Sectigo eIDAS

Certificate Policy and

Certification Practice Statement

Sectigo (Europe) S.L.
Version 1.0.1
Effective: November 11, 2025
Rambla Catalunya, 86 3 1,
08008 Barcelona, Spain
www.sectigo.com

Copyright Notice

Sectigo (Europe) S.L.
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 document.

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 amended by EU Regulation 1183/2024 of April 11th, 2024, commonly named eIDAS.

For issuance of specific Qualified secure server Certificates for websites, also named QWACs, Sectigo also conforms to the latest published version of the CA/B Forum Baseline Requirements of publicly-trusted TLS Server Certificates (BR) and EV Guidelines (EVG). In the event of any inconsistency between this document and the other documents specified in this paragraph, those documents take precedence over this document.

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

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

This document is only one of a set of documents relevant to the provision of certification services by Sectigo and that the list of documents contained in this clause are other documents that this document will from time to time mention, although this is not an exhaustive list.

This document, 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 Certificate Policy and Certification Practice Statement for Qualified Certificates. It outlines the legal, commercial and technical principles and practices that Sectigo employs in providing qualified certification services for PKI applications that include, but are not limited to, approving, issuing, using and managing of digital Certificates and in maintaining a X.509 Certificate based Public Key infrastructure (PKI) in accordance with the Certificate policies determined by Sectigo. These services are also accessible for persons with disabilities, where feasible.

It also defines the underlying certification processes for Subscribers and describes Sectigo's Repository operations. This document is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the Sectigo eIDAS qualified PKI.

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

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

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 *https://sectigo.com/eidascps*.

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 according to the eIDAS regulation. Sectigo conforms to this document 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 eIDAS qualified PKI. See annex A to check out Sectigo qualified PKI. Sectigo will:

- Conform its operations to this document (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 document,

- Upon receipt of a valid request to revoke the Certificate from a person authorized to request revocation using the revocation methods detailed in this document, 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 document,
- Distribute issued Certificates in accordance with the methods detailed in this document,
- Update CRLs in a timely manner as detailed in this document,
- Notify Subscribers via email (or any other method) of the imminent expiry of their Sectigo issued Certificate (for a period disclosed in this document).

1.3.2. Registration Authorities

Sectigo has established the necessary secure infrastructure to fully manage the lifecycle of Qualified Certificates within its PKI.

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

- The registration process
- The identification and authentication process.

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 document, 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 documents 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 document, 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.

In the case of QWACs Certificates, 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 document, the TLS 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. RAs may be enabled to perform validation of some or all of the subject identity information but are not able to undertake domain control validation in the case of TLS Certificates. Sectigo operates intermediate CAs from which it issues Qualified Certificates for which some part of the validation has been performed by a Registration Authority. Some of the intermediate CAs are dedicated to the work of a single RA, whilst others are dedicated to the work of multiple related RAs.

1.3.2.1. Internal Registration Authority

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

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 document, 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 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 to 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

A Relying Party is an entity that relies on the validity of the binding of the subscriber's name to a Public Key. The Relying Party uses a Subscriber's Certificate to verify or establish the identity and status of the Subscriber. 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.

A Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. 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.

A Relying Party may use information in the certificate to determine the suitability of the certificate for a particular use.

Furthermore, all Qualified Certificates shall be checked against the correspondent TSL.

1.3.5. Other participants

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

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.

The Web Host reseller program is a specific type of a reseller partner that 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 document, 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 document.

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, it 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 with 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 on 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.

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

1.5. Policy administration

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

1.5.1. Organization administering the document

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

The Policy Authority (PA):

- Establishes and maintains this document.
- 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 document are performed in accordance with the requirements, representations, and warranties of the present document.

1.5.2. Contact person

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

Sectigo Policy Authority
Unit 7, Campus Road, Listerhills Science Park, Bradford, BD7 1HR, United Kingdom
Tel: +44 (0) 161 874 7070
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 different alternatives for requesting a revocation. All these methods can be found at: *https://sectigo.com/support/revocation*

We encourage the use of our automated revocation portal, or ACME revokeCert for quickest response to issues requiring revocation.

1.5.3. Person determining CPS suitability for the policy

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

1.5.4. CPS approval procedures

The Sectigo Policy Authority approves the present document and any subsequent changes, amendments, or addenda, as specified in the *Sectigo Policy Authority (PA) Membership and Procedures* document.

1.6. Definitions and Acronyms

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

1.6.1. Acronyms

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

Acronym	Full Name
ADN	Authorization Domain Name
BR	TLS Baseline Requirements

CA	Certification Authority
CAB	Conformity Assessment Body
CA/B	Certificate Authority/Browser (Forum)
CMS	Certificate Management System
CP	Certificate Policy
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
MPIC	Multi Perspective Issuance Corroboration
NCA	National Competent Authority
NIST	National Institute for Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
PSD2	Payment Services Directive 2
PSP	Payment Service Provider
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 document shall have the meanings set forth below:

Term	Definition
Advanced Electronic Signature	means an Electronic Signature which meets the requirements set out in Article 26 of the eIDAS regulation
Advanced 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.
Authorization Number	A unique identifier of a Payment Service Provider acting as the Subscriber for PSD2 Certificates. The Authorization Number is used and recognized by the NCA.
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 TLS Server 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 Policy	Named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements.
Certificate Revocation List	Signed list indicating a set of Certificates that have been revoked by the Certificate issuer.
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
Coordinated Universal Time	Time scale based on the second as defined in Recommendation ITU-R TF.460-6
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;
Electronic Time-stamp	means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;
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*
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.
Multi-Perspective Issuance Corroboration	A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.
National Competent Authority	A national authority responsible for payment services. The NCA approves or rejects authorizations for Payment Service Providers in its country.
Object Identifier	Refers to the unique identification numbers organized hierarchically, which particularly enable referencing the conditions applicable to the Trust Service provided.
Payment Service Provider	An organization authorized to provide payment services to customers
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 Electronic Time-stamp	Means an Electronic Time-stamp which meets the requirements 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	Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA MAY assist in the Certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
Reliable Method of Communication	Means a method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.
Relying Party	Means an entity that relies upon the information contained within the Certificate.
Relying Party Agreement	means an agreement between Sectigo and a Relying Party that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference in the Repository.
Repository	Means Sectigo's Repository, available at *www.sectigo.com/legal*.
Request Token	Means a value derived in a method specified by Sectigo which binds a demonstration of control to the Certificate request.
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
X.509	Means the ITU-T standard for Certificates and their corresponding authentication framework

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

Sectigo publishes this document, 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 document.

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

2.1. Repositories

Sectigo publishes a Repository of legal notices regarding its PKI services, including this document, agreements and notices, references within this document, as well as any other information it considers essential to its services (e.g., all cross-certified subordinate CAs). 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 (Europe) S.L.
  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 document is reviewed and updated or modified versions are published at least once per year and in accordance with section 9.12 of this document. For CRL issuance frequency, see section 4.9.6 of this document.

2.4. Access controls on repositories

Documents published in the Repository are and will be for public information and access is freely available. Sectigo has security controls (logical and physical) measures in place to prevent unauthorized modification of the Repository.

2.5. Accuracy of information

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

3. IDENTIFICATION AND AUTHENTICATION

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

Sectigo conducts the overall certification management within the Sectigo 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.

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

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.

End entity certificates contain meaningful names with commonly understood semantics permitting the determination of the identity of the Subject of the Certificate.

The subject name in CA Certificates must match the issuer name in Certificates issued by the CA, as required by RFC5280.

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 document, Sectigo does not verify an Applicant's or Subscriber's right to use a trademark. Sectigo does not resolve trademark disputes. Sectigo may reject any application or revoke any Certificate that is part of a trademark dispute.

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

3.2. Initial identity validation

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

If the applicant is a natural person, Sectigo shall verify the applicant's name, applicant's address, and the authenticity of the certificate request.

The purpose of these EU Qualified Certificates is 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 meets 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 319 411-1 and 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 or best practices standards (e.g., ETSI TS 119 461).

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

For end entity certificates, Sectigo shall verify the subject information in accordance with the eIDAS regulation and the ETSI standards.

The purpose of these EU Qualified Certificates is 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 meets 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 or best practices standards (e.g., ETSI TS 119 461).

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 and follow the requisites identified above adding those from the CAB Forum throughout the BR and EV guidelines.

The purpose of these EU Qualified Certificates is 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” (QNCP-w or QEVCP-w).

The content of these Certificates meets 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 TLS Baseline Requirements, section 3.2.2.4, using one of the following methods for each FQDN (this is also specified in the Sectigo TLS CP/CPS for the issuance of TLS Server publicly-trusted Certificates, which in case of conflict with this document, the Sectigo TLS CP/CPS prevails):

1. Constructed email to Domain Contact as defined in section 3.2.2.4.4 of the Baseline Requirements

   Communicating directly with the Domain Contact confirming the Applicant's control over the requested FQDN using a constructed email address 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, which is unique, is generated by Sectigo and remains valid for use in a confirming response for no more than 30 days from its generation;

2. DNS Change as defined in section 3.2.2.4.7 of the Baseline Requirements

   Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token in a DNS CNAME or TXT record for an Authorization Domain Name or an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

This method implements the MPIC as specified in section 3.2.2.9 of the Baseline Requirements.

The Random Value, which is unique, is generated by Sectigo and remains valid for no more than 30 days from its generation;

3. IP Address as defined in section 3.2.2.4.8 of the Baseline Requirements

   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.

   This method implements the MPIC as specified in section 3.2.2.9 of the Baseline Requirements.

   This method is not used for validating wildcard Domain Names.

4. Email to DNS CAA contact as defined in section 3.2.2.4.13 of the Baseline Requirements

   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 8659 Section 3.

   This method implements the MPIC as specified in section 3.2.2.9 of the Baseline Requirements.

   The Random Value, which is unique, is generated by Sectigo and remains valid for no more than 30 days from its generation.

5. Email to DNS TXT contact as defined in Section 3.2.2.4.14 of the Baseline Requirements

   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.

   This method implements the MPIC as specified in section 3.2.2.9 of the Baseline Requirements.

   The Random Value, which is unique, is generated by Sectigo and remains valid for no more than 30 days from its generation.

6. Phone contact with DNS TXT record phone contact as defined in Section 3.2.2.4.16 of the Baseline Requirements.

   Confirming the Applicant's control over the FQDN by calling the DNS TXT record phone contact´s phone number and obtaining a confirming response to validate the ADN.

In the event of reaching voicemail, Sectigo will leave a Random Value and the ADNs being validated and then receive a confirming response utilizing the Random Value.

This method implements the MPIC as specified in section 3.2.2.9 of the Baseline Requirements.

The Random Value, which is unique, is generated by Sectigo and remains valid for no more than 30 days from its generation.

7. Phone contact with DNS CAA phone contact as defined in Section 3.2.2.4.17 of the Baseline Requirements.

   Confirming the Applicant's control over the FQDN by calling the DNS CAA phone contact´s phone number and obtaining a confirming response to validate the ADN. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659 Section 3.

   In the event of reaching voicemail, Sectigo will leave a Random Value and the ADNs being validated and then receive a confirming response utilizing the Random Value.

   This method implements the MPIC as specified in section 3.2.2.9 of the Baseline Requirements.

   The Random Value, which is unique, is generated by Sectigo and remains valid for no more than 30 days from its generation.

8. Agreed-upon change to website v2 as defined in section 3.2.2.4.18 of the Baseline Requirements

   Confirming the Applicant's control over the requested FQDN by verifying that the Request Token or Random Value is contained in the contents of a file.
   Confirming that the Request Token or Random Value is located on the Authorization Domain Name, under the HTTP[S]://<Authorization Domain>/.well-known/pki-validation/ over port 80 (HTTP) or 443 (HTTPS).

   The Random Value, which is unique, is generated by Sectigo and remains valid for use for no more than 30 days from its generation.

   This method implements the MPIC as specified in section 3.2.2.9 of the Baseline Requirements.

   This method is not used for validating wildcard Domain Names.

9. Agreed-upon change to website – ACME as defined in section 3.2.2.4.19 of the Baseline Requirements.

   Confirming the Applicant’s control over the FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method as defined in section 8.3 of RFC 8555.

The token (as defined in section 8.3 of the RFC 8555) is generated by Sectigo and remains valid for use for no more than 30 days from its generation.

This method implements the MPIC as specified in section 3.2.2.9 of the Baseline Requirements.

This method is not used for validating wildcard Domain Names.

10. TLS using ALPN as defined in section 3.2.2.4.20 of the Baseline Requirements.

    Confirming the Applicant's control over a FQDN by validating domain control of the FQDN by negotiating a new application layer protocol using the TLS Application-Layer Protocol Negotiation (ALPN) Extension [RFC7301] as defined in RFC 8737. The token (as defined in RFC 8737, section 3) SHALL NOT be used for more than 30 days from its creation.

    This method implements the MPIC as specified in section 3.2.2.9 of the Baseline Requirements.

    This method is not used for validating wildcard Domain Names.

11. DNS labeled with Account ID-ACME as defined in section 3.2.2.4.21 of the Baseline Requirements.

    Confirming the Applicant's control over the FQDN by performing the procedure documented for a "dns-account-01" challenge in draft 00 of "Automated Certificate Management Environment (ACME) DNS Labeled With ACME Account ID Challenge," available at *https://datatracker.ietf.org/doc/draft-ietf-acme-dns-account-label/*.

    The token MUST NOT be used for more than 30 days from its creation.

    This method implements the MPIC as specified in section 3.2.2.9 of the Baseline Requirements.

    This method is suitable for validating wildcard Domain Names.

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. Agreed-upon change to website as defined in section 3.2.2.5.1 of the Baseline requirements

   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.

When a Random Value, which is unique, is used it remains valid for use for no more than 30 days from its generation.

This method implements the MPIC as specified in section 3.2.2.9 of the Baseline Requirements.

2. Email, SMS, or Postal Mail to IP Address Contact as defined in section 3.2.2.5.2 of the Baseline Requirements

   Confirming the Applicant's control over the IP Address by sending a Random Value via email, 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, SMS, or postal mail. The Random Value remains valid for use in a confirming response for no more than 30 days from its creation.

3. Reverse address lookup as defined in section 3.2.2.5.3 of the Baseline Requirements

   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 3.2.3.1.1 above.

   This method implements the MPIC as specified in section 3.2.2.9 of the Baseline Requirements.

4. Phone contact with IP Address contact as defined in section 3.2.2.5.5 of the Baseline Requirements.

   Confirming the Applicant's control over the IP Adress by calling the IP Address contact´s phone number and obtain a confirming response to validate the IP Address. Sectigo makes the call to a phone number identified by the IP Address Registration Authority as the IP Address contact.

   In the event of reaching voicemail, Sectigo will leave a Random Value and the IP Address being validated and then receive a confirming response utilizing the Random Value.

   The Random Value, which is unique, is generated by Sectigo and remains valid for no more than 30 days from its generation.

5. ACME “http-01” method for IP Addresses as defined in section 3.2.2.5.6 of the Baseline Requirements.

   Confirming the Applicant’s control over the IP Address by performing the procedure documented for a “http-01” challenge in RFC 8738.

This method implements the MPIC as specified in section 3.2.2.9 of the Baseline Requirements.

6. ACME “tls-alpn-01” method for IP Addresses as defined in section 3.2.2.5.7 of the Baseline Requirements.

   Confirming the Applicant’s control over the IP Address by performing the procedure documented for a “tls-alpn-01” challenge in RFC 8738.

   This method implements the MPIC as specified in section 3.2.2.9 of the Baseline Requirements.

3.2.4. PSD2

These certificates are issued to legal persons only and shall follow the same requisites indicated in section 3.2.2. 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), (QEVCP-w), (QCP-w-psd2).

3.2.4.1. Identity verification process

Additional steps to verify PSD2 specific attributes include the name of the National Competent Authority (NCA), the PSD2 Authorization 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.

In the case where key generation is performed under the CA or RA's direct control (those issued in hardware devices, i.e., QSCDs), proof of possession is not required.

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 document.

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 document and this request is verified in accordance with the *CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates* section 3.2.2.5.

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.

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

The PA shall determine criteria for interoperation with this PKI.

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.

Identity may be established through the use of the device's current valid signature key.

3.3.2. Identification and authentication for re-key after revocation

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

Where a request for replacement or renewal of a Certificate after revocation is considered, Sectigo requires the Subscriber to authenticate itself using the original authentication details 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

Requests to revoke a certificate have different options. For example, they may be authenticated using that certificate's Public Key, regardless of whether the associated Private Key has been compromised.

Revocation at the Subscriber's request:

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

Revocation at the RA's request:

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

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

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, but is usually between 1 month and 3 years. Sectigo reserves the right to, at its discretion, issue Certificates that may fall outside of these set periods.

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

4.1. Certificate application

The certificate application process must provide sufficient information to:

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

These steps may be performed in any order that is convenient and that does not compromise security, but all must be completed before certificate issuance.

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.

Multiple certificate requests from one RA may be submitted as a batch.

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

Sectigo maintains an internal database of all previously revoked Certificates and previously rejected Certificate requests. That database is used to identify subsequent suspicious Certificate requests.

4.1.1.1. Reseller partner Certificate applications

Reseller Partners may act as RAs under the practices and policies stated within this document. The RA may make the application on behalf of the Applicant pursuant to the 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 document. Such responsibilities are detailed and maintained within the Web Host Reseller agreement and guidelines.

4.1.2. Enrollment process and responsibilities

All communications among CAs supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets and personally identifiable information shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/Private Key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data.

Applicants are responsible for providing accurate information on their certificate applications.

The enrollment process, for an applicant, includes the following:

- Completing the certificate application package
- Providing the requested information
- Responding to authentication requests in a timely manner
- Submitting required payment, where applicable

All Certificate Applicants must complete the 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 document and agree to the terms of the relevant Subscriber Agreement.
- Provide proof of identity through the submission of official documentation as requested by Sectigo during the enrolment process.

4.2. Certificate application processing

Information in certificate applications must be verified as accurate before certificates are issued.

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

The identification and authentication of the subscriber shall meet the requirements specified for subscriber authentication as specified in Sections 3.2 and 3.3. The components of the PKI (e.g., CA or RA) that are responsible for authenticating the subscriber's identity in each case are identified in this document.

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

Any certificate application that is received by Sectigo under this policy, for which the identity and authorization of the applicant has been validated, will be duly processed. However, Sectigo shall reject any application for which such validation cannot be completed (e.g., internal name), or when Sectigo has cause to lack confidence in the application or certification process.

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 certificate which includes a domain-name, for example a QWAC, Sectigo examines the Certification Authority Authorization (CAA) DNS Resource Records as specified in RFC 8659 and, if such CAA Records are present and do not grant Sectigo the authority to issue the Certificate, the application is rejected. Sectigo logs the results of the CAA checks.

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

Additionally, Entrust has contractually agreed to allow Sectigo to recognize the following domain names within the 'issue' and 'issuewild' tags as granting authorization for issuance by Sectigo.

- entrust.net
- affirmtrust.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 document). 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 document, in any jurisdiction in which such content may be used or viewed.

4.3.1. CA actions during Certificate issuance

Upon receiving the request, the CAs/RAs shall:

- Verify the identity of the requester as specified in Section 3.2.
- Verify the authority of the requester and the integrity of the information in the certificate request as specified in Section 4.1.
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate).
- Make the certificate available to the subscriber after confirming that the subscriber has formally acknowledged their obligations as described in Section 9.6.3.

Sectigo's 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.
- 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.
  - 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. Sectigo has no facility for the automated signature of such Certificates nor CRLs/OCSPs issued/signed from its correspondent root CAs, so this activity necessarily involves manual intervention by privileged users to sign such Certificates/CRLs/OCSPs. Certificate issuance by the Root CA requires an individual authorized by the CA (i.e., the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a Certificate signing operation.

Sectigo´s systems:

- do not backdate notBefore dates to avoid deadlines, prohibitions, or code-enforced restrictions.

- have in place pre-issuance and post-issuance mechanisms to reduce the potential mis-issuances that may occur. The use of linting tools help to achieve this goal.

  - CertificateSectigo performs preissuance linting using pkimetal

- Provide OCSP services for Certificates presumed to exist based on an existing PreCertificate including the ability to revoke such a Certificate.

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

CAs operating under this policy shall inform the subscriber (or other certificate subject) of the creation of a certificate and make the certificate available to the subscriber. For device certificates, the CA shall issue the certificate according to the certificate requesting protocol used by the device (this may be automated) and, if the protocol does not provide inherent notification, also notify the authorized organizational representative of the issuance (this may be in batch).

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 is delivered via email to the Subscriber using the administrator contact email address provided during the application process. The device 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.

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

4.4.1. Conduct constituting Certificate acceptance

An issued Certificate is either delivered via email or installed on a Subscriber's computer or token (QSCD or not) 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

As specified in Section 2.1, all CA certificates are published in repositories.

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

The Policy Authority must be notified whenever a CA operating under this policy issues a CA certificate.

RAs may receive notification of the issuance of certificates they approve.

QWACs certificates are also published in CT logs in compliance with the BR, EVG and/or Trust Store Provider policies.

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

4.4.3.1. Reseller partner

Issued Subscriber QWACs applied for through a Reseller Partner (i.e., Web Host Reseller Partner) on behalf of the Subscriber are emailed to the administrator contact of the Web Host Reseller Partner account. For Reseller Partners using the "auto-apply" interface, Resellers have the added option of collecting an issued Certificate from a 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.

Certificates may specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. All CAs operating under this policy should issue CRLs specifying the status of all unexpired certificates except for OCSP responder certificates. It is recommended that relying parties process and comply with this information whenever using certificates in a transaction.

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 document and named as Object Identifiers in the Certificate profile; and
- the Certificate applied for is appropriate for the application it is used in.

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

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

4.6. Certificate renewal

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

Depending on the option selected during application, the validity period of Sectigo Certificates is detailed in the relevant field within the Certificate.

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

4.6.1. Circumstance for Certificate renewal

End entity certificate renewal may be supported for certificates where the Private Key associated with the certificate has not been compromised. End entity certificates may be renewed to maintain continuity of certificate usage.

An end entity certificate may be renewed after expiration. The original certificate may or may not be revoked, but shall not be further re-keyed, renewed, or modified.

Sectigo shall make reasonable efforts to notify Subscribers via e-mail of the imminent expiration of a digital Certificate. Notice shall ordinarily be provided within at least 30-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.

If the Subscriber is responsible in providing a CSR, Sectigo will check 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 document.

4.6.5. Conduct constituting acceptance of a renewal Certificate

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

4.6.6. Publication of the renewal Certificate by the CA

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

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

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

4.7. Certificate re-key

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

An old certificate may or may not be revoked, but shall not be further re-keyed, renewed, or modified.

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.

4.7.1. Circumstances for Certificate re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a subscriber periodically obtain new keys. (Section 6.3.2 establishes usage periods for Private Keys for CAs and subscribers.) Examples of circumstances requiring certificate re-key include: expiration, loss or compromise, issuance of a new hardware token, and hardware token failure.

Certificate rekey will ordinarily take place as part of a Certificate renewal or Certificate replacement, as stated in section 3.2 of this document. 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-keying requests

For certificate re-key, Sectigo confirms the identity of the subscriber in accordance with the requirements specified in Section 3.2 for the authentication of an original certificate Application.

CA certificate re-key shall be approved by the Policy Authority.

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 document.

4.7.5. Conduct constituting acceptance of a re-keyed Certificate

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

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

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

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

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

4.8. Certificate modification

Sectigo does not offer Certificate modification.

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

4.9. Certificate revocation and suspension

Revocation of a Certificate is to permanently end the operational period of the Certificate prior to reaching the end of its stated validity period. In other words, upon revocation of a Certificate, the operational period of that Certificate is immediately considered terminated. The serial number of the revoked Certificate will be placed within the CRL and remains on the CRL as indicated in section 4.9.7. Sectigo informs Certificate Subject or Subscribers of the change of status of the Certificate.

For CA Certificates, Sectigo specifies the revocation reason.

For Subscriber Certificates, Sectigo specifies the revocation reason, if known. The Subscriber may submit their choice of revocation reason, but in some cases, this will be overridden by Sectigo (e.g., keyCompromise).

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; Sectigo is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);
- The Subscriber or Sectigo has breached a material obligation under this document or the relevant Subscriber Agreement;
- Either the Subscriber's or Sectigo's obligations under this document or the relevant Subscriber Agreement are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
- 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 document;
- The Subscriber has used the Certificate contrary to law, rule or regulation, or Sectigo reasonably believes that the Subscriber is using the Certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The Certificate was issued as a result of fraud or negligence;
- Sectigo 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;

- In the case of QWACs, the PreCertificate and the Certificate do not exactly match each other according to RFC 6962; or
- The Certificate, if not revoked, will compromise the trust status of Sectigo.

Note: the revocation of QWACs may have a maximum delay of 5 days as per the BRs.

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 document;
- Sectigo determines that any of the information appearing in the Subordinate CA Certificate is inaccurate or misleading;
- Sectigo or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- Sectigo's, or Subordinate CA's, right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless Sectigo has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by this document;
- The Subordinate CA has used the Certificate contrary to law, rule or regulation, or Sectigo reasonably believes that the Subordinate CA is using the Certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The Subordinate CA Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The Subordinate CA Certificate was issued as a result of fraud or negligence;
- The Subordinate CA Certificate, if not revoked, will compromise the trust status of Sectigo.

4.9.2. Who can request revocation

Revocation requests may be made by:

- The subscriber of the certificate or any authorized representative of the subscriber
- The CA, or affiliated RA or an authorized party that includes an RA
- The Policy Authority

Sectigo may revoke a Certificate without receiving a request and without reason. Other parties may report suspected Private Key Compromise, Certificate misuse, or other types of fraud,

compromise, misuse, inappropriate conduct, or any other matter related to Certificates, in the first instance, by email to *qcabuse@sectigo.com*.

See also section 1.5.2 of this document.

4.9.3. Procedure for revocation request

Sectigo accepts and responds to revocation requests and problem reports on a 24/7 basis. 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 document.

4.9.4. Time within which Sectigo will process the revocation request

Sectigo shall process revocation requests in accordance with this document. 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.

The time used for the provision of revocation services is synchronised with UTC at least every 24 hours.

4.9.5. Revocation checking requirement for relying parties

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this document.

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

4.9.6. CRL issuance frequency

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

All CRLs are available via a publicly-accessible HTTP URL.

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 Certificates issued. Sectigo issues a new CRL every 24 hours by default or within 6 hours if a Certificate has been revoked.

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

Sectigo may publish new CRLs prior to the expiry of the current CRL. All expired CRLs are archived (as described in section 3.4 of this document) for a period of 7 years or longer if applicable.

4.9.7. Maximum latency for CRLs

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

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

4.9.8. On-line revocation/status checking availability

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

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

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

In addition, Sectigo's Certificate 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 RFC 6960.

For the status of Subscriber Certificates:

All Sectigo's OCSP responses:

1. have a validity interval greater than or equal to eight hours;

2. have a validity interval less than or equal to ten days;

3. Sectigo SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.

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.

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

The OCSP responder may provide definitive responses about "reserved" Certificate serial numbers, as if there was a corresponding Certificate that matches the PreCertificate as stated in the RFC 6962. A Certificate serial number within an OCSP request is one of the following three options:

1. "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA Subject; or
2. "reserved" if a PreCertificate with that serial number has been issued by

    (a) the Issuing CA; or

(b) a PreCertificate Signing Certificate associated with the Issuing CA; or

3. “unused” if neither of the previous conditions are met.

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

4.10. 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. CRL and OCSP services are operated and maintained with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

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

CA equipment is dedicated to performing CA functions.

RA equipment shall be operated to ensure that the equipment meets all physical controls at all times.

Sectigo performs an annual risk assessment to identify internal and external threats and assess likelihood and potential impact of these threats to data and business processes.

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.

Sectigo implements physical Access Controls to reduce the risk of equipment tampering. All CA systems are protected against theft, loss, and unauthorized use.

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

5.1.1. Site location and construction

All CA systems are located within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CA, are consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

Such environments are based in part on the establishment of physical security tiers. A tier is a barrier such as a locked door or closed gate that provides mandatory Access Control for individuals and requires a positive response (e.g., door unlocks or gate opens) for each individual to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorized access. Moreover, each physical security tier encapsulates the next inner tier, such that an inner tier must be fully contained in

an outside tier and cannot have a common outside wall with the outside tier, the outermost tier being the outside barrier of the building (e.g., a perimeter fence or outside wall).

Sectigo houses their CA functions with at least four physical security tiers. Sectigo performs all validation operations within Tier 2 or higher. Sectigo places Information Services systems necessary to support CA functions in Tier 4 or higher. Online and offline cryptographic modules are placed in Tier 4 or higher. Sectigo protects offline cryptographic modules by placing them within Tier 4 or higher when not in use.

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

Every entry to the physically secure area of a non-authorized person shall be accompanied by an authorized person whilst in the secure area.

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

5.1.2.1. Physical Access for CA Equipment

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

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

5.1.2.2. Physical Access for RA Equipment

RA equipment is protected from unauthorized access while the RA cryptographic module is installed and activated. The RA shall implement physical Access Controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms are commensurate with the level of threat in the RA equipment environment.

5.1.3. Power and air conditioning

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

Sectigo´s facilities have backup capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning

causes a shutdown. The repositories (containing CA certificates and CRLs) are provided with uninterrupted power sufficient for a minimum of six (6) hours of operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4. Water exposures

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

5.1.5. Fire prevention and protection

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

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.

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

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

5.1.7. Waste disposal

Sectigo disposes of waste in accordance with industry best practice.

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

CA and Operations Staff and RA Staff shall remove and destroy normal office waste in accordance with local policy. Media used to collect or transmit privacy information shall be destroyed, such that the information is unrecoverable, prior to disposal. Sensitive media and paper is destroyed in accordance with the applicable policy for destruction of such material.

Destruction of media and documentation containing sensitive information, such as Private Key material, shall employ methods commensurate with those in NIST Special Publication 800-88.

5.1.8. Off-Site backup

Sectigo backs up 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.

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

5.2. Procedural controls

Sensitive data shall be protected against being revealed through re-used storage objects or storage media being accessible to unauthorized users.

5.2.1. Trusted roles

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

Trusted roles are assigned by senior members of the management team who decide 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. Sectigo ensures personnel assigned to a Trusted Role act only within the scope of their Trusted Role(s) when performing responsibilities, using privileges, or using access assigned to that Trusted Role.

Persons acting in trusted roles are only allowed to access a CMS after they are authenticated using a method approved as being suitable.

5.2.1.1. CA Administrators

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

CA Administrators do not issue Certificates to Subscribers.

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

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

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

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

5.2.2. Number of persons required per task

Multiparty control procedures are designed to ensure that at a minimum, the desired number of Trusted Persons are present to gain either physical or logical access to the CA equipment. Access to CA cryptographic modules is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a CA is activated with operational keys, further Access Controls shall be invoked to maintain split control over both physical and logical access to the CA.

Sectigo requires that at least two CA Administrators take action for:

- Physical Access
- CA key generation;
- CA signing key activation; and
- CA Private Key backup and restore.

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

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.

Sectigo confirms the identity and authorization of all personnel seeking to become Trusted Persons before such personnel are:

- Issued access devices and granted access to the required facilities;
- Given electronic credentials to access and perform specific functions on CA systems.

CA Private Keys can only be backed up, stored, and recovered by personnel in trusted roles using, at least, dual control in a physically secured environment.

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

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 (e.g., trusted roles) are properly trained and have suitable experience before being permitted to adopt those roles.

5.3.1. Qualifications, experience, and clearance requirements

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

All persons filling Trusted Roles are selected based on loyalty, trustworthiness, and integrity, and is subject to a background investigation. Personnel appointed to Trusted Roles shall:

- Possess the expert knowledge, experience and qualifications necessary for the offered services and appropriate job function;
- Have successfully completed an appropriate training program;
- Have demonstrated the ability to perform their duties;
- Be trustworthy;

- Have no other duties that would interfere or conflict with their duties for the Trusted Role;
- Have not been previously relieved of duties for reasons of negligence or non-performance of duties;
- Have not been convicted of a serious crime or other offense which affects his/her suitability for the position; and
- Have been appointed in writing by the CA management.

For Trusted Roles:

- 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, except those working for external RAs, 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.

Training shall be conducted in the following areas:

- CA or RA security principles and mechanisms;
- All PKI software versions in use on the CA or RA system;
- All PKI duties they are expected to perform;

- Incident and Compromise reporting and handling
- Disaster recovery and business continuity procedures; and
- Stipulations of this document.

For Trusted Roles:

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

Sectigo maintains records of who received training.

5.3.4. Retraining frequency and requirements

Sectigo provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

All individuals responsible for PKI roles shall be made aware of changes in the CA operation. Any significant change to the operations have a training (awareness) plan, and the execution of such plan is documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

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

Documentation is maintained identifying all personnel who received training and the level of training completed.

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

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

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

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

5.3.7. 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 document, 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 for each movement of the removable media. All this information is kept and maintained in Sectigo´s internal systems and is only accessible internally by authorized personnel or under specific requests.

CA & Certificate Lifecycle Management Events:

- CA 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
- Approval and rejections of Certificate requests
- Subscriber changes of affiliation that would invalidate the validity of an existing Certificate
- Cryptographic device lifecycle management events

- Signing of OCSP responses
- CRL updates, generations and issuances
- Custody of keys and of devices and media holding keys
- Compromise of a Private Key
- Certificate profiles

Subscriber Certificate lifecycle management events:

- Certificate requests, renewal, and re-key requests, and revocation
- Approval and rejection of Certificate requests
- Issuance of Certificates
- CRL generation and OCSP responses signing

Security Related Events:

- System downtime, software crashes and hardware failures, firewall and router activities
- Start-up and shutdown of the logging functions
- 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
- PKI and security systems actions performed
- Secure CA facility visitor entry and exit
- Security profiles changes
- Relevant router and firewall activities

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 synchronized with UTC, at least once a day
- Identity of entity making log entry (when applicable)
- Description of the entry

5.4.1.1. Router and firewall activities logs

Logging of router and firewall activities include:

- Successful and unsuccessful login attempts to routers and firewalls; and
- Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and

- Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
- Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

5.4.2. Frequency of processing log

The system administrator archives 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 two (2) years.

Those are:

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

For the RA, a system administrator other than the RA is responsible for managing the audit log.

5.4.4. Protection of audit log

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

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

5.4.5. Audit log backup procedures

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

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

5.4.6. Audit collection system (Internal vs. External)

Automatic audit collection processes run from system startup to system shutdown under the control of the Trusted Roles. The failure or alert of the audit collection system which may

adversely affect the integrity of the system, or the confidentiality of the information protected by the system will lead to Sectigo's Operators and/or CA Administrators evaluating whether a suspension of operations is required until the problem is remedied.

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

5.4.7. 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 quarterly schedule. Additional scans are run following system updates, changes, or when deemed necessary.

Sectigo will triage any critical vulnerability within a period of 48 hours after its discovery.

Sectigo performs annual risk assessments that identifies and assesses reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate data or Certificate issuance process.

Sectigo also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements to control risks identified in risk assessments.

Based on the risk assessment, Sectigo implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the risk assessment.

The risk assessments are regularly reviewed and revised, at least annually, which is finally approved by the management of Sectigo.

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

In detail,

- Patches, packages, & updates, however identified, with a critical risk rating shall be patched within 5 days. This timeline may be reduced if the vulnerability has a high likelihood of posing a risk to Sectigo.

- Patches, packages, & updates, however identified, with a high-risk rating shall be patched within 90 days.
- Patches, packages, & updates, however identified, with a medium or low risk rating do not have defined patching timelines and are uniquely evaluated.

5.5. Records archival

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

5.5.1. Types of records archived

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

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

5.5.2. Retention period for archive

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

Sectigo retains all documentation relating to Certificate requests and the verification thereof, and all Certificates and revocation thereof for a term of not less than 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

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

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

5.5.5. Requirements for Time-stamping of records

CA archive records are automatically time-stamped as they are created. System clocks used for time-stamping is maintained in synchrony with an authoritative time standard. This document describes how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

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

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

5.5.7. Procedures to obtain and verify archive information

Sectigo external RAs are required to submit appropriate documentation as detailed in the 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 private key´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 as well as the communication process to third parties. 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.

5.7.1.1. Mass Revocation Plan

Sectigo has a mass revocation plan, which is tested, reviewed and updated (if needed) annually.

This plan may be incorporated into our annual business continuity plan and is designed to cover a large-scale revocation event due to misissuances or other kinds of security issues.

This plan will follow our incident management policy and procedure focusing on the handling of the incident, responding, contacting affected subscribers, all with a clear definition on the roles of those executing this plan and the responsibilities included.

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.

Sectigo checks all the algorithms used in their systems and follow the best practices and industry standards, e.g., ETSI TS 119 312.

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. Sectigo will inform the Subscriber and Relying Party of this issue.

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 document.
- 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.
- Sectigo will destroy all CAs private keys, including backup copies as per section 6.2.6

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. 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 Electronic 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 and monitors its validity lifecycle.
    - If a QSCD loses its certification before generating the key pair and issuing a Certificate, Sectigo will replace the QSCD with a different approved one, but
    - If a QSCD loses its certification while Certificates are still valid, Sectigo will contact the customers to replace the existing Certificates, and tokens, to a different approved one.
- The Subscriber counter-signs Certificate requests that can be verified by using a manufacturer's Certificate or manufacturer's key indicating that the Subscriber key is managed in a suitable hardware module (e.g., Key attestation process),
- The Subscriber provides a suitable IT audit indicating that its operating environment achieves a level of security at least equivalent to 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 document, 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
- has a CAB witness the CA Key Pair generation process or records a video of the entire CA Key Pair generation process

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.

The report from the CA Key ceremony includes:

- roles participating in the ceremony
- functions performed by every role and in which phases
- responsibilities during and after the ceremony
- evidence collected of the ceremony
- the date of the ceremony
- an inventory of the keys generated
- the HSM model and identifier used in the ceremony
- the key generation algorithm and settings of the HSM used in the ceremony

6.1.2. Private Key delivery to Subscriber

Sectigo does not generate keys for QWACs nor for other Qualified Certificates where keys are generated on Subscriber´s software.

The subscriber or CA shall perform subscriber key pair generation. If the subscribers themselves generate Private Keys, then Private Key delivery to a subscriber is unnecessary.

When Sectigo´s CAs generate key pairs on behalf of the subscriber, the Private Key is delivered securely to the subscriber. Private keys are delivered electronically over an encrypted communication or on a FIPS or listed QSCD certified hardware cryptographic module. In all cases, the following requirements shall be met:

- Except in cases where the Sectigo operates a key archiving service on behalf of the subscriber, the CA shall not retain any copy of the key for more than two weeks after delivery of the Private Key to the subscriber.
- CAs shall use FIPS certified or QSCD listed systems and deliver Private Keys to subscribers via SSL/TLS and shall secure such delivery through the use of a PKCS#8 package or, at the CAs sole discretion, any other comparably equivalent means (e.g., PKCS#12 package) in order to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys.
- Where key pairs are pre-generated on hardware tokens, the entities distributing such tokens shall use best efforts to provide physical security of the tokens to prevent the

loss, disclosure, modification, or unauthorized use of the Private Keys on them. The RA shall maintain a record of the subscriber acknowledgment of receipt of the token.

- The subscriber shall acknowledge receipt of the Private Key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subscribers.
    - For hardware modules, accountability for the location and state of the module shall be maintained until the subscriber accepts possession of it.
    - For electronic delivery of Private Keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the Private Key. Activation data shall be delivered using a separate secure channel.

6.1.3. Public Key delivery to Certificate issuer

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

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

The Public Key of a trust anchor is provided to Relying Parties in a secure manner so that the trust anchor is not vulnerable to modification or substitution. 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.

Acceptable methods for delivery of a trust anchor include but are not limited to:

- Loading a trust anchor onto tokens delivered to Relying Parties via secure mechanisms;
- Secure distribution of trust anchor through secure out-of-band mechanisms;

- Comparison of certificate hash (fingerprint) against the trust anchor hash made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an Authentication mechanism); and
- Downloading a trust anchor from trusted web sites (e.g., CA web site) secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded and the trust anchor is not in the certificate chain for the web site certificate.

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

6.1.5. Key sizes

This document requires use of RSA or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy should contain RSA or elliptic curve Public Keys.

All certificates that expire on or before December 31, 2030 should contain subject Public Keys of at least 2048 bits for RSA/ECDSA, at least 256 bits for elliptic curve, and be signed with the corresponding Private Key.

All certificates that expire after December 31, 2030 should contain subject Public Keys of at least 3072 bits for RSA/ECDSA, at least 256 bits for elliptic curve, and be signed with the corresponding Private Key.

CAs that generate certificates and CRLs under this policy should use the SHA-256, or SHA-384 hash algorithm when generating digital signatures.

ECDSA signatures on certificates and CRLs should be generated using SHA-256 or SHA-384, as appropriate for the key length.

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

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 bits; 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, ISO/IEC 15408 or in a QSCD 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
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.

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

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

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

Table: keyUsage Extension for all CA certificates

Field	Format	Criticality	Value	Comment
keyUsage	BIT STRING	TRUE	{ id-ce 15 }	Included in all CA certificates
digitalSignature	(0)		0	Set
nonRepudiation	(1)		0	Not Set
keyEncipherment	(2)		0	Not Set
dataEnciphermen t	(3)		0	Not Set
keyAgreement	(4)		0	Not Set
keyCertSign	(5)		1	Set
cRLSign	(6)		1	Set
encipherOnly	(7)		0	Not Set
decipherOnly	(8)		0	Not Set

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.

All Sectigo´s cryptographic devices are reviewed and checked to avoid tampering during delivering by checking seals, while stored at Sectigo´s premises and that is functioning correct.

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, ISO/IEC 15408 or listed as QSCDs.

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.

Private key holders shall take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with this document and any existing contractual obligations.

6.2.2. Private Key transfer into or from a cryptographic module

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

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

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

6.2.3. 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, ISO/IEC 15408 or listed as QSCDs.

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. Subscribers must make all

reasonable efforts to protect the integrity and confidentiality of its Private Key(s). Private Keys remain active until deactivated.

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

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

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

6.2.4.1. CA Administrator Activation

Method of activating the CA system by a CA Administrator requires:

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

6.2.4.2. Offline CAs Private Key

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

6.2.4.3. Online CAs Private Keys

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

6.2.5. 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.

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

When an online CA is taken offline, the token containing the Private Key is removed from the reader in order to deactivate it.

With respect to the Private Keys of offline CAs, after the completion of a Key Generation Ceremony, in which such Private Keys are used for Private Key operations, the token containing the Private Keys are removed from the reader in order to deactivate them. Once removed from the reader, tokens are securely stored.

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

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 document.

6.3. Other aspects of Key Pair management

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

6.3.1. Public Key archival

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

The Public Key is archived as part of the certificate archival. The issuing CA retains all verification Public Keys for a minimum of 15 years or as further required by applicable law or industry regulation.

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 month to 3 years, however, Sectigo reserves the right to offer validity periods outside of this standard validity period.

Subordinate CA Certificates 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 this document. 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 are 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

Sectigo has implemented an information security policy which all employees must adhere to. The information security policy is reviewed on a regular basis and when significant changes occur.

This Information Security Policy has been approved by management and is communicated to all employees.

Sectigo retains overall responsibility for conformance with all the standards, best practices, procedures and guidelines related to information security.

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.

CA systems enforce multi-factor authentication for all accounts capable of directly causing Certificate issuance.

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 according to industry best practices (e.g., CAB Forum Network and Certificate System Security Requirements). In this security program, general protections for the network include, among others:

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

- Changing authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked.

6.7.1. Timeline for addressing vulnerabilities

The following timelines apply for the application and infrastructure critical and non-critical vulnerabilities.

Risk Assessment for every issue shall be completed within 48 hours and **Resolution time** shall be within:

Issues	Max Time
Critical	96 hours
High	30 days
Medium	90 days
Low	90 days

6.8. Time-stamping

Sectigo operates a Qualified Time-stamping Authority (TSA).

Sectigo synchronizes all TSP components with a time service provided by several services such as the National Institute of Standards and Technology (NIST) Atomic Clock through NTP (Network Time Protocol) Service based on time provided by UTC(k) laboratories. 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.

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

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

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

Certificates conform to RFC 5280 and RFC6818: Internet X.509 Public Key Infrastructure certificate and Certificate Revocation List (CRL) Profile, May 2008 & Updates to the Internet X.509 Public Key Infrastructure certificate and Certificate Revocation List (CRL) Profile, January 2013. Text fields are encoded using printableString encoding whenever possible and utf8String encoding if necessary.

Certificates contain the identity and attribute data of a subject using the base certificate with applicable extensions. The base certificate contains the version number of the certificate, the certificate's identifying serial number, the signature algorithm used to sign the certificate, the issuer's distinguished name, the validity period of the certificate, the subject's distinguished name, information about the subject's Public Key, and extensions as defined in this document.

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

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

A Certificate profile contains fields as specified below:

- key usage extension field (section 6.1.7)
- extension criticality field (section 7.1.9)
- Basic Constraints extension (section 7.1.7)

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

  - 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).

Sectigo generates non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.1. Version number(s)

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

7.1.2. Certificate extensions

Certificate extensions are in conformance to RFC 5280 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, digitalSignature and cRLSign are set.

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

Sectigo Root CA Certificates do not contain a certificatePolicies extension nor the Extended Key Usage 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, digitalSignature and cRLSign are set.
- An ExtendedKeyUsage extension not marked critical.

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 document.

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 one of these identifiers:

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

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

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

7.1.4. Name forms

Name forms are as stipulated in 3.1.1 of this document.

7.1.4.1. Encoding

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 document 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 this document 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 and PreCertificates 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	[Value 1]	
Issuer Name	be byte-for-byte identical to the `subject` field of the Issuing CA	

	Issuer DN, for example: CountryName = [Root Certificate Country Name], OrganizationName=[Root Certificate Organization], CommonName=[Root Certificate Common Name] [PrintableString encoding] OR [UTF8String encoding]	
This Update	[Date of Issuance]	
Next Update	[Date of Issuance + no more than 10 days for Subscriber Certificates or 12 months for CA Certificates]	
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, (picked by the Subscriber in the case of QWACs Certificates when creating the revocation request), as defined below:

- cessationOfOperation: this reason is used when the Subscriber no longer controls or is authorized to use the Domain Names, or the Subscriber is not using the Certificate or the CA is made aware of any circumstances that the Certificate is no longer permitted
- keyCompromise: this reason is used when Sectigo has received proof or reasonable suspicion of key compromise for revoked leaf certs
- caCompromise: this reason is used when Sectigo has received proof or reasonable suspicion of key compromise for revoked CA certs
- privilegeWithdrawn: this reason is used when there´s a Subscriber-side infraction that has not resulted in keyCompromise, e.g., misleading information in the Certificate
- affiliationChanged: this reason is used when the Subject´s name or other Subject identity information in the Certificate has changed

- superseded: this reason is used when the Subscriber has requested a replacement or Sectigo has obtained information that the domain validated information is not reliable or not in compliance with the present document or CAB Forum Baseline Requirements
- unspecified: Represented by the omission of a reasonCode.

CRL extension “ExpiredCertsOnCRL” is included in all CRLs under the Sectigo´s eIDAS hierarchy as defined by the ISO/IEC 9594-8 with the ExpiredCertsOnCRL date set to the CA Certificate's "notBefore" time and date value.

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

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 and PreCertificates issued under the terms of this document. 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.

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.

The OCSP responder for our eIDAS hierarchy uses the ArchiveCutOff extension as specified in RFC 6960 with the ArchiveCutOff date set to the CA´s Certificate “notBefore” time and date value.

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 document 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

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

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 in accordance with ETSI EN 319 403, or accredited to conduct such audits under an equivalent national scheme, or accredited by a national accreditation body in line with ISO 17065;
5. Bound by law, government regulation, or professional code of ethics

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

8.5. Actions taken as a result of deficiency

The accredited CAB 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. And when required by the Supervisory Body or the different root stores operators.

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 9.1.5 of this document). Such fees are detailed on the Sectigo´s website or in the applicable Subscriber Agreement.

Sectigo reserves the right to change such fees. Sectigo partners 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 does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties but may charge a reasonable fee for access to its Certificate databases.

9.1.3. Revocation or status information access fees

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

9.3.1. Scope of confidential information

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

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

9.3.2. Information not within the scope of confidential information

Subscribers acknowledge that revocation data of all certificates issued by Sectigo is public information and is published every 24 hours. Subscriber application data marked as "Public" in the relevant Subscriber Agreement or 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 adequate privacy safeguards and protections, and follows its published Privacy Policy, which complies with this document and applicable law.

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 provides notices to applicants and Subscribers about Sectigo's use of private information through its Privacy Policy. Sectigo also provides notices to applicants and Subscribers about Sectigo's use of private information at the time such information is collected. Sectigo will obtain an applicant's, or subscriber's, consent to use private information as required by applicable laws or regulations.

9.4.6. Disclosure pursuant to judicial or administrative process

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

Sectigo reserves the right to disclose 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 document.

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

- Comply with this document and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certification services, including but not limited to the establishment and operation of the Sectigo Repository and web site for the operation of PKI services.
- Provide trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.

- Provide prompt notice in case of compromise of its Private Key(s), data breach or any other security incident concerning Subscribers and relying parties' private data.
- Provide and validate application procedures for the various types of certificates that it may make publicly available.
- Issue certificates in accordance with this document and fulfill its obligations presented herein.
- Upon receipt of a request from an RA operating within the Sectigo network, act promptly to issue a certificate in accordance with this document.
- Upon receipt of a request for revocation from an RA operating within the Sectigo network, act promptly to revoke a certificate in accordance with this document.
- Publish accepted certificates in accordance with this document.
- Provide support to Subscribers and relying parties as described in this document.
- Revoke Certificates according to this document.
- Provide for the expiration and renewal of certificates according to this document.
- Make available a copy of this document and applicable policies to requesting parties.

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

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

9.6.2. RA representations and warranties

A Sectigo RA operates under the policies and practices detailed in this document and also the associated agreements (i.e., Reseller partner and/or Webhost reseller). The RA is bound under contract to:

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

9.6.3. Subscriber representations and warranties

Subscribers represent and warrant that when submitting to Sectigo 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 document.
- The Subscriber retains control of her Private Key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.
- The Subscriber is an end-user Subscriber and not a CA, and will not use the Private Key corresponding to any Public Key listed in the Certificate for purposes of signing any Certificate (or any other format of certified Public Key) or CRL, as a CA or otherwise, unless expressly agreed in writing between Subscriber and Sectigo.
- The Subscriber agrees with the terms and conditions of this document and other agreements and policy statements of Sectigo.
- The Subscriber abides by the laws 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.
- The Subscriber provides accurate and complete information at all times to Sectigo in the certificate request and as otherwise requested in connection with the issuance of certificates.
- The Subscriber uses the certificates only for the purposes listed in this document.

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.
- Not use a certificate, or rely upon a certificate, as control equipment in hazardous circumstances or circumstances requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, weapon control systems, or where failure could lead directly to death, personal injury, or severe environment damage, each of which is an unauthorized use of a certificate and for which a certificate is neither designed nor intended.
- Study the limitations to the usage of certificates and be aware through the Relying Party agreement the maximum value of the transactions that can be made using a Sectigo certificate.
- Read and agree with the terms of this document 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 document.

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 document 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 document.
- 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 document. 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, or a Subscriber Agreement, 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 9.2.2 of this document.

9.8.2. Exclusion of certain elements of damages

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

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

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

9.9. Indemnities

9.9.1. Indemnification by Sectigo

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

9.9.2. Indemnification by Subscriber

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

- Any false or misrepresented data supplied by the Subscriber or agent(s).
- Any failure of the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CA, Sectigo, or any person receiving or relying on the Certificate.
- Failure to protect the Subscriber's confidential data including their Private Key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's confidential data.
- 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.

9.9.3. Indemnification by Relying Parties

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

9.10. Term and termination

9.10.1. Term

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

9.10.2. Termination

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

9.10.3. Effect of termination and survival

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

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

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

9.11. Individual notices and communications with participants

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

Sectigo Policy Authority
Unit 7, Campus Road, Listerhills Science Park, Bradford, BD7 1HR, United Kingdom
Email: *legalnotices@sectigo.com*

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

9.12. Amendments

Upon the Sectigo Policy Authority accepting such changes it deems to have significant impact on the users of this document, Sectigo will, with seven (7) days' notice given of upcoming changes, communicate the updated version of this document to applicable users via registered mail, email, publishing in the Sectigo repository, (available at *https://www.sectigo.com/legal*), with suitable incremental version numbering used to identify new editions. This document is updated at least once per year.

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

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

9.12.1. Procedure for amendment

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

9.12.2. Notification mechanism and period

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

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

9.12.3. Circumstances under which OID must be changed

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

9.13. Dispute resolution provisions

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

9.14. Governing law, interpretation and jurisdiction

9.14.1. Governing law

This document is governed by and construed in accordance with the eIDAS regulation, to ensure uniform interpretation of this document, 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 document may apply or quoted implicitly or explicitly in relation to Sectigo qualified products and services where Sectigo acts as a provider, supplier, beneficiary receiver or otherwise.

9.14.2. Interpretation

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

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

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

9.14.3. Jurisdiction

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

9.15. Compliance with applicable law

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

In delivering its PKI qualified services, Sectigo complies in all material respects with high-level international standards including those on qualified certificates pursuant to the European Regulation 910/2014 and the relevant law on electronic signatures and all other relevant legislation and regulation.

9.16. Miscellaneous provisions

9.16.1. Entire agreement

This document and all documents referred to herein constitute the entire agreement between the parties, superseding all other agreements that may exist with respect to the subject matter.

Section headings are for reference and convenience only and are not part of the interpretation of this agreement.

9.16.2. Assignment

This document shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this document are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this document 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 document, or the application thereof, is for any reason and to any extent held to be invalid, void, or unenforceable, (i) such provision shall be reformed to the minimum extent necessary to make it valid and enforceable as to affect the original intention of the parties, and (ii) the remainder of the terms, provisions, covenants, and restrictions of this document shall remain in full force and effect and shall in no way be affected, impaired or invalidated.

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

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

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

9.16.5. Force Majeure

Neither Sectigo nor any independent third-party RA operating under a Sectigo Certification Authority, nor any Resellers, co-marketers, nor any subcontractors, distributors, agents, suppliers, employees, or directors of any of the forgoing shall be in default hereunder or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or related to delays in performance or from failure to perform or comply with the terms of this document, any Subscription Agreement, or any Relying Party Agreement due to any causes beyond its reasonable control, which causes, 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 document conflicts with other rules, guidelines, or contracts, this document shall prevail and bind the Subscriber and other parties except as to other contracts either:

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

9.17. Other provisions

9.17.1. Subscriber liability to relying parties

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

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 document or upon prior written approval of Sectigo. Failure to comply with this as a Subscriber will result in the revocation of the Subscriber's Certificate without further notice to the Subscriber and the Subscriber shall pay any charges payable but that have not yet been paid under the agreement. Failure to comply with this as a Relying Party will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the Sectigo Repository and any Certificate or Service provided by Sectigo.

9.17.5. Choice of cryptographic method

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

9.17.6. Sectigo partnerships limitations

Partners of the Sectigo network shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the Sectigo 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 document, 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.
- Ensure that digital signatures are only created by a QSCD device when the Certificates are issued within a QSCD
- 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 was 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 document 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 document.
- Cease using a Sectigo Certificate if any information in it becomes misleading obsolete or invalid.
- Cease using a Sectigo Certificate if such Certificate is expired and remove it from any applications and/or devices it has been installed on.
- Refrain from using the Subscriber's Private Key corresponding to the Public Key in a Sectigo issued Certificate to issue end-entity digital Certificates or subordinate CAs.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the Private Key corresponding to the Public Key published in a Sectigo Certificate.
- Request the revocation of a Certificate in case of an occurrence that materially affects the integrity of a Sectigo Certificate.
- For acts and omissions of partners and agents, that a Subscriber uses to generate, retain or destroy their Private Keys.
  Use the Private Key(s) for cryptographic functions within the secure cryptographic device when in QSCD or HSM.

Annex A: Qualified CA hierarchy and profiles

See the list at sectigo.com/eidascps

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 Electronic Signature
Citizen	QSCD	QCP-n-qscd	1.3.6.1.4.1.6449.1.2.1.7.2	Qualified Electronic 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 Electronic Signature
Employee	QSCD	QCP-n-qscd	1.3.6.1.4.1.6449.1.2.1.7.4	Qualified Electronic 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 Electronic Seal
Seal	QSCD	QCP-l-qscd	1.3.6.1.4.1.6449.1.2.1.8.2	Qualified Electronic Seal

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 Electronic Seal

Seal Certificate for PSD2	QSCD	QCP-l-qscd	1.3.6.1.4.1.6449.1.2.1.8.6	Qualified Electronic Seal

Sectigo QWACs

Sectigo QWAC for Legal Person

Description	Device	Policy	Sectigo OID
QWAC for Legal Persons	No QSCD	QEVCP-w	1.3.6.1.4.1.6449.1.2.1.8.3 1.3.6.1.4.1.6449.1.2.1.5.1

Sectigo QWAC for natural person

Description	Device	Policy	Sectigo OID
QWAC for natural persons	No QSCD	QNCP-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	QEVCP-w QCP-w-psd2	1.3.6.1.4.1.6449.1.2.1.8.4 1.3.6.1.4.1.6449.1.2.1.5.1

Annex C: ChangeLog

Version	Change Description	Date
1.0.0	New combined CP/CPS for Qualified Certificates according to the eIDAS regulation	August 1, 2025
1.0.1	Clarification on 5.4.8 regarding vulnerabilities Added section 5.7.1.1 with the plan for mass revocation Added section 6.7.1 with the timeline for addressing vulnerabilities	November 11, 2025

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

RFC 6962 - Certificate Transparency

RFC 8659 – DNS Certification Authority Authorization (CAA) Resource Record

RFC 8738 - Automated Certificate Management Environment (ACME) IP Identifier Validation Extension

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 TS 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