

Verification of a digital signature is used to determine that:

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

3.2.6. Validation of authority

Validation of authority involves a determination of whether a natural person has specific rights, entitlements, or permissions, including the permission to act on behalf of a legal person to obtain a certificate. Validation of authority is dependent on the type of certificate requested and is performed in accordance with section 3.2 of this CPS.

For legal person certificates, Sectigo shall use a reliable method of communication to verify the authenticity of the applicant representative's certificate request.

Sectigo may establish the authenticity of the certificate request directly with the applicant representative, the natural person authorized representative of the legal person, or with an authoritative source within the applicant's organization.

In addition, Sectigo shall establish a process that allows an applicant to specify the natural persons who may request certificates. If an applicant specifies, in writing, the natural persons 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.

Specifically for QWACs, authorization by the Domain Name Registrant is verified as documented in section 3.2.3.1 of this CPS and this request is verified in accordance with the *CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates* section 11.5.

3.2.7. Criteria for interoperation

Sectigo may provide services allowing for another TSP 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 TSPs; the terms and criteria of which are to be set forth in the applicable agreement.

3.2.8. Application validation

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

3.3. Identification and authentication for re-key requests

Sectigo supports rekeys on:

- Replacement, which is when a subscriber wishes to change some (or none) of the subject details in an already issued certificate and may (or may not) also wish to change the key associated with the new certificate; and

- Renewal, which is when a subscriber wishes to extend the lifetime of a certificate which has been issued they may at the same time vary some (or none) of the subject details and may also change the key associated with the certificate.

In both cases, Sectigo requires the subscriber to use the same authentication details 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 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 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:

Either the subscriber must be in possession of the authentication details which were used to purchase the certificate originally or the subscriber must be able to send an 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 qualified certificates varies dependent on the certificate type. Sectigo reserves the right to, at its discretion, issue certificates that may fall outside of these set periods.

The following steps describe the main milestones to issue a 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) in case of QWACs or those not issued within a QSCD, e-mail address if needed, common name, organizational information, country code, identity verification method, billing information, etc.
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 identifies the applicant either a natural or legal person who is going to be the subject certificate and 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:

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

Via email: Sectigo may at its discretion, accept applications via email.

RAs: Sectigo may grant some RAs to accept applications at its discretion

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.

The applicant, a representative or an RA on behalf of the subscriber shall submit a subscriber certificate application to the CA.

Under special circumstances, the applicant may submit an application via email; however, this process is available at the discretion of Sectigo or its RAs.

4.1.1.1. 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) in the case of QWACs or those not issued within a token. For those issued in devices, key pairs are generated by Sectigo and later deliver securely that device to the applicant, with the difference of the HSMs in where there´s no such specific delivery.
- 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 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
Qualified certificate for natural person	End user or entity subscriber	Sectigo or entity subscriber	Sectigo
Qualified certificate for legal person	Entity subscriber	Sectigo	Sectigo
Qualified certificate for websites	End user or entity subscriber	Sectigo	Sectigo

4.2.1. Performing identification and authentication functions

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

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

Sectigo may use the services of a third party to confirm the information of a natural or legal person that applies for a qualified 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 a natural or legal person applicant. Sectigo reserves right of refusal in its absolute discretion.

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

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 period. The period 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 (for QWACs only)

Where an application is for a QWAC, 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 Sectigo recognizes 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 qualified certificate is deemed to be valid at the moment a Subscriber accepts it (refer to section 4.4 of this CPS). Issuing a qualified certificate means that Sectigo accepts a certificate application.

Sectigo qualified certificates are issued to organizations (legal persons) or individuals (natural persons).

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.

The only certificates Sectigo issues from its root CAs are intermediate CA certificates and cross certificates. Our CA has no facility for the automated signature of such certificates, so this activity necessarily involves manual intervention by privileged users to sign such certificates. Certificate issuance by the Root CA requires an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.2. Notification to subscriber by the CA of issuance of certificate

Sectigo notifies subscriber of the issuance of a qualified certificate either via email and/or through delivery. Delivery of subscriber certificates to the associated subscriber is dependent on who generates the key pairs and device used:

Qualified certificates for natural and legal person issued within a device (QSCD or not QSCD)

> Notification of issuance of these certificates are delivered via email to the Subscriber using the administrator contact email address provided during the application process. The certificate will be delivered to the subscriber using a reliable and secure method, usually by a courier.

Qualified certificates for natural and legal person not issued within a device

> Upon issuance of these qualified 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. Another option is to deliver the certificate directly via email to the subscriber using the administrator contact email address provided during the application process.

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:

- by Sectigo making the certificate available in the Repository; and
- 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

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

4.4.3.1. Web Host reseller partner

Issued Subscriber QWACs 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.

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 advanced/qualified signature/seal is exclusively that of the Relying Party. Reliance on a qualified/advanced signature/seal should only occur if:

- the signature/seal 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 has checked against the correspondent TSL.
- the Relying Party understands that a qualified certificate is issued to a subscriber for a specific purpose and that the qualified certificate may only be used in accordance with the usages suggested in this 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 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 but checking that the cryptographic material is still sufficient for the new certificate and that there´s no indications that the subject´s private key has been compromised nor the certificate has been revoked due to a security breach.

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 re-key

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

4.7.1. Circumstances for certificate re-key

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

4.7.2. Who may request certificate re-key

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 re-key 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 re-key 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.

4.9. 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 as indicated in section 4.9.7. Sectigo informs certificate subject or subscribers of the change of status of the certificate.

Sectigo does not utilize certificate suspension.

4.9.1. Circumstances for revocation

Sectigo shall revoke a certificate within 24 hours of receiving the revoking request 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;
- The Subscriber or Sectigo has breached a material obligation under this CPS or the relevant Subscriber Agreement;
- 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 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
- 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 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 *qcabuse@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 natural or legal person that has made the certificate application.
- Made by the RA on behalf of the natural or legal person 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. Time within which Sectigo will process the revocation request

Sectigo shall process revocation requests in accordance with this CPS. Once a certificate has been revoked the revocation will be reflected in the OCSP responses issued within 1 hour, and in the CRLs within 6 hours.

4.9.5. Revocation checking requirement for relying parties

Parties relying on a qualified 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 shows 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.

4.9.6. CRL issuance frequency

For the status of Subscriber certificates:

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 by default or within 6 hours if a certificate has been revoked. All expired CRLs are archived (as described in section 3.4 of this CPS) for a period of 15 years or longer if applicable. For revoked qualified certificates, Sectigo will maintain certificate information on CRLs for at least 20 years.

For the status of CA certificates:

Sectigo shall update and reissue CRLs at least:

- once every twelve months
- within 24 hours after revoking a CA certificate, and the value of the nextUpdate field must not be more than twelve months beyond the value of the thisUpdate field
- within 24 hours after expiration of a CA certificate
- every 30 days if Sectigo cross-certifies this hierarchy with a third party TSP

4.9.7. 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.

4.9.8. 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.

4.9.9. 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.

For the status of Subscriber certificates:

Sectigo shall update this information provided via OCSP at least every four days. OCSP responses from this service must have a maximum expiration time of ten days.

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder does not respond with a "good" status. The TSP monitors the responder for such requests as part of its security response procedures.

For the status of Subordinate CA certificates:

Sectigo shall update this information provided via an Online Certificate Status Protocol at least:

- every twelve months
- within 24 hours after revoking a Subordinate CA certificate.
- within 24 hours after expiration of a CA certificate

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

4.10. Certificate status services

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

Revocation status information is available beyond the validity period of the certificate

4.10.1. Operational characteristics

Lightweight OCSP conforms to RFC 5019. Sectigo provides revocation information for qualified certificates past the expiry date.

4.10.2. Service availability

Certificate status services are available 24/7.

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 provide key escrow or key backup services.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

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

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

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 worldwide, with separate operations, research & development and server operation sites. Physical barriers are used to segregate secure areas within buildings and are constructed 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 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 and assign permissions on the “principle of least privilege” basis through a formal authorization process 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 Qualified 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

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.

There´s a specific role for QWACs when acting as validation specialist as indicated in the BRs

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.

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.

5.3. 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 qualified 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 or alike 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. 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.

5.3.6. 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.

5.3.7. 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 eIDAS regulation, the CA/B Forum Baseline Requirements, EV Guidelines 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
- QSCDs (e.g., HSMs or USB tokens) events, such as usage, de-installation, service or repair and retirement
- Successful and unsuccessful Sectigo Qualified 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

The system administrator archive logs and event journals reviewed by CA management on a weekly basis.

5.4.3. Retention period for audit log

Audit logs shall be retained for a minimum of 7 years. 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.

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. 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 automatically 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 archives 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 all documentation relating to certificate requests and the verification thereof, and all certificates and revocation thereof for a term of not less than 15 years after any certificate based on that documentation ceases to be valid, or as necessary to comply with applicable laws. The retention term begins on the date of expiration or revocation. Copies of certificates are held, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that Sectigo may see fit.

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

5.5.3. Protection of archive

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

5.5.4. Archive backup procedures

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
- Certificate revocation
- All logs

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 external RAs are required to submit appropriate documentation as detailed in the Web Host Reseller 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.

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. CA 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. Algorithm compromise procedures

Cryptographic algorithms are exposed to attacks and therefore remain insufficient for its intended usage. Sectigo uses suitable algorithms which are up to date. Sectigo does not use any algorithm which is not considered suitable for its usage according to the different industry standards and best practices.

For subscribers that request certificates to Sectigo using a CSR, Sectigo checks the algorithm used by the subscriber and reject the request if this is not according to the standards nor suitable.

5.7.5. 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. TSP termination

In case of termination of TSP 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 TSP 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 TSP.
- 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 TSP 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.

In the event that Sectigo decides to transfer the activity to another TSP, it will notify the Supervisory Body and the subscriber of its certificates of the transfer agreements. To this end, Sectigo will send the document explaining the transfer conditions as well as the conditions of use that will regulate the relations between the subscriber and the TSP to which the certificates are transferred.

The subscriber must expressly consent to the transfer of the certificates, accepting the conditions of the TSP to which they are transferred. After the period of 90 days, without a transfer agreement or without the subscriber expressly accepting it, the certificates will be revoked.

When another Sectigo cross certified TSP stops all operations, including handling revocation, all cross certificates to that TSP shall be revoked following the conditions and requirements set above.

These requirements may be varied by contract, to the extent that such modifications affect only the contracting parties.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair generation and installation

6.1.1. Key Pair generation

6.1.1.1. Subscriber Key Pairs

There are two options for the generation of the subscriber key pairs:

- Generated by the subscriber
- Generated by Sectigo

In general, subscriber is solely responsible for the generation of an asymmetric cryptographic key pair (RSA or ECDSA) appropriate to the certificate type being applied for, usually those not issued within QSCDs and not in the cloud. 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.

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

Other 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.

Qualified certificates providing qualified signatures or seals respectively shall be issued in QSCDs. 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. Sectigo checks that the device is a QSCD before using it
- The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate or manufacturers key indicating that the subscriber key is managed in a suitable hardware module,
- The Subscriber provides a suitable IT audit indicating that its operating environment achieves a level of security at least equivalent to that of FIPS 140-2 level 2 or being listed as a QSCD for qualified certificates.

Where the Subscriber is generating, managing and/or storing keys in a Cloud (e.g. Azure) HSM the subscriber must provide sufficient evidence to prove that all end entity key pairs have:

a) been generated

   1. using a trustworthy system, taking all reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key, and then securely transferred into a Cloud (e.g. Azure) HSM; or

   2. directly generated by and stored in a Cloud (e.g. Azure) HSM.

b) been stored in a Cloud (e.g. Azure) HSM.

6.1.1.2. CA and subCA Key Pairs

For Root CA Key Pairs created under this CPS Sectigo:

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

Sectigo's CA keys are generated in Hardware Security Modules (HSM)s that are compliant, as a minimum, to FIPS 140-2 level 3, be certified according to ISO/IEC 15408 or listed as QSCDs. CA keys are never available outside the HSM or key ceremonies in plain text form. All CA key operations are performed within the security of the HSM, whether this be the initial key generation or their end use in the live production environment. All keys that are exported from the HSM are encrypted with a suitable encryption algorithm with the encryption key generated by the HSM.

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

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

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

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

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

6.1.2. Private Key delivery to subscriber

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 QWACs nor for other qualified certificates where keys are generated on subscriber´s software

Where key pairs for qualified certificates are generated by Sectigo, Sectigo authorized personnel will deliver the FIPS140-2, ISO 15408 or QSCD certified crypto module device and 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

QWACs 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.

Qualified certificates, not issued within devices, requests generated using the subscriber´s cryptographic service provider software, are 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 subscriber´s 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

Root certificates and any certificates which chain up to them have:

- RSA keys whose modulus size in bits is divisible by 8, and is at least 2048; or

- ECDSA keys on the P-256 or P-384 curves.

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 or ISO/IEC 15408 certified HSM.

Sectigo follows ETSI TS 119 312 and NIST SP 800-89 for RSA or NIST SP 800-56A for ECC

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

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

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

1. Digital signature, for verifying digital signatures that is, for entity authentication and data origin authentication with integrity
2. Non-repudiation, for verifying digital signatures used in providing a nonrepudiation service which protects against the signing entity falsely denying some action
3. Key encipherment, for enciphering keys or other security information, e.g. for key transport
4. Data encipherment, for enciphering user data, but not keys or other security information 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 does not indicate that Sectigo does or will issue a certificate with that key usage.

Private Keys corresponding to Root certificates shall not be used to sign certificates except in the following cases:

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

6.2. Private Key protection and cryptographic module engineering controls

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

6.2.1. Cryptographic module standards and controls

Sectigo securely generates and protects its own Private Key(s), using a trustworthy system and takes necessary precautions to prevent the compromise or unauthorized usage of it. Such system shall be certified at least to FIPS 140-2 Level 3 or ISO/IEC 15408.

The Sectigo Root keys are 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 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.

6.2.3. Private Key storage on cryptographic module

Private Keys are generated and stored inside Sectigo's Hardware Security Modules (HSMs). HSMs shall be certified to at least FIPS 140-2 Level 3 or ISO/IEC 15408.

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

6.2.4. 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.

6.2.5. 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.

6.2.6. Method of destroying Private Key

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

6.2.7. 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, 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 subscriber certificate validity period will be from 1 to 5 years, however, Sectigo reserves the right to offer validity periods outside of this standard validity period.

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

- Root CA certificates MAY have a validity period of up to 25 years
- Sub-CA certificates MAY have a validity period of up to 15 years

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

When a CA certificate is about to expire, Sectigo generates a new CA certificate with new keys time in advance to cover the longest validity time of the end entity certificates issued by that CA.

6.4. Activation data

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

6.4.1. Activation data generation and installation

Activation data is generated in accordance with the specifications of the HSM.

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.

6.5. 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.

6.6. Lifecycle technical controls

6.6.1. System development controls

Sectigo has formal policies in place to control, document and monitor the development of its PKI 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. Sectigo develops the majority of changes in-house. 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.

Sectigo performs internal audits quarterly to verify and check that all systems are secured and configured properly.

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 three Time-Stamping Authorities (TSA).

Sectigo synchronizes all TSP components with a time service provided by several services through NTP (Network Time Protocol) Service. Time derived from this time service is used for establishing the time of:

- Initial validity type of a certificate;
- Revocation of a certificate;
- Posting of CRL updates; and
- OCSP responses.

The Sectigo TSAs are intended for use when need to provide accurate time to document signed or sealed and to give the integrity needed for this.

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

Sectigo also offers a RFC3161 TSA, whose URL is:

http://timestamp.sectigo.com/rfc3161

Sectigo qualified TSA is at:

http://timestamp.sectigo.com/qualified

7. CERTIFICATE, CRL, AND OCSP PROFILES

Sectigo uses version 3 of the X.509 standard to construct qualified certificates for use within the Sectigo Qualified 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. X.509v3 is a standard of the International Telecommunications Union for digital certificates. Sectigo also uses different ETSI standards, such EN 319 412 part 1 to 5 for additional extensions and ETSI TS 119 495 for those specific to the PSD2, the Payment Service Directive

7.1. Certificate profile

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

- Terms and conditions.
- 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:

  - 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.
- qcStatements indicating specifities of the qualified certificates as stated in ETSI certificates profiles standards.

- QWACs additionally have:
  - Applicant's fully qualified domain name(s).

7.1.1. Version number(s)

Certificate versions are all X.509 version 3. The certificate version number shall be set to the integer value of "2" for version 3 certificates.

7.1.2. Certificate extensions

Certificate extensions are in conformance to RFC 5280 as a general rule.

For Qualified certificates, ETSI standards require additional extensions that Sectigo´s certificates shall conform.

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

- a non-critical authorityInformationAccess extension containing the HTTP URL of the Issuing CA's OCSP responder and containing the HTTP URL of the Issuing CA's certificate.
- a basicConstraints extension marked critical. The cA field is set true. The pathLenConstraint is often present and the pathLenConstraint is usually set to 0.
- 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.
- a non-critical authorityInformationAccess extension containing the HTTP URL of the Issuing CA's OCSP responder and containing the HTTP URL of the Issuing CA's certificate.
- a basicConstraints extension marked critical. The cA field is not set.
- a keyUsage extension marked critical. Bit positions for keyCertSign and cRLSign are NOT set.

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

For additional information, check out certificate profiles document.

7.1.2.4. All certificates

All other fields and extensions are in accordance with RFC5280 and ETSI EN 319 412 part 1 to 5 and ETSI TS 119 495 specifically for PSD2 certificates.

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:

- such value falls within an OID arc for which the applicant demonstrates ownership, or
- 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

7.1.2.5. Application of RFC 5280

Only for QWACs, as well as for all other SSL/TLS certificate types, and for purposes of clarification, a Precertificate, as described in RFC 6962 – Certificate Transparency, shall not be considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure certificate and Certificate Revocation List (CRL) Profile under this CPS.

7.1.3. Algorithm Object Identifiers

Sectigo certificates are signed using algorithms including but not limited to RSA and ECDSA.

Sectigo certificates are signed using algorithms with these identifiers:

From RFC3279:

(not used for qualified certificates 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 this CPS to verify that, as of the certificate's issuance date, all of the subject information was accurate.

For additional information, check out certificate profiles document.

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.

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

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.

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.

7.1.6. Certificate Policy Object Identifier

Sectigo uses policy OIDs under the arcs:

iso(1)
identified-organization(3)
dod(6)

internet(1)
private(4)
enterprise(1)
6449
certificates(1)
policies(2),

and:

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

and:

itu-t (0)
identified-organization (4)
etsi (0)
id-cert-profile (194112)
policy-identifiers (1)
qcp-natural (0), qcp-legal (1), qcp-natural-qscd (2), qcp-legal-qscd (3), qcp-web (4)

See Annex B for additional information

7.1.7. Policy qualifiers syntax and semantics

Sectigo includes in end entity certificates a non-critical certificate policy extension as defined in RFC5280. Sectigo includes a single PolicyInformation extension that includes the Certificate Policy Identifier and a single Policy Qualifier referring to this CPS URI but not including a userNotice.

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

If present, the reasonCode extension shall not be marked critical and shall not be unspecified (0). If the CRL entry is for a Root CA or Subordinate CA Certificate the reasonCode extension shall be present.

If the reason for revocation is unspecified the reasonCode extension is omitted. If a reasonCode CRL entry extension is present, the CRLReason indicates the most appropriate reason for revocation of the certificate, as defined below:

• “cessationOfOperation”

• “keyCompromise” for revoked leaf certs (where Sectigo has received proof of key compromise), and;

• “caCompromise” for revoked CA certs (where Sectigo has received proof of key compromise).

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’.

For qualified certificates, the OCSP responders will continue to give a ‘good’ status for unrevoked certificates even after their expiry.

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.

For end entity certificates Sectigo publishes a signed OCSP response for every certificate at least every four days, and the signed OCSP responses are never valid for more than ten days.

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

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

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus shall be present.

The CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1. Version number(s)

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

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 ETSI standards for Trust Service Providers, and other industry standards related to the operation of CAs.

An independent external auditor to assess Sectigo's compliancy with eIDAS and ETSI performs a regular audit.

8.1. Frequency or Circumstances of Assessment

The audit scheme 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 two years in duration with a yearly surveillance audit.

8.2. Identity/Qualifications of Assessor

For ETSI/eIDAS audits, these shall be performed by a certified or accredited CAB.

In any case, a CAB means a (group of) natural or legal person(s) 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. Be accredited as per ETSI EN 319 403 and/or ISO 17065;
5. Bound by law, government regulation, or professional code of ethics; and

8.3. Assessor's relationship to assessed entity

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

8.4. Topics covered by assessment

Topics covered by the assessment include but are not limited to the following:

- Business Practices Disclosure, meaning
  - the CA discloses its business practices, and
  - the CA provides its services in accordance with its CPS
- Key Lifecycle Management, meaning
  - the CA maintains effective controls to provide reasonable assurance that the integrity of keys and certificates it manages is established and protected throughout their lifecycles.
- Certificate Lifecycle Management, meaning that
  - The CA maintains effective controls to provide reasonable assurance that Subscriber information was properly authenticated for specific registration activities, and

    - The CA maintains effective controls to provide reasonable assurance that subordinate CA certificate requests are accurate, authenticated, and approved.
- CA Environmental Control, meaning that
    - the CA maintains effective controls to provide reasonable assurance that
        - Logical and physical access to CA systems and data is restricted to authorized individuals,
        - The continuity of key and certificate management operations is maintained, and
        - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity.

Check out ETSI standards at *https://www.etsi.org* or at Annex D.

8.5. Actions taken as a result of deficiency

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

8.6. Communication of results

The audit requires that Sectigo make the Audit Report available to the public. 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 the different standards and industry best practices and guidelines.

9. OTHER BUSINESS AND LEGAL MATTERS

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

9.1. Fees

Sectigo may charge Subscriber fees for some or all of the certificate services that Sectigo offers, including issuance, renewal and reissuances (in accordance with the Sectigo Reissue Policy

stated in 9.1.6 of this CPS). Such fees are detailed on the Sectigo´s website or in the applicable subscriber agreement.

Sectigo reserves the right to change such fees. Sectigo distributors and resellers will be suitably advised of price amendments as detailed in the relevant partner agreements.

9.1.1. Certificate issuance or renewal fees

Sectigo may charge Subscribers for the issuance, management, and renewal of certificates. In most circumstances, applicable certificate fees will be delineated in the Subscriber Agreement or the Sectigo´s website 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 or OCSP.

9.1.4. Refund policy

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

9.1.5. Reissue policy

Sectigo offers a 30-day reissue policy. During the 30-day period, beginning when a certificate is first issued, subscriber may request a reissue of their certificate and incur no further fees for the reissuance. 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 subscriber.

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

9.2. Financial responsibility

9.2.1. Insurance coverage

Sectigo maintains professional Errors and Omissions Insurance.

9.2.2. Insurance or warranty coverage for end-entities

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

9.3. Confidentiality of business information

Sectigo observes applicable rules on the protection of personal data as 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 eIDAS/ETSI 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 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

Sectigo personnel in trusted positions handle confidential information in strict confidence and are required to sign confidentiality agreements before being employed in a trusted position.

Sectigo personnel, especially those on the RA/LRA, must comply with the requirements of applicable data protection laws, i.e., GDPR, 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 Privacy Policy is published at *https://sectigo.com/privacy-policy* (see clause 1.6.2)

9.4.2. Information treated as confidential

See Privacy Policy. Additionally, personal information obtained from an applicant during the application or identity verification process is considered confidential information if the information is not included in the certificate and if the information is not public information.

9.4.3. Information not deemed confidential

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

9.4.4. Responsibility to protect confidential information

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

9.4.5. Notice and consent to use confidential information

Sectigo will only use confidential information in accordance with the Privacy Policy.

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; and
- 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 certain representations regarding its public service to all Subscribers and relying parties, as described below. Sectigo reserves the right to modify such representations as it sees fit or as 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 this 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 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 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 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 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 Reseller Partner and Web Host Reseller agreements. 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.
- Act according to relevant laws and regulations.

9.6.3. Subscriber representations and warranties

Subscribers represent and warrant that when submitting to Sectigo 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 information 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 any natural or legal person.

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, and consistent with this CPS.
- 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 and regulations applicable in the jurisdictions in which it operates, 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 qualified 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 relying party accepts that in order to reasonably rely on a Sectigo qualified certificate, the relying party must:

- Minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected certificate;
- Have made reasonable efforts to acquire sufficient knowledge on using qualified certificates and PKI.
- Read and agree with the terms of the Sectigo CPS and Relying Party agreement.
- Verify a Sectigo qualified 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 qualified certificate only if it is valid and has not been revoked or has expired.
- Rely on a Sectigo qualified certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this CPS.

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 it may have otherwise been stated in relation to Qualified certificates issued pursuant to the requirements of the European Regulation 910/2014 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.
- Representations made as to information contained in a certificate except as it may be stated in the relevant product description in this CPS.
- The quality, functions or performance of any software or hardware device.
- The revocation of a certificate, if Sectigo cannot revoke the certificate due to reasons outside of its 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 does not represent or 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 complies with article 13 of the eIDAS regulation.

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 and Conditions before signing-up for a certificate. To communicate this 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 Sectigo´s 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 verified information in a certificate.
- Any liability due to fraud or willful misconduct of the applicant, including the Applicant's provision of false or misleading information during the verification process of a certificate
- Any liability that arises from the usage of a certificate that has not been issued or used in accordance 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 this 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.
- Violation of any applicable laws or regulations , whether local or foreign, including but not limited to those related to intellectual property protection, viruses, accessing computer systems, data protection and export compliance.
- Infringement of a third-party's intellectual property rights.

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.

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 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 Policy Authority

3rd Floor, Building 26 Exchange Quay, Trafford Road
Salford, Greater Manchester, M5 3EQ, United Kingdom
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 a material change to this CPS, an updated edition of this CPS will be published at the Sectigo repository (available at *https://www.sectigo.com/legal*), with suitable incremental version numbering used to identify new editions. This CPS is updated at least once per year.

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

9.12.1. Procedure for amendment

When the Sectigo Policy Authority makes an amendment to this CPS it will approve such amendments, and Sectigo will publish such 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 this CPS.

9.12.2. Notification mechanism and period

Sectigo may provide notice of an amendment to this 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 Policy Authority has the sole authority to determine whether an amendment to this 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 the eIDAS regulation, to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of Sectigo qualified products and services. eIDAS regulation applies in all Sectigo commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to Sectigo qualified products and services where Sectigo acts as a provider.

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 certificate. 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 this 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.

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.

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, by way of example only, 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 relying parties.

9.17.2. Duty to monitor agents

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

9.17.3. Ownership

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

9.17.4. Interference with Sectigo implementation

Subscribers, Relying Parties, and any other parties shall not interfere with, or reverse engineer the technical implementation of Sectigo Qualified 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.

9.17.5. Choice of cryptographic method

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

9.17.6. Sectigo partnerships limitations

Partners of the Sectigo network shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the Sectigo certificates. 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 partner, the removal of permission to use or access the Sectigo repository and any Digital certificate or Service provided by Sectigo.

9.17.7. Subscriber obligations

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

- Minimize internal risk of Private Key compromise by ensuring that adequate knowledge and training on PKI is provided internally.
- Generate their own Private / Public Key pair to be used in association with the certificate request submitted to Sectigo or a Sectigo RA for those not issued within QSCDs or HSMs managed by Sectigo.
- Ensure that the Public Key submitted to Sectigo or a Sectigo RA corresponds with the Private Key used for those not issued within QSCDs or HSMs managed by Sectigo.
- Ensure that the Public Key submitted to Sectigo or a Sectigo RA is the correct one for those not issued within QSCDs or HSMs managed by Sectigo.
- 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 for those not issued within QSCDs or HSMs managed by Sectigo.
- Read, understand and agree with all terms and conditions in this Sectigo CPS and associated policies published in the Sectigo Repository.
- 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, that a subscriber uses to generate, retain or destroy their Private Keys.

Annex A: Qualified CA hierarchy and profiles

Natural person hierarchy

Root certificate

Version:	3 (0x2)	
Serial Number:	containing at least 64 bits of output from a CSPRNG	RSA: 29c39ebe521f1d39cf0bcad43ba5f33f ECDSA: 7e0aa94f2cbb01ea668b51e9e9423f57
Signature Algorithm:	sha384WithRSAEncryption or ecdsa-with-SHA384	
Issuer:	commonName	Sectigo Qualified Natural Person Root R/E45
	organizationName	Sectigo (Europe) S.L.
	countryName	ES
Validity (25y):	Not Before:	Monday, October 5, 2020
	Not After:	Wednesday, October 4, 2045
Subject:	commonName	Sectigo Qualified Natural Person Root R/E45
	organizationName	Sectigo (Europe) S.L.
	countryName	ES
Thumbprint		RSA: eb5df65bb1c831e612f586d3fb77f10cdace7535 ECDSA: 21a43ad4c989cd31c5ec205d142d6e3e9d9db17b

ISSUING CA certificate

Sectigo Qualified Natural Person CA R/E35

Version:	3 (0x2)	
Serial Number:	containing at least 64 bits of output from a CSPRNG	RSA: 42211ba7e8e10a81d25da9bd8fd8120a ECDSA: 00c0721eeb06ad9b21780fa4db48c9db25
Signature Algorithm:	sha384WithRSAEncryption or ecdsa-with-SHA384	
Issuer:	commonName	Sectigo Qualified Natural Person Root R/E45
	organizationName	Sectigo (Europe) S.L.
	countryName	ES
Validity (15y):	Not Before:	Monday, October 5, 2020
	Not After:	Thursday, October 4, 2035
Subject:	commonName	Sectigo Qualified Natural Person CA R/E35
	organizationName	Sectigo (Europe) S.L.
	locality	Barcelona
	countryName	ES
Thumbprint		RSA: 4fd206b1c19e54c35dd46d2fe49eb3b6984050e4 ECDSA: e53b95055f93030d965f2c9e629446628d146896

Legal person hierarchy

Root certificate

Version:	3 (0x2)	
Serial Number:	containing at least 64 bits of output from a CSPRNG	RSA: 20655a1b3ef150d79171ce6d8034ddbd ECDSA: 18ba1a9ac0ee669ffc9c703d032dc189
Signature Algorithm:	sha384WithRSAEncryption or ecdsa-with-SHA384	
Issuer:	commonName	Sectigo Qualified Legal Person Root R/E45
	organizationName	Sectigo (Europe) S.L.
	countryName	ES
Validity (25y):	Not Before:	Monday, October 5, 2020
	Not After:	Wednesday, October 4, 2045
Subject:	commonName	Sectigo Qualified Legal Person Root R/E45
	organizationName	Sectigo (Europe) S.L.
	countryName	ES
Thumbprint		RSA: 3155ebf15661313c0a98fa965d283d504f6eb6d4 ECDSA: 6bb7178f2ba92338a60d263cf63e6f269d922365

ISSUING CA certificate

Sectigo Qualified Legal Person CA R/E35

Version:	3 (0x2)	
Serial Number:	containing at least 64 bits of output from a CSPRNG	RSA: 00d40b1204c9e4513275768b644f7a9df5 ECDSA: 00bf55b3b08ba28abad271e2ef2492b3c8
Signature Algorithm:	sha384WithRSAEncryption or ecdsa-with-SHA384	
Issuer:	commonName	Sectigo Qualified Legal Person Root R/E45
	organizationName	Sectigo (Europe) S.L.
	countryName	ES
Validity (15y):	Not Before:	Monday, October 5, 2020
	Not After:	Thursday, October 4, 2035
Subject:	commonName	Sectigo Qualified Legal Person R/E35
	organizationName	Sectigo (Europe) S.L.
	locality	Barcelona
	countryName	ES
Thumbprint		RSA: 5e4a378921acc8ad49df63f1a5294cb6fac45853 ECDSA: 8bb032718459d725c3dc7a7eaa8ebaae8bf4455a

Web CA hierarchy

Root certificate

Version:	3 (0x2)	
Serial Number:	containing at least 64 bits of output from a CSPRNG	RSA: 01fd6d30fca3ca51a81bbc640e35032d ECDSA: 5c8b99c55a94c5d27156decd8980cc26
Signature Algorithm:	sha384WithRSAEncryption or ecdsa-with-SHA384	
Issuer:	commonName	USERTrust RSA/ECC Certification Authority
	organizationName	The USERTRUST Network
	locality	Jersey City
	stateOrProvince	New Jersey
	countryName	US
Validity:	Not Before:	Feb 1 2010
	Not After:	Jan 18 2038
Subject:	commonName	USERTrust RSA/ECC Certification Authority
	organizationName	The USERTRUST Network
	locality	Jersey City
	stateOrProvince	New Jersey
	countryName	US
Thumbprint		RSA: 2B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E ECDSA: d1cbca5db2d52a7f693b674de5f05a1d0c957df0

ISSUING CA certificate

Sectigo Qualified Website Authentication CA R/E35

Version:	3 (0x2)	
Serial Number:	containing at least 64 bits of output from a CSPRNG	RSA: 2762378048a1b3628d507e29220de220 ECDSA: 009e568d21ded89307c34080ff2d995901
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 (15y):	Not Before:	Monday, October 5, 2020
	Not After:	Thursday, October 4, 2035
Subject:	commonName	Sectigo Qualified Website Authentication CA R/E35
	organizationName	Sectigo (Europe) S.L.
	locality	Barcelona
	countryName	ES
Thumbprint		RSA: 237014489151d07ce77a21061083d00fc5cf93f7 ECDSA: 9fc32441f3e04946432d86e81a99f96718b9738d

END ENTITY certificate

See certificate profiles document

Annex B: Types of Sectigo qualified certificates

Sectigo qualified certificates for natural person

Sectigo citizen

Description	Device	Policy	Sectigo OID	Signature/seal
Citizen	No QSCD	QCP-n	1.3.6.1.4.1.6449.1.2.1.7.1	Advanced signature
Citizen	QSCD	QCP-n-qscd	1.3.6.1.4.1.6449.1.2.1.7.2	Qualified signature

Sectigo employee

Description	Device	Policy	Sectigo OID	Signature/seal
Employee	No QSCD	QCP-n	1.3.6.1.4.1.6449.1.2.1.7.3	Advanced signature
Employee	QSCD	QCP-n-qscd	1.3.6.1.4.1.6449.1.2.1.7.4	Qualified signature

Sectigo qualified certificates for legal person

Sectigo seal

Description	Device	Policy	Sectigo OID	Signature/seal
Seal	No QSCD	QCP-l	1.3.6.1.4.1.6449.1.2.1.8.1	Advanced sealing
Seal	QSCD	QCP-l-qscd	1.3.6.1.4.1.6449.1.2.1.8.2	Qualified sealing

Sectigo seal for PSD2

Description	Device	Policy	Sectigo OID	Signature/seal
Seal certificate for PSD2	No QSCD	QCP-l	1.3.6.1.4.1.6449.1.2.1.8.5	Advanced sealing

Sectigo QWACs

Sectigo QWAC for legal person

Description	Device	Policy	Sectigo OID
QWAC for legal persons	No QSCD	QCP-w	1.3.6.1.4.1.6449.1.2.1.8.3

Sectigo QWAC for natural person

Description	Device	Policy	Sectigo OID
QWAC for natural persons	No QSCD	QCP-w	1.3.6.1.4.1.6449.1.2.1.7.5

Sectigo QWAC for PSD2

Description	Device	Policy	Sectigo OID
QWAC for PSD2	No QSCD	QCP-w QCP-w-psd2	1.3.6.1.4.1.6449.1.2.1.8.4

Annex C: ChangeLog

Version	Change Description	Date
1.0	New CPS for qualified certificates	May 2020
1.0.1	• Removed sections 1.6.3, 4.12, 4.9.4, 6.2.2, 6.2.3, 6.2.4 and 6.2.5 • Removed all sections with “no stipulation” • Removed the EPKI and powered partners from section 1.3.5 • Reorganized section 3.2 • Reworded and corrected some typos and sentences • Added new section 5.7.4	August 20, 2020
1.0.2	• Specified the F2F identification procedure or equivalent methods in section 3 • Section 6.1.1 updated regarding QSCD monitoring • Remove the “cloud” options from Annexes	September 8, 2020
1.0.3	• Change Barcelona office address • Explained in section 6.3.2 what it´s done before a CA certificate expires • Changed section 5.8 from CA or RA termination to TSP termination • Included the internal audits performed every 3 months on section 6.6.2	September 18, 2020
1.0.4	Adding the CA information in the annexes	October 5, 2020
1.0.5	Adding CA and certificates OIDs information in the annexes	October 15,2020
1.0.6	Updated the qualified TSA URL	October 20, 2020
1.0.7	• Update section 3.2.3.1.2 adding new validation methods for IP verification • Clarification on 3.1.5 about uniqueness of names • Updated section 4.2.4 adding some other domains for CAA checking • Updating typos in sections 5.5.7 and 6.1.2 • Adding CABF requirements on CRL and OCSP revocation reasons in sections 7.2.2 and 7.3 • Correcting timings in Annex A for CA certificates	October 20, 2020
1.0.8	Updated the CAs not after value and serial number	October 22, 2020
1.0.9	Correcting some typos and update section 5.4.7	October 22, 2020

Annex D: Bibliography

RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels

RFC 2253 - Lightweight Directory Access Protocol (v3) - UTF-8 String Representation of Distinguished Names

RFC 3161 - Internet X.509 Public Key Infrastructure - Time-stamp Protocol (TSP)

RFC 3279 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile

RFC 3647 - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework

RFC 5019 - The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments

RFC 5280 - Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile

RFC 5754 – Using SHA2 Algorithms with Cryptographic Message Syntax

RFC 5758 – Internet X.509 Public Key Infrastructure - Additional Algorithms and Identifiers for DSA and ECDSA

RFC 6844 - DNS Certification Authority Authorization (CAA) Resource Record

RFC 6960 - X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP

RFC 6962 - Certificate Transparency

ETSI EN 319 401 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

ETSI EN 319 411-1 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

ETSI EN 319 411-2 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

ETSI EN 319 403 - Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

ETSI EN 319 412-2 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

ETSI EN 319 412-3 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

ETSI EN 319 412-4 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

ETSI EN 319 412-5 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

ETSI TS 119 495 - Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

ETSI 119 312 - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

ANSI X9.79 - Public Key Infrastructure - Practices and Policy Framework

ITU-T X.500 - Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services

ITU-T X.503 - Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

ITU-T X.520 - Information technology - Open Systems Interconnection - The Directory: Selected attribute types

ISO 3166-1 - Codes for the representation of names of countries and their subdivisions – Part 1: Country codes

ISO/IEC 9594-8/Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks"

ISO/IEC 15408 - Information technology - Security techniques - Evaluation criteria for IT security

ISO/IEC 17065 - Conformity assessment — Requirements for bodies certifying products, processes and services

FIPS PUB 140-2 - Security Requirements for Cryptographic Module

NIST SP 800-89 - Recommendation for Obtaining Assurances for Digital Signature Applications

NIST SP 800-56A - Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography