Sectigo eIDAS Certificate Policy

Sectigo
Version 1.0.5
Effective: October 22, 2020
Rambla Catalunya, 86 3 1,
08008 Barcelona, Spain
www.sectigo.com

Copyright Notice

Copyright Sectigo 2020. All rights reserved.

No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without prior written permission of Sectigo. Requests for any other permission to reproduce this Sectigo document (as well as requests for copies from Sectigo) must be addressed to:

Sectigo
Rambla Catalunya, 86 3 1,
08008 Barcelona, Spain
www.sectigo.com

SECTIGO

Contents

1. INTRODUCTION 12
   1.1. Overview 12
   1.2. Document name and identification 12
   1.3. PKI participants 12
      1.3.1. Certification Authorities 12
      1.3.2. Registration authorities 13
      1.3.3. Subscribers 14
      1.3.4. Relying parties 14
      1.3.5. Other participants 14
   1.4. Certificate usage 14
      1.4.1. Appropriate certificate uses 14
      1.4.2. Prohibited certificate uses 14
   1.5. Policy administration 14
      1.5.1. Organization administering the document 14
      1.5.2. Contact person 15
      1.5.3. Person determining CP suitability for the policy 15
      1.5.4. CP approval procedures 15
   1.6. Definitions and acronyms 15
      1.6.1. Definitions 15
      1.6.2. Acronyms 20
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 22
   2.1. Repositories 22
   2.2. Publication of certification information 22
   2.3. Time or frequency of publication 23
   2.4. Access controls on repositories 23
   2.5. Accuracy of Information 23
3. IDENTIFICATION AND AUTHENTICATION 23
   3.1. Naming 23
      3.1.1. Types of names 23

3.1.2. Need for names to be meaningful ... 23
3.1.3. Anonymity or pseudonymity of subscribers ... 23
3.1.4. Rules for interpreting various name forms ... 24
3.1.5. Uniqueness of names ... 24
3.1.6. Recognition, authentication, and role of trademarks ... 24
3.2. Initial identity validation ... 24
3.2.1. Authentication of a natural person identity ... 24
3.2.2. Authentication of a legal person identity ... 24
3.2.3. QWACs ... 25
3.2.4. PSD2 ... 25
3.2.5. Method to prove possession of Private Key ... 25
3.2.6. Validation of authority ... 25
3.2.7. Criteria for interoperation ... 25
3.2.8. Application validation ... 25
3.3. Identification and authentication for re-key requests ... 25
3.3.1. Identification and authentication for routine re-key ... 25
3.3.2. Identification and authentication for re-key after revocation ... 26
3.4. Identification and authentication for revocation request ... 26
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS ... 27
4.1. Certificate application ... 27
4.1.1. Who can submit a certificate application? ... 27
4.1.2. Enrollment process and responsibilities ... 27
4.2. Certificate application processing ... 28
4.2.1. Performing identification and authentication functions ... 28
4.2.2. Approval or rejection of certificate applications ... 28
4.2.3. Time to process certificate applications ... 28
4.2.4. Certificate Authority Authorization ... 29
4.3. Certificate issuance ... 29
4.3.1. CA actions during certificate issuance ... 29
4.3.2. Notification to subscriber by the CA of issuance of certificate ... 30
4.3.3. Refusal to Issue a certificate ... 30
4.4. Certificate acceptance ... 30

4.4.1. Conduct constituting certificate acceptance 30
4.4.2. Publication of the certificate by the CA 30
4.4.3. Notification of certificate issuance by the CA to other entities 31
4.5. Key pair and certificate usage 31
4.5.1. Subscriber Private Key and certificate usage 31
4.5.2. Relying party Public Key and certificate usage 31
4.6. Certificate renewal 31
4.6.1. Circumstance for certificate renewal 31
4.6.2. Who may request renewal 31
4.6.3. Processing certificate renewal requests 31
4.6.4. Notification of new certificate issuance to subscriber 32
4.6.5. Conduct constituting acceptance of a renewal certificate 32
4.6.6. Publication of the renewal certificate by the CA 32
4.6.7. Notification of certificate issuance by the CA to other entities 32
4.7. Certificate re-key 32
4.7.1. Circumstance for certificate re-key 32
4.7.2. Who may request certification of a new Public Key 32
4.7.3. Processing certificate re-keying requests 32
4.7.4. Notification of new certificate issuance to subscriber 32
4.7.5. Conduct constituting acceptance of a re-keyed certificate 32
4.7.6. Publication of the re-keyed certificate by the CA 33
4.7.7. Notification of certificate issuance by the CA to other entities 33
4.8. Certificate modification 33
4.9. Certificate revocation and suspension 33
4.9.1. Circumstances for revocation 33
4.9.2. Who can request revocation 35
4.9.3. Procedure for revocation request 35
4.9.4. Time within which CA must process the revocation request 36
4.9.5. Revocation checking requirement for relying parties 36
4.9.6. CRL issuance frequency (if applicable) 36
4.9.7. Maximum latency for CRLs (if applicable) 36
4.9.8. On-line revocation/status checking availability 36

4.9.9. On-line revocation checking requirements 37
4.10. Certificate status services 37
4.10.1. Operational characteristics 37
4.10.2. Service availability 37
4.11. End of subscription 37
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 38
5.1. Physical controls 38
5.1.1. Site location and construction 38
5.1.2. Physical access 39
5.1.3. Power and air conditioning 39
5.1.4. Water exposures 39
5.1.5. Fire prevention and protection 39
5.1.6. Media storage 39
5.1.7. Waste disposal 40
5.1.8. Off-site backup 40
5.2. Procedural controls 40
5.2.1. Trusted roles 40
5.2.2. Number of persons required per task 41
5.2.3. Identification and authentication for each role 42
5.3. Personnel controls 42
5.3.1. Qualifications, experience, and clearance requirements 42
5.3.2. Background check procedures 43
5.3.3. Training requirements 43
5.3.4. Retraining frequency and requirements 43
5.3.5. Sanctions for unauthorized actions 44
5.3.6. Independent contractor requirements 44
5.3.7. Documentation supplied to personnel 44
5.4. Audit logging procedures 44
5.4.1. Types of events recorded 44
5.4.2. Frequency of processing log 45
5.4.3. Retention period for audit log 45
5.4.4. Protection of audit log 45

5.4.5. Audit log backup procedures ... 46
5.4.6. Audit collection system (internal vs. external) ... 46
5.4.7. Vulnerability assessments ... 46
5.5. Records archival ... 46
5.5.1. Types of records archived ... 46
5.5.2. Retention period for archive ... 46
5.5.3. Protection of archive ... 47
5.5.4. Archive backup procedures ... 47
5.5.5. Requirements for time-stamping of records ... 47
5.5.6. Archive collection system (internal or external) ... 48
5.5.7. Procedures to obtain and verify archive information ... 48
5.6. Key changeover ... 48
5.7. Compromise and disaster recovery ... 48
5.7.1. Incident and compromise handling procedures ... 48
5.7.2. Computing resources, software, and/or data are corrupted ... 49
5.7.3. CA Private Key compromise procedures ... 49
5.7.4. Algorithm compromise procedures ... 49
5.7.5. Business continuity capabilities after a disaster ... 49
5.8. TSP termination ... 50
6. TECHNICAL SECURITY CONTROLS ... 50
6.1. Key pair generation and installation ... 50
6.1.1. Key pair generation ... 50
6.1.2. Private key delivery to subscriber ... 50
6.1.3. Public key delivery to certificate issuer ... 51
6.1.4. CA Public Key delivery to relying parties ... 51
6.1.5. Key sizes ... 52
6.1.6. Public key parameters generation and quality checking ... 52
6.1.7. Key usage purposes ... 52
6.2. Private Key Protection and Cryptographic Module Engineering Controls ... 54
6.2.1. Cryptographic module standards and controls ... 54
6.2.2. Private key transfer into or from a cryptographic module ... 54
6.2.3. Private key storage on cryptographic module ... 54

6.2.4. Method of activating Private Key 54
6.2.5. Method of deactivating Private Key 55
6.2.6. Method of destroying Private Key 55
6.2.7. Cryptographic Module Rating 55
6.3. Other aspects of key pair management 56
6.3.1. Public key archival 56
6.3.2. Certificate operational periods and key pair usage periods 56
6.4. Activation data 56
6.4.1. Activation data generation and installation 56
6.4.2. Activation data protection 56
6.5. Computer security controls 56
6.5.1. Specific computer security technical requirements 56
6.6. Life cycle technical controls 57
6.6.1. System development controls 57
6.6.2. Security management controls 58
6.7. Network security controls 58
6.8. Time-stamping 58
7. CERTIFICATE, CRL, AND OCSP PROFILES 59
7.1. Certificate profile 59
7.1.1. Version number(s) 59
7.1.2. Certificate extensions 59
7.1.3. Algorithm object identifiers 59
7.1.4. Name forms 59
7.1.5. Certificate policy object identifier 59
7.1.6. Policy qualifiers syntax and semantics 59
7.2. CRL profile 59
7.2.1. Version number(s) 60
7.2.2. CRL and CRL entry extensions 60
7.3. OCSP profile 60
7.3.1. Version number(s) 61
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 61
8.1. Frequency or circumstances of assessment 61

8.2. Identity/qualifications of assessor 61
8.3. Assessor's relationship to assessed entity 62
8.4. Topics covered by assessment 62
8.5. Actions taken as a result of deficiency 62
8.6. Communication of results 63
8.7. Self Audits 63
9. OTHER BUSINESS AND LEGAL MATTERS 63
9.1. Fees 63
9.1.1. Certificate issuance or renewal fees 63
9.1.2. Certificate access fees 63
9.1.3. Revocation or status information access fees 63
9.2. Financial responsibility 63
9.2.1. Insurance coverage 63
9.3. Confidentiality of business information 63
9.3.1. Scope of confidential information 63
9.3.2. Information not within the scope of confidential information 64
9.3.3. Responsibility to protect confidential information 64
9.4. Privacy of personal information 64
9.4.1. Privacy plan 64
9.4.2. Information treated as confidential 64
9.4.3. Information not deemed confidential 64
9.4.4. Responsibility to protect confidential information 64
9.4.5. Notice and consent to use confidential information 65
9.4.6. Disclosure pursuant to judicial or administrative process 65
9.5. Intellectual property rights 65
9.6. Representations and warranties 65
9.6.1. CA representations and warranties 65
9.6.2. RA representations and warranties 66
9.6.3. Subscriber representations and warranties 66
9.6.4. Relying party representations and warranties 67
9.7. Disclaimers of warranties 68
9.7.1. Fitness for a particular purpose 68

9.7.2. Other warranties ... 68
9.8. Limitations of liability ... 68
9.8.1. Damage and loss limitations ... 69
9.8.2. Exclusion of certain elements of damages ... 69
9.9. Indemnities ... 69
9.9.1. Indemnification by subscriber ... 69
9.10. Term and termination ... 70
9.10.1. Term ... 70
9.10.2. Termination ... 70
9.10.3. Effect of termination and survival ... 70
9.11. Individual notices and communications with participants ... 71
9.12. Amendments ... 71
9.12.1. Procedure for amendment ... 71
9.12.2. Notification mechanism and period ... 71
9.12.3. Circumstances under which OID must be changed ... 72
9.13. Dispute resolution provisions ... 72
9.14. Governing law, Interpretation, and Jurisdiction ... 72
9.14.1. Governing Law ... 72
9.14.2. Interpretation ... 72
9.14.3. Jurisdiction ... 72
9.15. Compliance with applicable law ... 73
9.16. Miscellaneous provisions ... 73
9.16.1. Entire agreement ... 73
9.16.2. Assignment ... 73
9.16.3. Severability ... 73
9.16.4. Enforcement (attorneys' fees and waiver of rights) ... 73
9.16.5. Force Majeure ... 73
9.16.6. Conflict of Rules ... 74
9.17. Other provisions ... 74
9.17.1. Subscriber Liability to Relying Parties ... 74
9.17.2. Duty to Monitor Agents ... 74
9.17.3. Ownership ... 74

9.17.4. Interference with Sectigo Implementation 74
9.17.5. Choice of Cryptographic Method 75
9.17.6. Sectigo Partnerships Limitations 75
9.17.7. Subscriber Obligations 75
Appendix A: ChangeLog 76

1. INTRODUCTION

1.1. Overview

This document defines the Certificate Policy for the Sectigo eIDAS PKI which governs issuance of qualified certificates.

Sectigo conforms to the EU regulation 910/2014 (aka eIDAS), to the ETSI standards and to the current version of the Baseline Requirements (BR) and EV Guidelines (EVG). In the event of any inconsistency between this CP and the BR or EVG, the BR or EVG take precedence over this document when the issued qualified certificates are intended to authenticate web sites over the SSL/TLS protocol.

Sectigo extends, 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.

1.2. Document name and identification

This document is the *Sectigo eIDAS Certificate Policy (CP)*. 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. It also defines the underlying certification processes for subscribers and describes Sectigo's repository operations. The CP is also a means of notification of roles and responsibilities for parties involved in certificate based practices within the Sectigo eIDAS PKI.

The Sectigo eIDAS CP 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.

1.3. PKI participants

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

1.3.1. Certification Authorities

Sectigo provides certificate services within the Sectigo eIDAS PKI. Sectigo will:

- Conform its operations to the CP (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the repository,
- Issue and publish certificates in a timely manner in accordance with the issuance times set out in this CP,
- Upon receipt of a valid request to revoke the certificate from a person authorized to request revocation using the revocation methods detailed in this CP, revoke a certificate issued for use within the Sectigo eIDAS PKI,

- Publish CRLs on a regular basis, in accordance with the applicable Certificate Policy and with provisions described in this CP,
- Distribute issued certificates in accordance with the methods detailed in this CP,
- Update CRLs in a timely manner as detailed in this CP,

1.3.1.1. Policy Authority:

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

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

1.3.2. Registration authorities

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

- The registration process
- The identification and authentication process.

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

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 SSL certificates.

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

Sectigo operates a number of 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

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

1.3.3. Subscribers

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

1.3.4. Relying parties

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

1.3.5. Other participants

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

1.4. Certificate usage

1.4.1. Appropriate certificate uses

Sectigo offers a range of distinct qualified certificate types. The different types have differing intended usages and differing policies.

Specific certificate usage will be defined in the CPS.

1.4.2. Prohibited certificate uses

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

1.5. Policy administration

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

1.5.1. Organization administering the document

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

1.5.2. Contact person

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

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

1.5.3. Person determining CP suitability for the policy

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

1.5.4. CP approval procedures

The Sectigo Policy Authority approves this CP and any subsequent changes, amendments, or addenda.

1.6. Definitions and acronyms

1.6.1. Definitions

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 entity that controls or operates the device named in the certificate, even if the device is sending the actual certificate request.

Applicant Representative: Means a natural person or human sponsor who is either the applicant, employed by the applicant, or an authorized agent who has express authority to represent the applicant: (i) who signs and submits, or approves a certificate request on behalf of the applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the applicant, and/or (iii) who acknowledges and agrees to the certificate Terms of Use on behalf of the applicant when the applicant is an Affiliate of the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses certificates and incorporates Root certificates.

Audit Report: Means a report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the eIDAS regulation and ETSI standards requirements.

Authorized Organizational Representative: A person (potentially among several) within an organization who is authorized to vouch for person and non-person identities. Any particular

AOR is not permanently linked to any particular non-person identity; the CA must only ascertain that the AOR is legitimately associated with the organization, and that the AOR is identified as having authority to request certificates for the organization.

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

Baseline Requirements: The CA/Browser Forum *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*, published at https://cabforum.org/

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

Certificate: Means an electronic document that uses a digital signature to bind a Public Key and an entity.

Certificate Management System: Means a system used by Sectigo to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.

Certificate Management: Means the functions that include but are not limited to the following: verification of the identity of an applicant of a certificate; authorizing the issuance of certificates; issuance of certificates; revocation of certificates; listing of certificates; distributing certificates; publishing certificates; storing certificates; storing Private Keys; escrowing Private Keys; generating, issuing, decommissioning, and destruction of key pairs; retrieving certificates in accordance with their particular intended use; and verification of the domain of an applicant of a certificate.

Certificate Manager: Means the software issued by Sectigo and used by subscribers to download certificates.

Certification Practice Statement: One of several documents forming the governance framework in which certificates are created, issued, managed, and used.

Certificate Policy: Means a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context.

Certificate Status Server: A trusted entity that provides on-line verification to a relying party of a subject certificate's revocation status, and may also provide additional attribute information for the subject certificate.

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.

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

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 Domain Name System (DNS) SOA record.

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

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

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

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;

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: The CA/Browser Forum *Guidelines For The Issuance And Management Of Extended Validation Certificates*, published at https://cabforum.org/

Front End/Internal Support System: Means a system with a public IP address, including a web server, mail server, DNS server, jump host, or authentication server.

Grace Period: Means the period during which the subscriber must make a revocation request.

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

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

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

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) No 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) No 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) No 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: Under the context of Regulation (EU) No 910/2014 (eIDAS), means an electronic signature or seal creation device that meets the requirements as stipulated in the Annex II of the eIDAS Regulation.

Qualified Trust Service Provider: 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: Under the context of Regulation (EU) No 910/2014 (eIDAS), means a certificate for identifying 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.

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.

Renewal: Placing a new order for a certificate having the same subject information for which the subscriber possesses a current and valid certificate issued by Sectigo. This is typically done <= 90 days prior to the current certificates expiration.

Replacement: Requesting the issuance of a new certificate to replace a current valid certificate issued by Sectigo without placing a new order.

Repository: Means Sectigo's repository, available at https://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.

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

Subscriber: Means an entity that has been issued a certificate.

Subscriber Agreement: Means an agreement that must be read and accepted by an applicant before applying for a certificate. The Subscriber Agreement is specific to the digital certificate

product type as presented during the product online order process and is available for reference in the repository.

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

Trust Store Provider: An Application Software Supplier which maintains a database of trusted root certificates, and CA requirements for being included therein, which is typically distributed either as part of a web browser or operating system.

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

1.6.2. Acronyms

AOR: Authorized Organization Representative

BR: Baseline Requirements

CA: Certification Authority

CAB: Conformity Assessment Body

CPS: Certification Practice Statement

CRL(s): Certificate Revocation List(s)

CSR: Certificate Signing Request

CSS: Certificate Status Server

DN: Distinguished Name

DSA: Digital Signature Algorithm

ECDSA: Elliptic Curve Digital Signature Algorithm

eIDAS: electronic Identification, Authentication and trust Services

ETSI: European Telecommunications and Standards Institute

EPKI: Enterprise Public Key Infrastructure Manager

EVG: EV Guidelines

FIPS PUB: Federal Information Processing Standards Publication

FQDN: Fully Qualified Domain Name

FTP: File Transfer Protocol

HSM: Hardware Security Module

HTTP: Hypertext Transfer Protocol

ICANN: Internet Corporation for Assigned Names and Numbers

ITU: International Telecommunication Union

ITU-T: ITU Telecommunication Standardization Sector

MDC: Multiple Domain Certificate

NIST: National Institute for Standards and Technology

OCSP: Online Certificate Status Protocol

PAC: Personal Authentication Certificate

PIN: Personal Identification Number

PKI: Public Key Infrastructure

PKIX: Public Key Infrastructure (based on X.509 Digital Certificates)

PKCS: Public Key Cryptography Standard

PSD2: Payment Services Directive 2

QSCD: Qualified Signature/Seal Creation Device

QTSP: Qualified Trust Service Provider

QWAC: Qualified Website Authentication Certificate

RA(s): Registration Authority(ies)

RFC: Request for Comments

RSA: Rivest Shamir Adleman

SAN: Subject Alternative Name

SHA: Secure Hash Algorithm

SGC: Server Gated Cryptography

S/MIME: Secure/Multipurpose Internet Mail Extension(s)

SSL: Secure Sockets Layer

TLS: Transport Layer Security

TSA: Time Stamping Authority

TSP: Trust Service Provider

UTC: Coordinated Universal Time

URL: Uniform Resource Locator

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

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

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

2.1. Repositories

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

2.2. Publication of certification information

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

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

Sectigo
Rambla Catalunya, 86 3 1,
08008 Barcelona, Spain
www.sectigo.com

2.3. Time or frequency of publication

Issuance and revocation information regarding certificates will be published as soon as possible. Updated or modified versions of Subscriber Agreements and Relying Party Agreements are usually published within seven days after approval. Updated or modified versions of the Sectigo eIDAS CP are published at least once per year and in accordance with section 9.12 of this CP. For CRL issuance frequency, see section 4.9.7 of this CP.

2.4. Access controls on repositories

Documents published in the Repository are for public information and access is freely available. Sectigo has logical access control and version control measures in place to prevent unauthorized modification of the Repository.

2.5. Accuracy of Information

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

3. IDENTIFICATION AND AUTHENTICATION

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 **Error! Reference source not found.** of this CP.

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

3.1.2. Need for names to be meaningful

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

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 assigns certificate serial numbers that appear in Sectigo certificates. Assigned serial numbers are unique.

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 CP, 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 checks subject names against a limited number of trademarks and brand names which are perceived to be of high value. A match between a part of the subject name and one of these high value names triggers a more careful examination of the subject name and applicant.

3.2. Initial identity validation

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

From time to time, Sectigo may modify the requirements related to application information to respond to Sectigo's requirements, the business context of the usage of a 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. Verification practices are detailed in the CPS.

3.2.2. Authentication of a legal person identity

For end entity certificates, the CA shall verify the subject information in accordance with the eIDAS regulation and the ETSI standards. Verification practices are detailed in the CPS. Including also PSD2 certificate types.

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.

3.2.4. PSD2

These certificates are issued to legal persons only and shall follow the same requisites indicated in section 3.2.2 but being issued for a specific sector need to specify and validate additional information as explained in the CPS.

3.2.5. Method to prove possession of Private Key

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

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

3.2.6. Validation of authority

Before issuing certificates to legal persons that assert organizational authority, Sectigo validates the subscriber's authority to act in the name of the legal person.

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.

The PA shall determine criteria for interoperation with this PKI.

3.2.8. Application validation

Sectigo employs specific applications to validate the identity of the subscriber. These have specific controls that depend on the certificate type.

3.3. Identification and authentication for re-key requests

Sectigo supports rekeys on Replacement and Renewal. Sectigo requires the subscriber to use the same authentication details (typically username and password) which they used in the original purchase of the certificate. In either case, if any of the subject details are changed during the replacement or renewal process, or if the previous verification data is older than the stipulated time for every certificate type, then the subject must be reverified.

3.3.1. Identification and authentication for routine re-key

CA and subscriber certificate re-key follows the same procedures as initial certificate issuance. Identity may be established through the use of the device's current valid signature key.

3.3.2. Identification and authentication for re-key after revocation

Sectigo does not routinely permit rekeying (or any form of Replacement or Renewal) after revocation. Revocation is generally considered a terminal event in the certificate lifecycle.

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

3.4. Identification and authentication for revocation request

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

Revocation at the subscriber's request:

Either the subscriber must be in possession of the authentication details (typically username and password) which were used to purchase the certificate originally or the subscriber must be able to send an email signed with the Private Key associated with the certificate.

Revocation at the RA's request:

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

Revocation at the CA's request:

Sectigo does not revoke certificates at the request of other TSPs. Sectigo can and does revoke subscriber certificates for cause as set out in section **Error! Reference source not found.** of this CP, but identification and authentication is not required in these cases.

Other acceptable procedures for authenticating revocation requests include:

- Having the subscriber log in to their account and revoking their certificates via their account portal. The subscriber will submit their request via their online account.
- Communication with the subscriber providing reasonable assurances that the person or organization requesting revocation is, in fact the subscriber. Such communication shall include two or more of the following: telephone confirmation, signed facsimile, signed email, postal mail, or courier service.
- The representative is the Corporate Contact, Administrator, Legal, or Technical contact authenticated in this CP section 3.2.5.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

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

The validity period of Sectigo certificates varies dependent on the certificate type, but typically, a certificate will be valid for either 1 year for QWACs, and up to 5 years for the other types. Sectigo reserves the right to, at its discretion, issue certificates that may fall outside of these set periods.

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 that does not compromise security, but all must be completed before certificate issuance.

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

4.1.1. Who can submit a certificate application?

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

The subscriber, AOR, or an RA on behalf of the subscriber shall submit a subscriber certificate application to the CA. Multiple certificate requests from one RA or AOR may be submitted as a batch.

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

4.2. Certificate application processing

Information in certificate applications must be verified as accurate before certificates are issued. Procedures to verify information in certificate applications are specified in the CPS.

4.2.1. Performing identification and authentication functions

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

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, or when Sectigo has cause to lack confidence in the application or certification process.

Sectigo reserves the right to reject an application to issue a certificate to an applicant if, in Sectigo's sole opinion, by issuing a certificate to such applicant the good and trusted name of Sectigo might be tarnished, diminished or have its value reduced, and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal.

An applicant whose application has been rejected may subsequently reapply.

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

4.2.3. Time to process certificate applications

Sectigo makes reasonable efforts to confirm certificate application information and issue a certificate within a reasonable period. The period is greatly dependent on the type of certificate and the verification requirements as stated in the CPS.

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

4.2.4. Certificate Authority Authorization

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

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

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

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

- comodo.com
- comodoca.com

4.3. Certificate issuance

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 automated systems receive and collate:

- Evidence gathered during the verification process, and/or

- Assertions that the verification has been completed according to the policy and internal documentation that sets out the acceptable means of verifying subject information.

Sectigo's automated systems record the details of the business transaction associated with the submission of a certificate request and the eventual issuance of a certificate.

Sectigo's automated (and manual) systems record the source of, and all details submitted with, evidence of verification, having been performed either by external RAs or by Sectigo's internal RA.

The correct authentication of verification evidence provided by external RAs is required before that evidence will be considered for certificate issuance.

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

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

4.3.3. Refusal to Issue a certificate

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

4.4. Certificate acceptance

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

The following conduct constitutes certificate acceptance by the subscriber:

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

4.4.2. Publication of the certificate by the CA

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

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

4.4.3. Notification of certificate issuance by the CA to other entities

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.

4.5. Key pair and certificate usage

4.5.1. Subscriber Private Key and certificate usage

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

4.5.2. Relying party Public Key and certificate usage

The final decision concerning whether to rely on a verified electronic signature or 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.

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.

4.6.1. Circumstance for certificate renewal

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

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

4.6.2. Who may request renewal

The subscriber, RA, or AOR may request the renewal of a subscriber certificate.

4.6.3. Processing certificate renewal requests

For a certificate renewal request the identity of the applicant shall be confirmed in accordance with the requirements specified in Section 3.2.

4.6.4. Notification of new certificate issuance to subscriber

As per Section 4.3.2.

4.6.5. Conduct constituting acceptance of a renewal certificate

As per Section 4.4.1.

4.6.6. Publication of the renewal certificate by the CA

As per Section 4.4.2.

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

As per Section 4.4.3

4.7. Certificate re-key

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

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

4.7.1. Circumstance for certificate re-key

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

4.7.2. Who may request certification of a new Public Key

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

4.7.3. Processing certificate re-keying requests

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

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

4.7.4. Notification of new certificate issuance to subscriber

As per Section 4.3.2.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

As per Section 4.4.1.

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

As per Section 4.4.2.

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

As per Section 4.4.3.

4.8. Certificate modification

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

4.9. Certificate revocation and suspension

CAs operating under this policy may issue CRLs, and must provide OCSP responses covering all unexpired certificates issued under this policy except for OCSP responder.

Sectigo does not utilize certificate suspension.

4.9.1. Circumstances for revocation

A certificate shall be revoked when the binding between the subject and the subject's Public Key defined within the certificate is no longer considered valid. When this occurs the associated certificate shall be revoked and placed on the CRL and/or added to the OCSP responder. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

CAs operating under this policy shall revoke a certificate within 24 hours if one or more of the following occurs:

- The subscriber requests in writing that the CA revoke the certificate;
- The subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
- The CA obtains evidence that the subscriber's Private Key corresponding to the Public Key in the certificate suffered a Key Compromise;
- Specifically for QWACs, the CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the certificate should not be relied upon.

CAs operating under this policy should revoke a certificate within 24 hours and must revoke a certificate within 5 days if one or more of the following occurs:

- The certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
- The CA obtains evidence that the certificate was misused;
- The CA is made aware that a subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
- Specifically for QWACs, the CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the certificate is no longer legally

permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);

- Specifically for QWACs, the CA is made aware that a Wildcard certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- The CA is made aware of a material change in the information contained in the certificate;
- The CA is made aware that the certificate was not issued in accordance with these Requirements or the CA's certificate Policy or Certification Practice Statement;
- The CA determines or is made aware that any of the information appearing in the certificate is inaccurate;
- The CA's right to issue certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by the CA's certificate Policy and/or Certification Practice Statement; or
- The CA 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 (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Sectigo may also revoke a certificate if any of the following occur:

- Either the subscriber’s or Sectigo’s obligations under this CP or the relevant Subscriber Agreement are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person’s information is materially threatened or compromised;
- There has been a modification of the information pertaining to the subscriber that is contained within the certificate;
- A personal identification number, Private Key or password has, or is likely to become known to someone not authorized to use it, or is being or is likely to be used in an unauthorized way;
- A subscriber's Digital certificate has not been issued in accordance with the policies set out in this CP;
- The subscriber has used the Subscription Service contrary to law, rule or regulation, or Sectigo reasonably believes that the subscriber is using the certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The certificate was issued to natural or legal persons identified as publishers of malicious software or that impersonated other natural or legal persons;
- The certificate was issued as a result of fraud or negligence; or
- The certificate, if not revoked, will compromise the trust status of Sectigo.

Sectigo shall 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 CP;
- 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 expires or is revoked or terminated, unless Sectigo has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by this CP;
- 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 natural or legal persons 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
- The Policy Authority

Other parties may report suspected Private Key Compromise, certificate misuse, or other types of fraud, compromise, inappropriate conduct, or any other matter related to certificates, in the first instance, by email to qcabuse@sectigo.com.

4.9.3. Procedure for revocation request

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

- Made by the natural or legal person that has made the certificate application.

- Made by the RA on behalf of the natural or legal person that used the RA to make the certificate application, and
- Has been authenticated by the procedures in Section 3.4 of this CP.

4.9.4. Time within which CA must 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.

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 CP.

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

By means of this CP, Sectigo has adequately informed relying parties on the usage and validation of electronic signatures or seals through this CP 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 CP.

4.9.6. CRL issuance frequency (if applicable)

For the status of subscriber certificates:

If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every 24 hours

For the status of CA certificates:

The CA shall update and reissue CRLs at least (i) once every twelve months (ii) within 24 hours after revoking a Subordinate CA certificate, and the value of the nextUpdate field must not be more than twelve months beyond the value of the thisUpdate field (iii) within 24 hours after expiration of a CA certificate

4.9.7. Maximum latency for CRLs (if applicable)

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

4.9.8. 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.

4.9.9. On-line revocation checking requirements

All CAs operating under this CP support an OCSP capability using the GET method for certificates issued in accordance with these Requirements.

For the status of subscriber certificates:

CAs operating under this policy shall update information provided via OCSP at least every four days. OCSP responses from this service have a maximum expiration time of ten days.

For the status of Subordinate CA certificates:

- Sectigo shall update information provided via an Online Certificate Status Protocol (OCSP) at least (i) every twelve months (ii) within 24 hours after revoking a Subordinate CA certificate (iii) within 24 hours after expiration of a Subordinate CA certificate

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder must not respond with a "good" status. Sectigo should monitor the responder for such requests as part of its security response procedures.

4.10. Certificate status services

4.10.1. Operational characteristics

Revocation entries on a CRL or OCSP Response are available beyond the validity period of the certificate.

Lightweight OCSP conforms to RFC 5019.

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

It´s specified in the CPS and/or Subscriber Agreement.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

All CA and RA equipment is protected from theft, loss, and unauthorized access at all times. Unauthorized use of CA and RA equipment is prohibited. 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.

5.1. Physical controls

All CA systems are protected from unauthorized access. The TSP 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).

The TSP shall construct the facilities housing their CA functions with at least four physical security tiers. TSPs shall perform 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. TSPs shall further protect offline cryptographic modules by placing them within Tier 4 or higher when not in use.

Site Location and Construction is described in more detail in the CPS.

5.1.2. Physical access

5.1.2.1. Physical Access for CA Equipment

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

Card access systems are in place to control and monitor access to all areas of the facility. Access to the Sectigo physical machinery within the secure facility is protected with locked cabinets and logical access controls. Security perimeters are clearly defined for all Sectigo locations. All 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

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

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

5.1.5. Fire prevention and protection

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

5.1.6. Media storage

Sectigo CA 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

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 secure, off-site locations which are sufficiently distant from each other to escape potential damage from a disaster at the primary location effecting a back up location.

The infrastructure team, taking into account the criticality and security requirements of the information, determines the frequency, retention, and extent of the backup. Backup of critical CA software is performed weekly and is stored offsite. Backup of critical business information is performed daily and is stored offsite. Access to backup servers/media is restricted to authorized personnel only. Backup media is regularly tested through restoration to ensure it can be relied on in the event of a disaster. Backup servers/media are appropriately labeled according to the sensitivity of the information.

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

5.2. Procedural controls

5.2.1. Trusted roles

Trusted roles are assigned by senior members of the management team who assign permissions on the “principle of least privilege” basis through a formal authorization process with authorizations being archived.

The list of personnel appointed to trusted roles is maintained and reviewed annually.

The functions and duties performed by persons in trusted roles are distributed so that a lone person cannot subvert the security and trustworthiness of PKI operations. All personnel in trusted roles are free from conflicts of interest that might prejudice the impartiality of Sectigo PKI operations.

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

5.2.1.1.CA Administrators

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

CA Administrators do not issue certificates to subscribers.

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

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

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

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

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

5.2.1.4. Internal Auditors

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

5.2.1.5. RA Staff

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

5.2.2. Number of persons required per task

Multiparty control procedures are designed to ensure that at a minimum, the desired number of Trusted Persons are present to gain either physical or logical access to the CA equipment. Access to CA cryptographic modules are 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

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.

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

5.3.1. Qualifications, experience, and clearance requirements

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

All persons filling Trusted Roles 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.

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.

5.3.2. Background check procedures

All trusted personnel have background checks before access is granted to Sectigo's systems. These checks may include, but are not limited to, verification of the individual's identity using a government issued photo ID, credit history, employment history, education, character references, social security number, criminal background, and a Companies House, or alike, cross-reference to disqualified directors.

5.3.3. Training requirements

Sectigo provides suitable training to all staff before they take on a Trusted Role should they not already have the complete skill-set required for that role. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached.

Training shall be conducted in the following areas:

- CA or RA security principles and mechanisms;
- All PKI software versions in use on the CA or RA system;
- All PKI duties they are expected to perform;
- Incident and Compromise reporting and handling
- Disaster recovery and business continuity procedures; and
- Stipulations of this CP.

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

5.3.4. Retraining frequency and requirements

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.

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. The TSP should only use contractors or consultants as Trusted Persons if the CA does not have suitable employees available to fill the roles of Trusted Persons. Independent contractors and consultants 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, physical access rights assigned to that contractor are removed as soon as possible and within 24 hours from the time of termination.

5.3.7. Documentation supplied to personnel

Sectigo gives their personnel the requisite training and documentation needed to perform their job responsibilities competently and satisfactorily.

5.4. Audit logging procedures

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

5.4.1. Types of events recorded

An audit log is maintained of each movement of the removable media.

CA & Certificate Lifecycle Management Events:

- CA Root signing key functions, including key generation, backup, recovery and destruction
- Subscriber certificate lifecycle management, including successful and unsuccessful certificate applications, certificate issuances, certificate re-issuances and certificate renewals
- Subscriber certificate revocation requests, including revocation reason

- Subscriber changes of affiliation that would invalidate the validity of an existing certificate
- CRL updates, generations and issuances
- Custody of keys and of devices and media holding keys
- Compromise of a Private Key

Security Related Events:

- System downtime, software crashes and hardware failures
- CA system actions performed by Sectigo personnel, including software updates, hardware replacements and upgrades
- Cryptographic HSM events, such as usage, de-installation, service or repair and retirement
- Successful and unsuccessful Sectigo PKI access attempts
- Secure CA facility entry and exit

Certificate Application Information:

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

All logs include the following elements:

- Date and time of entry
- Method of entry
- Source of entry
- Identity of entity making log entry

5.4.2. Frequency of processing log

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

5.4.3. Retention period for audit log

Audit logs are retained for at least 7 years and must be retained in the manner described below. 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 archived logs are maintained in a form that prevents unauthorized modification, substitution or destruction.

5.4.5. Audit log backup procedures

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

5.4.6. Audit collection system (internal vs. external)

Automatic audit collection processes run from system startup to system shutdown. The failure of an automated audit system which may adversely affect the integrity of the system or the confidentiality of the information protected by the system will lead to Sectigo's Operators and/or CA Administrators evaluating whether a suspension of operations is required until the problem is remedied.

5.4.7. Vulnerability assessments

A vulnerability is a weakness in the organization or in an information system that might be exploited by a threat, with the possibility of causing harm to assets. In order to mitigate the risk or possibility of causing harm to assets, Sectigo performs regular vulnerability assessment by taking a two-pronged approach. Sectigo assesses vulnerabilities by (1) making an assessment of the threats to, impacts on, and the vulnerabilities of assets and the likelihood of their occurrence, and (2) by developing a process of selecting and implementing security controls in order to reduce the risks identified in the risk assessment to an acceptable level. Sectigo routinely performs vulnerability assessments by identifying the vulnerability categories that face an asset. Some of the vulnerability categories that Sectigo evaluates are technical, logical, human, physical, environmental, and operational.

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

5.5. Records archival

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

5.5.1. Types of records archived

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

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

5.5.2. Retention period for archive

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

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

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

5.5.3. Protection of archive

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

5.5.4. Archive backup procedures

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

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

5.5.5. Requirements for time-stamping of records

CA archive records are automatically time-stamped as they are created. System clocks used for time-stamping is maintained in synchrony with an authoritative time standard. The CPS 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, and
- Certificate revocation.

5.5.6. Archive collection system (internal or external)

Sectigo's archive collection system is both internal and external. As part of its internal collection procedures, Sectigo may require subscribers to submit appropriate documentation in support of a certificate application.

As part of Sectigo's external collection procedures, RAs may require documentation from subscribers to support certificate applications, in their role as a Sectigo RA. In such circumstances, RAs are obliged to retain such records in line with the practices of record retention and protection as used by Sectigo and as stated in this CP.

5.5.7. Procedures to obtain and verify archive information

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

5.6. Key changeover

Towards the end of each Private Key's lifetime, a new CA signing key pair is commissioned. When a CA certificate is rekeyed only the new key is used to sign certificates from that time on. If the old Private Key is used to sign OCSP responder certificates or CRLs that cover certificates signed with that key, the old key shall be retained and protected. The corresponding new CA Public Key certificate is provided to subscribers and relying parties through the delivery methods detailed in the CPS.

5.7. Compromise and disaster recovery

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

5.7.1. Incident and compromise handling procedures

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

These procedures are in place to ensure that

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

To maintain the integrity of its services, Sectigo implements, documents, and periodically tests appropriate contingency and disaster recovery plans and procedures. These procedures define and contain a formal incident management reporting process, incident response, and incident escalation procedures to ensure professional incident management and the return to normal operations within a timely manner. The process also enables incidents to be analyzed in a way as to identify possible causes such that any weaknesses in Sectigo's processes are improved in order to prevent reoccurrence. Such plans are revised and updated at least once a year.

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

If Sectigo determines that its computing resources, software, or data operations have been compromised, Sectigo will investigate the extent of the compromise and the risk presented to affected parties. Depending on the extent of the compromise, Sectigo reserves the right to revoke affected certificates, to revoke entity keys, to provide new Public Keys to users, and to recertify subjects.

5.7.3. CA Private Key compromise procedures

Due to the nature of the CA Private Keys, these are classified as highly critical to Sectigo's business operations and continuity. If any of the CA's private signing keys were compromised or were suspected of having been compromised, Sectigo would make an assessment to determine the nature and extent of the compromise. In the most severe circumstances, Sectigo would revoke all certificates ever issued by the use of those keys, notify all owners of certificates (by email) of that revocation, and offer to re-issue the certificates to the customers with an alternative or new private signing key.

5.7.4. Algorithm compromise procedures

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

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 co-location facilities run by independent commercial data center providers, and all of the critical computer equipment is duplicated within the facility. Incoming power and connectivity feeds are duplicated. The duplicate equipment is ready to take over the role of providing the implementation of the CA, and allows Sectigo to specify a maximum system outage time (in case of critical systems failure) of 1 hour. Sectigo operations are distributed across several sites worldwide. All sites offer facilities to manage the lifecycle of a certificate, including but not limited to the application, issuance, revocation and renewal of such certificates. As well as a fully redundant CA system, Sectigo maintains provisions for the activation of a backup CA at a secondary site should the primary site suffer a total loss of systems. This disaster recovery plan states that Sectigo will endeavor to minimize interruptions to its CA operations.

5.8. 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 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 CP.
- 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.

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

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

6.1.1. Key pair generation

Subscriber key pair generation is described in the CPS.

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

CA keys are generated in a Key Generation Ceremony as specified in the CPS.

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

6.1.2. Private key delivery to subscriber

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 CAs generate key pairs on behalf of the subscriber, the Private Key is delivered securely to the subscriber. Private keys are delivered electronically 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).

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. 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 CP requires use of RSA PKCS #1, RSASSA-PSS, DSA, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy should contain RSA or elliptic curve Public Keys.

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

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

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

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

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

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

6.1.6. Public key parameters generation and quality checking

Sectigo generates the Public Key parameters. Sectigo's CA keys shall be generated within a FIPS 140-2 Level 3 or QSCD listed certified HSM.

6.1.7. Key usage purposes

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

Specific keyUsage extension settings for end entity certificates will be specified in the CPS.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

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

6.2.2. Private key transfer into or from a cryptographic module

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

6.2.3. Private key storage on cryptographic module

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

6.2.4. Method of activating Private Key

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.

6.2.4.4. Device Private Keys

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

6.2.5. Method of deactivating Private Key

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

6.2.7. Cryptographic Module Rating

See section 6.2.1.

6.3. Other aspects of key pair management

6.3.1. Public key archival

The Public Key is archived as part of the certificate archival. The issuing CA 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

Generally, the certificate validity period will be set as follows, however, Sectigo reserves the right to offer validity periods outside of this standard

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

End entity qualified certificates may have a validity period of up to 5 years. Validity periods are nested such that the validity periods of issued certificates are contained within the validity period of the issuing CA.

6.4. Activation data

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

6.4.1. Activation data generation and installation

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

6.4.2. Activation data protection

The procedures used to protect activation data is dependent on whether the data is for smartcards or passwords. Highly trusted personnel hold Smartcards. Passwords and smartcards are subject to Sectigo's Cryptographic Policy.

6.5. Computer security controls

6.5.1. Specific computer security technical requirements

Sectigo ensures the integrity of its computer systems by implementing controls, such as:

- Applying the same security controls to all systems co-located in the same zone with a certificate System;
- Maintaining online Root CA Systems in a high security zone
- Maintaining offline Root CAs air-gapped from other networks;
- Maintaining and protecting Issuing Systems, Certificate Management Systems, and Security Support systems;

- Configuring Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End/Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in Sectigo's operations and allowing only those that are approved by Sectigo;
- Reviewing configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End/Internal-Support Systems on a weekly basis;
- Undergoing penetration tests on a periodic basis and after significant infrastructure or application upgrades;
- Granting administration access to Certificate Systems only to persons acting in trusted roles and requiring their accountability for the Certificate System's security; and
- Changing authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked.

6.6. Life cycle technical controls

6.6.1. System development controls

Sectigo has formal policies in place to control, document and monitor the development of its CA systems. Development requests may only be raised by a restricted set of personnel. Development tasks are prioritized by the 'task requesters' within their area and then further prioritized by the development manager whilst considering the development task list in its entirety. 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 is tested and signed off by the QA team before being deployed to the production environment. Developers are not permitted to be involved in the testing of their own work. When issues are found by QA the QA team provide feedback to the developer to resolve the issues before development may proceed to release.

Development and QA team members do not have any access to the production environment. Access to these areas is strictly controlled.

Once the change has gone live to the production environment the task requester along with the testing team are advised and the change re-tested.

6.6.2. Security management controls

Sectigo has tools and procedures to ensure that Sectigo's operational systems and applications retain their integrity and remain configured securely. These tools and procedures include checking the integrity of the application and security software.

6.7. Network security controls

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

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

6.8. Time-stamping

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

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

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

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate profile

Certificates 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 contain the version number of the certificate, the certificate's identifying serial number, the signature algorithm used to sign the certificate, the issuer's distinguished name, the validity period of the certificate, the subject's distinguished name, information about the subject's Public Key, and extensions as defined in the *Sectigo eIDAS Certificate Profiles* document or the CPS.

CAs operating under this policy shall generate 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)

Sectigo certificates are X.509 v3 certificates. The certificate version number is set to the integer value of "2" for Version 3 certificates.

7.1.2. Certificate extensions

As described in the *Sectigo eIDAS Certificate Profiles* document or the CPS.

7.1.3. Algorithm object identifiers

Sectigo certificates are signed using algorithms including but not limited to RSA and ECDSA. Additional detail maybe found in the *Sectigo eIDAS Certificate Profiles* document or the CPS.

7.1.4. Name forms

As specified in Section 3.1.1.

7.1.5. Certificate policy object identifier

As specified in the *Sectigo eIDAS Certificate Profiles* document or the CPS.

7.1.6. Policy qualifiers syntax and semantics

A common use of policy qualifiers is to provide location information (e.g., URI) for a certificate policy. If this is desirable usage will be specified in the *Sectigo eIDAS Certificate Profiles* document or the CPS.

7.2. CRL profile

Sectigo manages and makes publicly available directories of revoked certificates using CRLs. All CRLs issued by Sectigo are X.509v2 CRLs, in particular as profiled in RFC5280. Users and relying

parties are strongly urged to consult the directories of revoked certificates at all times prior to relying on information featured in a certificate. Sectigo updates and publishes a new CRL every 24 hours or more frequently under special circumstances. The CRL for any certificate issued by Sectigo (whether Subscriber certificate or CA certificate) is found at the URL encoded within the CRLDP field of the certificate itself.

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

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

7.2.1. Version number(s)

Sectigo issues version 2 CRLs.

7.2.2. CRL and CRL entry extensions

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

7.3. OCSP profile

Sectigo publishes certificate status information using Online Certificate Status Protocol (OCSP). Sectigo's OCSP responders are capable of providing a 'good' or 'revoked' status for all

certificates issued under the terms of this CP. The OCSP responders will give an 'unknown' response for expired certificates.

Sectigo operates an OCSP service at http://ocsp.sectigo.com. Revocation information is made immediately available through the OCSP services. The OCSP responder and responses are available 24x7.

7.3.1. Version number(s)

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

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including ETSI standards for Trust Service Providers, and other industry standards related to the operation of CAs.

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

8.1. Frequency or circumstances of assessment

The audit 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.

8.2. Identity/qualifications of assessor

For ETSI/eIDAS audits, a certified or accredited CAB shall perform these.

In any case, a CAB means a (group of) natural or legal person(s) that collectively possess the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an eligible audit scheme (see 8.1);
- 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;
- 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;
- 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 audit 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 its CPS
- 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.

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.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

Sectigo charges Subscriber fees for some of the certificate services it offers. Sectigo retains its right to effectuate changes to such fees. Sectigo partners will be advised of price amendments as detailed in their respective agreements.

9.1.1. Certificate issuance or renewal fees

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

9.1.2. Certificate access fees

Sectigo 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.

9.2. Financial responsibility

9.2.1. Insurance coverage

Sectigo maintains professional Errors and Omissions Insurance.

9.3. Confidentiality of business information

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

9.3.1. Scope of confidential information

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

- 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 submitted as part of a certificate application to be published within an issued certificate, is not considered confidential information.

9.3.3. Responsibility to protect confidential information

All personnel in trusted positions handle all confidential information in strict confidence.

Sectigo personnel, especially those on the RA/LRA, must comply with the requirements of the respective laws on the protection of confidential information.

9.4. Privacy of personal information

9.4.1. Privacy plan

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

9.4.2. Information treated as confidential

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

9.4.3. Information not deemed 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 private.

9.4.4. Responsibility to protect confidential information

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

9.4.5. Notice and consent to use 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 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.

9.5. Intellectual property rights

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

9.6. Representations and warranties

9.6.1. CA representations and warranties

Sectigo makes certain representations regarding certificate services performed pursuant to this CP, as described below. Sectigo reserves its right to modify such representations as it sees fit or required by law.

Except as expressly stated in this CP or in a separate agreement with subscriber, to the extent specified in the relevant sections of the CP, Sectigo represents to:

- Comply with this CP and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certification services, including but not limited to the establishment and operation of the Sectigo Repository and web site for the operation of PKI services.
- Provide trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its Private Key(s).
- Provide and validate application procedures for the various types of certificates that it may make available.
- Issue certificates in accordance with this CP and fulfill its obligations presented herein.
- Upon receipt of a request from an RA operating within the Sectigo network, act promptly to issue a certificate in accordance with this CP.
- Upon receipt of a request for revocation from an RA operating within the Sectigo network, act promptly to revoke a Sectigo certificate in accordance with this CP.

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

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

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

9.6.2. RA representations and warranties

Sectigo's RAs operate under the policies and practices detailed in this CP and also the associated agreement. The RA is bound under contract to:

- Receive applications for Sectigo certificates in accordance with this CP.
- Perform all verification actions prescribed by the Sectigo validation procedures and this CP.
- Receive, verify, and relay to Sectigo all requests for revocation of a Sectigo certificate in accordance with the Sectigo revocation procedures and this CP.
- Act according to relevant laws and regulations.

9.6.3. Subscriber representations and warranties

Subscribers represent and warrant that when submitting to Sectigo and using a domain and distinguished name (and all other certificate application information) they do not interfere with or infringe any rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

Upon accepting a certificate, the subscriber represents to Sectigo and to relying parties that at the time of acceptance and until further notice:

- provide accurate and complete information at all times to Sectigo in the certificate request and as otherwise requested in connection with the issuance of certificates;
- install and use each certificate 1) only on domains owned or controlled by subscriber and 2) only on the server(s) accessible at the domain name listed in the certificate if the certificate is a QWAC;
- use the certificates only for the purposes listed in this CP;
- review and verify the accuracy of the data in each certificate prior to installing and using the certificate, and immediately inform Sectigo if any data listed in a certificate changes or ceases to be accurate;
- be responsible, at subscriber's expense, for 1) all computers, telecommunication equipment, software, access to the Internet, and communications networks (if any)

required to use the certificates, 2) subscriber's conduct and its website maintenance, operation, development, and content;
- promptly inform Sectigo if subscriber becomes aware of any misuse of the certificates and assist Sectigo in preventing, curing, and rectifying any misuse;
- take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in a certificate;
- immediately cease using a certificate and the related Private Key and request revocation of the certificate if 1) any information in the certificate is or becomes incorrect or inaccurate, or 2) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate;
- cease all use of the certificate and its Private Key upon expiration or revocation of the certificate;
- comply with all regulations, policies, and procedures of its networks while using certificates,
- obtain and keep in force any consent, authorization, permission or license that may be required for subscriber's lawful use of the certificates; and
- abide by all applicable laws, rules, regulations, and guidelines when using a certificate.
- The subscriber retains control of the Private Key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.
- The subscriber is an end-user subscriber and not a CA, and will not use the Private Key corresponding to any Public Key listed in the certificate for purposes of signing any certificate (or any other format of certified Public Key) or CRL, as a CA or otherwise, unless expressly agreed in writing between subscriber and Sectigo.

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

9.6.4. Relying party representations and warranties

A party relying on a Sectigo certificate accepts and acknowledges that in order to reasonably rely on a Sectigo certificate, such party must:

- Minimize the risk of relying on an electronic signature or seal created by an invalid, revoked, expired or rejected certificate; the Relying Party must have reasonably made the effort to acquire sufficient knowledge on using certificates and PKI.
- Not use a certificate, or rely upon a certificate, as control equipment in hazardous circumstances or circumstances requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, weapon control systems, or where failure could lead directly to death, personal injury, or severe environment damage, each of which is an unauthorized use of a certificate and for which a certificate is neither designed nor intended.

- Study the limitations to the usage of certificates and be aware through the Relying Party agreement the maximum value of the transactions that can be made using a Sectigo certificate.
- Read and agree with the terms of the Sectigo CP and Relying Party agreement.
- Verify a Sectigo certificate by referring to the relevant CRL and the CRLs of intermediate CA and root CA or by checking the OCSP response using the Sectigo OCSP responder.
- Trust a certificate only if it is valid and has not been revoked or has expired.
- Rely on a certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this CP.

9.7. 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 CP and in the Sectigo insurance policy.
- In addition, shall not incur liability for representations of information contained in a certificate except as it may be stated in the relevant product description in this CP.
- Does not warrant the quality, functions or performance of any software or hardware device.
- Although Sectigo is responsible for the revocation of a certificate, it cannot be held liable if it cannot execute it for reasons outside its own control.
- The validity, completeness or availability of directories of certificates issued by a third party (including an agent) unless specifically stated by Sectigo.

Sectigo assumes that user software that is claimed to be compliant with X.509v3 and other applicable standards enforces the requirements set out in this CP. Sectigo cannot warrant that such user software will support and enforce controls required by Sectigo, whilst the user should seek appropriate advice.

9.8. Limitations of liability

Sectigo certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the certificate and disclaimers of warranty that may apply. Subscribers must agree to Sectigo Terms

& Conditions, or a Subscriber Agreement, before signing-up for a certificate. To communicate information Sectigo may use:

- An organizational unit attribute.
- A Sectigo standard resource qualifier to a certificate policy.
- Proprietary or other vendors' registered extensions.

9.8.1. Damage and loss limitations

In no event (except for fraud or willful misconduct) will the aggregate liability of Sectigo to all parties including without any limitation a subscriber, an applicant, a recipient, or a Relying Party for all digital signatures and transactions related to such certificate exceed the cumulative maximum liability for such certificate as stated in the Sectigo insurance plan detailed section **Error! Reference source not found.** of this CP.

9.8.2. Exclusion of certain elements of damages

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

- Any indirect, incidental, consequential, or special damages.
- Any loss of profits.
- Any loss of data.
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of certificates or electronic signatures or seals.
- Any other transactions or services offered within the framework of this CP.
- Any other damages except for those due to reliance, on the information featured on a certificate, on the verified information in a certificate.
- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful misconduct of the applicant. Any liability that arises from the usage of a certificate that has not been issued or used in conformance with this CP.
- Any liability that arises from the usage of a certificate that is not valid.
- Any liability that arises from usage of a certificate that exceeds the limitations in usage and value and transactions stated upon it or on the CP.
- Any liability that arises from security, usability, integrity of products, including hardware and software a subscriber uses.
- Any liability that arises from compromise of a subscriber's Private Key.

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

9.9. Indemnities

9.9.1. Indemnification by subscriber

By accepting a certificate, the subscriber agrees to indemnify and hold Sectigo, as well as its agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that

Sectigo, and the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from:

- Any false or misrepresented data supplied by the subscriber or agent(s).
- Any failure of the subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CA, Sectigo, or any person receiving or relying on the certificate.
- Failure to protect the subscriber's confidential data including their Private Key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the subscriber's confidential data.
- Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.

For certificates issued at the request of a subscriber's agent, both the agent and the subscriber shall jointly and severally indemnify Sectigo, and its agents and contractors.

Although Sectigo will provide all reasonable assistance, a subscriber shall defend, indemnify, and hold Sectigo harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions on behalf of Sectigo.

9.10. Term and termination

9.10.1. Term

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

9.10.2. Termination

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

9.10.3. Effect of termination and survival

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

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

Termination of this CP shall not affect any Subscriber Agreements executed during the term of this CP. Upon termination of this CP, all PKI participants are bound by the terms of this CP for certificates issued during the term of this CP and for the remainder of the validity periods of such certificates.

9.11. Individual notices and communications with participants

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

Sectigo Policy Authority
3rd Floor, 26 Exchange Quay, Trafford Road
Salford, Greater Manchester, M5 3EQ, United Kingdom
Email: legalnotices@sectigo.com

9.12. Amendments

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

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 the CP and without changing the version number of this CP.

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

9.12.1. Procedure for amendment

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

9.12.2. Notification mechanism and period

Sectigo provides notice of an amendment to the CP by posting it to the Repository. Amendments become effective on the date provided in the document, when an amendment is

written in a separate document, or on the date provided in this CP, when written in this document.

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

9.12.3. Circumstances under which OID must be changed

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

9.13. Dispute resolution provisions

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

9.14. Governing law, Interpretation, and Jurisdiction

9.14.1. Governing Law

This CP is governed by, and construed in accordance with the eIDAS regulation. This choice of law is made to ensure uniform interpretation of this CP, regardless of the place of residence or place of use of Sectigo certificates or other products and services. The eIDAS regulation applies in all Sectigo commercial or contractual relationships in which this CP may apply or quoted implicitly or explicitly in relation to Sectigo products and services where Sectigo acts as a provider, supplier, beneficiary receiver or otherwise.

9.14.2. Interpretation

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

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

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

9.14.3. Jurisdiction

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

9.15. Compliance with applicable law

This CP is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders, including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. In delivering its PKI services Sectigo complies in all material respects with high-level international standards 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 CP and all documents referred to herein constitute the entire agreement between the parties, superseding all other agreements that may exist with respect to the subject matter. Section headings are for reference and convenience only and are not part of the interpretation of this agreement.

9.16.2. Assignment

This CP shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this CP are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CP articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

9.16.3. Severability

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

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

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

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

9.16.5. Force Majeure

Neither Sectigo nor any independent third-party RA operating under a Sectigo Certification Authority, nor any Resellers, Co-marketers, nor any subcontractors, distributors, agents, suppliers, employees, or directors of any of the forgoing shall be in default hereunder or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of

or related to delays in performance or from failure to perform or comply with the terms of the Sectigo CP, any Subscription Agreement, or any Relying Party Agreement due to any causes beyond its reasonable control, which causes include acts of God or the public enemy, riots and insurrections, war, accidents, fire, strikes and other labor difficulties (whether or not Sectigo is in a position to concede to such demands), embargoes, judicial action, failure or default of any superior certification authority, lack of or inability to obtain export permits or approvals, necessary labor materials, energy, utilities, components or machinery, acts of civil or military authorities.

9.16.6. Conflict of Rules

When this CP conflicts with other rules, guidelines, or contracts, this CP shall prevail and bind the subscriber and other parties except as to other contracts either:

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

9.17. Other provisions

9.17.1. Subscriber Liability to Relying Parties

Without limiting other subscriber obligations stated in this CP, subscribers are liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein and have verified one or more 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 an agent supplies to Sectigo. The subscriber must promptly notify the issuer of any misrepresentations and omissions made by an agent. The duty of this article is continuous.

9.17.3. Ownership

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

9.17.4. Interference with Sectigo Implementation

Subscribers, Relying Parties, and any other parties shall not interfere with, or reverse engineer the technical implementation of Sectigo PKI services including the key generation process, the public web site and the Sectigo repositories except as explicitly permitted by this CP or upon prior written approval of Sectigo. Failure to comply with this as a subscriber will result in the revocation of the subscriber's certificate without further notice to the subscriber and the subscriber shall pay any charges payable but that have not yet been paid under the agreement.

Failure to comply with this as a Relying Party will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the Sectigo repository and any certificate or Service provided by Sectigo.

9.17.5. Choice of Cryptographic Method

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

9.17.6. Sectigo Partnerships Limitations

Partners of the Sectigo network shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the Sectigo products and services. Sectigo partners shall specifically refrain from seeking partnerships with other root authorities or apply procedures originating from such authorities. Failure to comply with this will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the Sectigo repository and any Digital certificate or Service provided by Sectigo.

9.17.7. Subscriber Obligations

Unless otherwise stated in this CP, subscribers shall exclusively be responsible:

- To minimize internal risk of Private Key compromise by ensuring adequate knowledge and training on PKI is provided internally.
- To generate their own Private / Public Key pair to be used in association with the certificate request submitted to Sectigo or a Sectigo RA.
- Ensure that the Public Key submitted to Sectigo or a Sectigo RA corresponds with the Private Key used.
- Ensure that the Public Key submitted to Sectigo or a Sectigo RA is the correct one.
- Provide correct and accurate information in its communications with Sectigo or a Sectigo RA.
- Alert Sectigo or a Sectigo RA if at any stage whilst the certificate is valid, any information originally submitted has changed since it had been submitted to Sectigo.
- Generate a new, secure key pair to be used in association with a certificate that it requests from Sectigo or a Sectigo RA.
- Read, understand and agree with all terms and conditions in this Sectigo CP and associated policies published in the Sectigo Repository at https://www.sectigo.com/legal/
- Refrain from tampering with a Sectigo certificate.
- Use Sectigo certificates for legal and authorized purposes in accordance with the suggested usages and practices in this CP.
- Cease using a Sectigo certificate if any information in it becomes misleading obsolete or invalid.
- Cease using a Sectigo certificate if such certificate is expired and remove it from any applications and/or devices it has been installed on.

- Refrain from using the subscriber's Private Key corresponding to the Public Key in a Sectigo issued certificate to issue end-entity certificates or subordinate CAs.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the Private Key corresponding to the Public Key published in a Sectigo certificate.
- Request the revocation of a certificate in case of an occurrence that materially affects the integrity of a Sectigo certificate.
- For acts and omissions of partners and agents, they use to generate, retain, escrow, or destroy their Private Keys.

Appendix A: ChangeLog

Version	Change Description	Date
1.0	Create new CP for eIDAS qualified certificates	August 1, 2020
1.0.1	Update CP accordingly with CPS	August 20, 2020
1.0.2	Update section 3.2 and remove of some other sections	September 17, 2020
1.0.3	Corrected some typos and updated some URLs	October 19, 2020
1.0.4	Clarification of sections 1.1 and 3.2.5	October 20, 2020
1.0.5	Corrected some typos in 1.6.1, removed of an unclear sentence in 3.1.5 and add the transitional domains for CAA check in 4.2.4 as in the CPS.	October 22, 2020