

# Business Practices Disclosure for S/MIME Certificates

---

## Content

1	INTRODUCTION .....	11
1.1	Overview .....	11
1.2	Document Name and Identification .....	11
1.2.1	Revisions .....	12
1.3	PKI Participants .....	12
1.3.1	Certification Authorities .....	12
1.3.2	Registration Authorities.....	12
1.3.2.1	Internal Registration Authority .....	12
1.3.2.2	External Registration Authority.....	12
1.3.3	Subscribers (End Entities).....	13
1.3.4	Relying Parties .....	13
1.3.5	Other Participants.....	13
1.3.5.1	Reseller Partners .....	13
1.3.5.2	EPKI Manager Accounts .....	13
1.4	Certificate Usage.....	13
1.4.1	Appropriate Certificate Uses .....	13
1.4.2	Prohibited Certificate Uses.....	13
1.5	Policy Administration .....	13
1.5.1	Organization Administering the Document.....	13
1.5.2	Contact Person .....	13
1.5.2.1	Problem Reporting Address.....	13
1.5.3	Person Determining CP/CPS Suitability for the Policy .....	14
1.5.4	CP/CPS approval procedures .....	14
1.6	Definitions and Acronyms .....	14
1.6.1	Definitions.....	14
1.6.2	Acronyms .....	14
1.6.3	Conventions.....	14
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES.....	15

- 2.1 Repositories..... 15
- 2.2 Publication of Certification Information..... 15
- 2.3 Time or Frequency of Publication..... 15
- 2.4 Access Controls on Repositories..... 15
- 2.5 Accuracy of Information..... 15
- 3 IDENTIFICATION AND AUTHENTICATION ..... 16
  - 3.1 Naming..... 16
    - 3.1.1 Types of Names ..... 16
    - 3.1.2 Need for Names to be Meaningful ..... 16
    - 3.1.3 Anonymity or Pseudonymity of Subscribers..... 16
    - 3.1.4 Rules for Interpreting Various Name Forms ..... 16
      - 3.1.4.1 Non ASCII character substitution..... 16
      - 3.1.4.2 Geographic names ..... 16
    - 3.1.5 Uniqueness of Names..... 16
    - 3.1.6 Recognition, Authentication, and Role of Trademarks ..... 16
  - 3.2 Initial Identity Validation ..... 16
    - 3.2.1 Method to Prove Possession of Private Key ..... 16
    - 3.2.2 Validation of mailbox authorization or control ..... 16
      - 3.2.2.1 Validating authority over mailbox via domain ..... 16
      - 3.2.2.2 Validating control over mailbox via email..... 16
      - 3.2.2.3 Validating applicant as operator of associated mail server(s)..... 16
      - 3.2.2.4 Validating control over mailbox usingACME extensions ..... 16
    - 3.2.3 Authentication of Organization Identity..... 16
      - 3.2.3.1 Attribute collection of organization identity..... 17
      - 3.2.3.2 Validation of organization identity ..... 17
      - 3.2.3.3 Disclosure of verification sources ..... 17
    - 3.2.4 Authentication of Individual Identity ..... 17
      - 3.2.4.1 Attribute collection and validation of individual identity..... 17
    - 3.2.5 Non-Verified Subscriber Information..... 17
    - 3.2.6 Validation of Authority..... 17
    - 3.2.7 Criteria for Interoperation ..... 17
    - 3.2.8 Reliability of verification sources ..... 17
  - 3.3 Identification and Authentication for Re-Key Requests ..... 17
    - 3.3.1 Identification and Authentication for Routine Re-Key ..... 17
    - 3.3.2 Identification and Authentication for Re-Key after Revocation..... 17
  - 3.4 Identification and Authentication for Revocation Request ..... 17

- 4 CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS ..... 18
  - 4.1 Certificate Application ..... 18
    - 4.1.1 Who can Submit a Certificate Application ..... 18
      - 4.1.1.1 EPKI Manager Account Holder Certificate Applications ..... 18
      - 4.1.1.2 Reseller Partner Certificate Applications ..... 18
    - 4.1.2 Enrollment Process and Responsibilities ..... 18
  - 4.2 Certificate Application Processing ..... 18
    - 4.2.1 Performing Identification and Authentication Functions ..... 18
    - 4.2.2 Approval or Rejection of Certificate Applications ..... 18
    - 4.2.3 Time to Process Certificate Applications ..... 18
    - 4.2.4 Certificate Authority Authorization ..... 18
      - 4.2.4.1 DNSSEC Validation of CAA records ..... 18
  - 4.3 Certificate Issuance ..... 18
    - 4.3.1 CA Actions during Certificate Issuance ..... 18
    - 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate ..... 19
    - 4.3.3 Refusal to Issue a Certificate ..... 19
  - 4.4 Certificate Acceptance ..... 19
    - 4.4.1 Conduct Constituting Certificate Acceptance ..... 19
    - 4.4.2 Publication of the Certificate by the CA ..... 19
    - 4.4.3 Notification of Certificate Issuance by the CA to Other Entities ..... 19
      - 4.4.3.1 Reseller Partner ..... 19
      - 4.4.3.2 EPKI Manager Account Holder ..... 19
  - 4.5 Key Pair and Certificate Usage ..... 19
    - 4.5.1 Subscriber Private Key and Certificate Usage ..... 19
    - 4.5.2 Relying Party Public Key and Certificate Usage ..... 19
  - 4.6 Certificate Renewal ..... 19
    - 4.6.1 Circumstance for Certificate Renewal ..... 19
    - 4.6.2 Who May Request Renewal ..... 19
    - 4.6.3 Processing Certificate Renewal Requests ..... 19
    - 4.6.4 Notification of New Certificate Issuance to Subscriber ..... 19
    - 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate ..... 19
    - 4.6.6 Publication of the Renewal Certificate by the CA ..... 19
    - 4.6.7 Notification of Certificate Issuance by the CA to Other Entities ..... 20
  - 4.7 Certificate Re-key ..... 20
    - 4.7.1 Circumstances for Certificate Re-Key ..... 20
    - 4.7.2 Who May Request Certificate Re-key ..... 20

- 4.7.3 Processing Certificate Rekeying Requests ..... 20
- 4.7.4 Notification of Re-key to Subscriber..... 20
- 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate ..... 20
- 4.7.6 Publication of the Re-Keyed Certificate by the CA ..... 20
- 4.7.7 Notification of Certificate Issuance by the CA to Other Entities ..... 20
- 4.8 Certificate Modification ..... 20
  - 4.8.1 Circumstance for Certificate Modification..... 20
  - 4.8.2 Who May Request Certificate Modification ..... 20
  - 4.8.3 Processing Certificate Modification Requests ..... 20
  - 4.8.4 Notification of New Certificate Issuance to Subscriber ..... 20
  - 4.8.5 Conduct Constituting Acceptance of Modified Certificate ..... 20
  - 4.8.6 Publication of the Modified Certificate by the CA ..... 20
  - 4.8.7 Notification of Certificate Issuance by the CA to Other Entities ..... 20
- 4.9 Certificate Revocation and Suspension..... 20
  - 4.9.1 Circumstances for Revocation ..... 21
  - 4.9.2 Who Can Request Revocation..... 21
  - 4.9.3 Procedure for Revocation Request ..... 21
  - 4.9.4 Revocation Request Grace Period..... 21
  - 4.9.5 Time Within which CA Must Process the Revocation Request ..... 21
  - 4.9.6 Revocation Checking Requirement for Relying Parties..... 21
  - 4.9.7 CRL Issuance Frequency..... 21
  - 4.9.8 Maximum Latency for CRLs ..... 21
  - 4.9.9 On-Line Revocation/Status Checking Availability ..... 21
  - 4.9.10 On-Line Revocation Checking Requirements ..... 21
  - 4.9.11 Other Forms of Revocation Advertisements Available..... 21
  - 4.9.12 Special Requirements for Key Compromise..... 21
  - 4.9.13 Circumstances for Suspension ..... 21
  - 4.9.14 Who can Request Suspension ..... 21
  - 4.9.15 Procedure for Suspension Request..... 21
  - 4.9.16 Limits on Suspension Period ..... 21
- 4.10 Certificate Status Services ..... 21
  - 4.10.1 Operational Characteristics ..... 22
  - 4.10.2 Service Availability..... 22
  - 4.10.3 Optional Features ..... 22
- 4.11 End of Subscription..... 22
- 4.12 Key Escrow and Recovery ..... 22

4.12.1	Key Escrow and Recovery Policy and Practices .....	22
4.12.2	Session Key Encapsulation and Recovery Policy and Practices.....	22
5	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS .....	23
5.1	Physical Controls .....	23
5.1.1	Site Location and Construction .....	23
5.1.2	Physical Access .....	23
5.1.2.1	Physical Access for CA Equipment .....	23
5.1.2.2	Physical Access for RA Equipment .....	23
5.1.3	Power and Air Conditioning.....	23
5.1.4	Water Exposures.....	23
5.1.5	Fire Prevention and Protection.....	23
5.1.6	Media Storage .....	23
5.1.7	Waste Disposal .....	23
5.1.8	Off-Site Backup.....	23
5.2	Procedural Controls.....	23
5.2.1	Trusted Roles.....	23
5.2.1.1	CA Administrators .....	23
5.2.1.2	CA Officers (e.g., CMS, RA, Validation and Vetting Personnel) .....	23
5.2.1.3	Operator (e.g., System Administrators/ System Engineers) .....	24
5.2.1.4	Internal Auditors .....	24
5.2.2	Number of Persons Required per Task.....	24
5.2.3	Identification and Authentication for Each Role.....	24
5.2.4	Roles Requiring Separation of Duties .....	24
5.3	Personnel Controls .....	24
5.3.1	Qualifications, Experience, and Clearance Requirements .....	24
5.3.2	Background Check Procedures .....	24
5.3.3	Training Requirements .....	24
5.3.4	Retraining Frequency and Requirements .....	24
5.3.5	Job Rotation Frequency and Sequence.....	24
5.3.6	Sanctions for Unauthorized Actions.....	24
5.3.7	Independent Contractor Requirements.....	24
5.3.8	Documentation Supplied to Personnel .....	24
5.4	Audit Logging Procedures .....	24
5.4.1	Types of Events Recorded.....	24
5.4.1.1	Router and firewall activities log.....	24
5.4.2	Frequency of Processing Log.....	25

- 5.4.3 Retention Period for Audit Log..... 25
- 5.4.4 Protection of Audit Log..... 25
- 5.4.5 Audit Log Backup Procedures ..... 25
- 5.4.6 Audit Collection System (Internal vs. External) ..... 25
- 5.4.7 Notification to Event-Causing Subject..... 25
- 5.4.8 Vulnerability Assessments..... 25
- 5.5 Records Archival..... 25
  - 5.5.1 Types of Records Archived ..... 25
  - 5.5.2 Retention Period for Archive..... 25
  - 5.5.3 Protection of Archive ..... 25
  - 5.5.4 Archive Backup Procedures ..... 25
  - 5.5.5 Requirements for Time-Stamping of Records..... 25
  - 5.5.6 Archive Collection System (Internal or External)..... 25
  - 5.5.7 Procedures to Obtain and Verify Archive Information..... 25
- 5.6 Key Changeover..... 25
- 5.7 Compromise and Disaster Recovery ..... 25
  - 5.7.1 Incident and Compromise Handling Procedures ..... 26
  - 5.7.2 Computing Resources, Software, and/or Data are corrupted ..... 26
  - 5.7.3 Entity Private Key Compromise Procedures..... 26
  - 5.7.4 Business Continuity Capabilities after a Disaster ..... 26
- 5.8 CA or RA Termination ..... 26
- 6 TECHNICAL SECURITY CONTROLS..... 27
  - 6.1 Key Pair Generation and Installation ..... 27
    - 6.1.1 Key Pair Generation ..... 27
      - 6.1.1.1 Subscriber Key Pairs ..... 27
      - 6.1.1.2 CA and subCA Key Pairs..... 27
    - 6.1.2 Private Key Delivery to Subscriber..... 27
    - 6.1.3 Public Key Delivery to Certificate Issuer..... 27
    - 6.1.4 CA Public Key Delivery to Relying Parties ..... 27
    - 6.1.5 Key Sizes..... 27
    - 6.1.6 Public Key Parameters Generation and Quality Checking..... 27
    - 6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)..... 27
  - 6.2 Private Key Protection and Cryptographic Module Engineering Controls ..... 27
    - 6.2.1 Cryptographic Module Standards and Controls ..... 27
    - 6.2.2 Private Key (n out of m) Multi-Person Control ..... 27
    - 6.2.3 Private Key Escrow..... 27

- 6.2.4 Private Key Backup..... 27
- 6.2.5 Private Key Archival ..... 27
- 6.2.6 Private Key Transfer into or from a Cryptographic Module ..... 27
- 6.2.7 Private Key Storage on Cryptographic Module ..... 28
- 6.2.8 Method of Activating Private Key ..... 28
  - 6.2.8.1 CA Administrator Activation ..... 28
  - 6.2.8.2 Offline CAs Private Key..... 28
  - 6.2.8.3 Online CAs Private Keys..... 28
- 6.2.9 Method of Deactivating Private Key..... 28
- 6.2.10 Method of Destroying Private Key ..... 28
- 6.2.11 Cryptographic Module Rating ..... 28
- 6.3 Other Aspects of Key Pair Management..... 28
  - 6.3.1 Public Key Archival ..... 28
  - 6.3.2 Certificate Operational Periods and Key Pair Usage Periods ..... 28
- 6.4 Activation Data ..... 28
  - 6.4.1 Activation Data Generation and Installation ..... 28
  - 6.4.2 Activation Data Protection ..... 28
  - 6.4.3 Other Aspects of Activation Data ..... 28
- 6.5 Computer Security Controls..... 28
  - 6.5.1 Specific Computer Security Technical Requirements ..... 28
  - 6.5.2 Computer Security Rating ..... 28
- 6.6 Lifecycle Technical Controls ..... 29
  - 6.6.1 System Development Controls..... 29
  - 6.6.2 Security Management Controls ..... 29
  - 6.6.3 Lifecycle Security Controls..... 29
- 6.7 Network Security Controls..... 29
  - 6.7.1 Network Segmentation ..... 29
  - 6.7.2 CA Infrastructure Security ..... 29
- 6.8 Time-Stamping..... 29
- 7 CERTIFICATE, CRL, AND OCSP PROFILES ..... 30
  - 7.1 Certificate Profile ..... 30
    - 7.1.1 Version Number(s) ..... 30
    - 7.1.2 Certificate Extensions ..... 30
      - 7.1.2.1 Root CAs ..... 30
      - 7.1.2.2 Subordinate CAs..... 30
      - 7.1.2.3 Subscriber Certificates..... 30

- 7.1.2.4 All Certificates..... 30
- 7.1.3 Algorithm Object Identifiers ..... 30
- 7.1.4 Name Forms ..... 30
  - 7.1.4.1 Encoding..... 30
  - 7.1.4.2 Subject Information – Subscriber Certificates..... 30
  - 7.1.4.3 Subject Information – Root Certificates and Subordinate CA Certificates ..... 30
- 7.1.5 Name Constraints ..... 30
  - 7.1.5.1 E-mail Protection..... 30
- 7.1.6 Certificate Policy Object Identifier ..... 30
- 7.1.7 Usage of Policy Constraints Extension ..... 31
- 7.1.8 Policy Qualifiers Syntax and Semantics ..... 31
- 7.1.9 Processing Semantics for the Critical Certificate Policies Extension ..... 31
- 7.2 CRL Profile ..... 31
  - 7.2.1 Version Number(s) ..... 31
  - 7.2.2 CRL and CRL Entry Extensions ..... 31
- 7.3 OCSP Profile..... 31
  - 7.3.1 Version Number(s) ..... 31
  - 7.3.2 OCSP Extensions ..... 31
- 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS ..... 32
  - 8.1 Frequency or Circumstances of Assessment ..... 32
  - 8.2 Identity/Qualifications of Assessor ..... 32
  - 8.3 Assessor’s Relationship to Assessed Entity ..... 32
  - 8.4 Topics Covered by Assessment..... 32
  - 8.5 Actions Taken as a Result of Deficiency ..... 32
  - 8.6 Communication of Results..... 32
  - 8.7 Self-Audits ..... 32
  - 8.8 Review of delegated parties ..... 32
- 9 OTHER BUSINESS AND LEGAL MATTERS..... 33
  - 9.1 Fees ..... 33
    - 9.1.1 Certificate Issuance or Renewal Fees..... 33
    - 9.1.2 Certificate Access Fees..... 33
    - 9.1.3 Revocation or Status Information Access Fees ..... 33
    - 9.1.4 Fees for Other Services ..... 33
    - 9.1.5 Refund Policy ..... 33
    - 9.1.6 Reissue Policy ..... 33
  - 9.2 Financial Responsibility..... 33

9.2.1	Insurance Coverage .....	33
9.2.2	Other Assets .....	33
9.2.3	Insurance or extended Warranty Coverage.....	33
9.3	Confidentiality of Business Information.....	33
9.3.1	Scope of Confidential Information.....	33
9.3.2	Information Not Within the Scope of Confidential Information .....	33
9.3.3	Responsibility to Protect Confidential Information .....	33
9.3.4	Publication of Certificate Revocation Data.....	33
9.4	Privacy of Personal Information .....	34
9.4.1	Privacy Plan .....	34
9.4.2	Information Treated as Private .....	34
9.4.3	Information not Deemed Private .....	34
9.4.4	Responsibility to Protect Private Information .....	34
9.4.5	Notice and Consent to Use Private Information.....	34
9.4.6	Disclosure Pursuant to Judicial or Administrative Process .....	34
9.4.7	Other Information Disclosure Circumstances .....	34
9.5	Intellectual Property Rights .....	34
9.6	Representations and Warranties .....	34
9.6.1	CA Representations and Warranties .....	34
9.6.2	RA Representations and Warranties .....	34
9.6.3	Subscriber Representations and Warranties .....	34
9.6.4	Relying Party Representations and Warranties .....	34
9.6.5	Representations and Warranties of other Participants .....	34
9.7	Disclaimers of Warranties .....	34
9.7.1	Fitness for a Particular Purpose.....	34
9.7.2	Other Warranties.....	34
9.8	Limitations of Liability .....	35
9.8.1	Damage and Loss Limitations.....	35
9.8.2	Exclusion of Certain Elements of Damages.....	35
9.9	Indemnities.....	35
9.9.1	Indemnification by Sectigo .....	35
9.9.2	Indemnification by Subscriber .....	35
9.9.3	Indemnification by Relying Parties.....	35
9.10	Term and Termination .....	35
9.10.1	Term .....	35
9.10.2	Termination.....	35

- 9.10.3 Effect of Termination and Survival..... 35
- 9.11 Individual Notices and Communications with Participants ..... 35
- 9.12 Amendments ..... 35
  - 9.12.1 Procedure for Amendment ..... 35
  - 9.12.2 Notification Mechanism and Period ..... 35
  - 9.12.3 Circumstances Under Which OID Must be Changed ..... 35
- 9.13 Dispute Resolution Provisions ..... 35
- 9.14 Governing Law, Interpretation, and Jurisdiction..... 36
  - 9.14.1 Governing Law ..... 36
  - 9.14.2 Interpretation..... 36
  - 9.14.3 Jurisdiction..... 36
- 9.15 Compliance with Applicable Law..... 36
- 9.16 Miscellaneous Provisions..... 36
  - 9.16.1 Entire Agreement ..... 36
  - 9.16.2 Assignment ..... 36
  - 9.16.3 Severability ..... 36
  - 9.16.4 Enforcement (Attorneys’ Fees and Waiver of Rights) ..... 36
  - 9.16.5 Force Majeure ..... 36
  - 9.16.6 Conflict of Rules ..... 36
- 9.17 Other Provisions..... 36
  - 9.17.1 Subscriber Liability to Relying Parties ..... 36
  - 9.17.2 Duty to Monitor Agents ..... 36
  - 9.17.3 Ownership..... 36
  - 9.17.4 Interference with Sectigo Implementation..... 36
  - 9.17.5 Choice of Cryptographic Method ..... 36
  - 9.17.6 Sectigo Partnerships Limitations ..... 36
  - 9.17.7 Subscriber Obligations..... 37

## 1 INTRODUCTION

This document defines the business activities performed by PSW GROUP GmbH & Co. KG (PSW GROUP) as Registration Authority (RA) of the Sectigo Web PKI of Sectigo Limited for S/MIME certificates. The Sectigo Web PKI regulates the issuance of S/MIME certificates that are to be trusted on the public Internet.

PSW GROUP acts as a Registration Authority for Sectigo, performing registrations and facilitating the trading of digital certificates under the Sectigo Web PKI.

### 1.1 Overview

PSW GROUP is one of the leading service providers for certificate solutions in Germany. We successfully cooperate with the largest certification authorities worldwide. An important part of PSW GROUP's business activities comprises the registration of organization-validated and sponsor-validated S/MIME certificates. For the Certification Authorities for which we perform these validation activities, we verify the identity of the subscriber/certificate holder, and typically conduct the validation call in German. In accordance with WEBTRUST PRINCIPLES AND CRITERIA FOR REGISTRATION AUTHORITIES, we provide the following information about the services we provide as part of our work for Sectigo.

### 1.2 Document Name and Identification

This document is an addendum by PSW GROUP to the combined S/MIME CP/CPS of Sectigo.

This Addendum specifies additional requirements for Registration Authorities (RAs) acting on behalf of Sectigo. The goal is to ensure compliance with the current WebTrust Principles and Criteria for Registration Authorities, supporting the integrity, traceability, and trustworthiness of registration processes.

PSW GROUP acts in accordance with the current specifications of the CA/B Forum:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates - Link: <https://cabforum.org/working-groups/smime/documents/>
- Network and Certificate System Security Requirements - Link: <https://cabforum.org/working-groups/netsec/documents/>

PSW GROUP complies with the current version of the following WebTrust documents by CPA Canada:

- WebTrust Principles and Criteria for Registration Authorities – Link: <https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria>

And according to the requirements of the Certification Authority (CA) Sectigo including the documents:

- S/MIME Certificate Policy and Certification Practice Statement v1.0.6 - Link: <https://www.sectigo.com/legal>

If any inconsistency exists between this document and the normative provisions of any applicable industry guideline or standard, the industry guideline or standard shall take precedence over this Business Practices Disclosure.

Our Business Practices Disclosure documents address our collaboration with Sectigo in the validation of TLS, S/MIME and Code Signing Certificates.

In sections that do not concern PSW GROUP as RA no stipulation is made to the combined CP/CPS of Sectigo. In these sections, "No stipulation." is noted.

### 1.2.1 Revisions

This document is reviewed at least annually and adopts changes in Sectigo S/MIME CP/CPS in a timely manner.

Document version	Effective Date	Changes
1.0	2025/08/19	Adoption of combined CP/CPS of Sectigo
1.1	2025/11/21	Compliance with Sectigo S/MIME Certificates CP/CPS 1.0.6 – no changes
1.2	2026/04/02	Added 4.2.4.1 for compliance with Sectigo S/MIME CP/CPS 1.0.8

## 1.3 PKI Participants

No stipulation.

### 1.3.1 Certification Authorities

No stipulation.

### 1.3.2 Registration Authorities

PSW GROUP collects and verifies the identity of each Subscriber and the information to be enrolled in the Subscriber's certificate. PSW GROUP performs its function in accordance with the CP/CPS approved by the Policy Authority. PSW GROUP regularly performs the following tasks:

- the registration process
- the identification and authentication process.

PSW GROUP operates locally within its own geographic or business partnerships, subject to approval and authorization by Sectigo, and in accordance with Sectigo's practices and procedures.

PSW GROUP does not itself issue digital certificates, nor does it arrange for their issuance. PSW GROUP registers some or all of the subject's identity information, but does not perform domain control validation.

The RA is responsible for recording all validation steps and maintaining tamper-evident logs of all registration-related actions. The CA reserves the right to audit these logs at any time. All RA staff involved in certificate approvals must be uniquely identified and actions must require dual control (two-person rule) where required by WebTrust.

Sectigo operates a number of intermediate CAs from which it issues certificates for which PSW GROUP has performed the registration process.

#### 1.3.2.1 Internal Registration Authority

No stipulation.

#### 1.3.2.2 External Registration Authority

PSW GROUP acts as an External Registration Authority for Sectigo.

External Registration Authorities must comply with WebTrust for RAs, including maintaining their own documented controls and undergoing independent annual audits. Audit results must be shared with Sectigo and may be required for CA/Browser Forum compliance verification.

### **1.3.3 Subscribers (End Entities)**

No stipulation.

### **1.3.4 Relying Parties**

No stipulation.

### **1.3.5 Other Participants**

No stipulation.

#### **1.3.5.1 Reseller Partners**

No stipulation.

#### **1.3.5.2 EPKI Manager Accounts**

No stipulation.

## **1.4 Certificate Usage**

No stipulation.

### **1.4.1 Appropriate Certificate Uses**

No stipulation.

### **1.4.2 Prohibited Certificate Uses**

No stipulation.

## **1.5 Policy Administration**

No stipulation.

### **1.5.1 Organization Administering the Document**

PSW GROUP is responsible for administering this document.

### **1.5.2 Contact Person**

PSW GROUP can be contacted as follows:

#### **PSW GROUP GmbH & Co. KG**

Flemingstraße 20-22

36041 Fulda

Hessen, Germany

TEL: +49 (0) 661 480 276 10

E-MAIL: [info@psw.de](mailto:info@psw.de)

URL: <https://www.psw-group.de>

Contact information for the Sectigo Policy Authority is provided in the Sectigo CP/CPS documents at [sectigo.com/legal](https://sectigo.com/legal).

### **1.5.2.1 Problem Reporting Address**

No stipulation.

#### **1.5.2.1.1 Revocation Portal**

No stipulation.

#### **1.5.2.1.2 ACME revokeCert**

No stipulation.

1.5.2.1.3 Notifying Us Via Email  
No stipulation.

**1.5.3 Person Determining CP/CPS Suitability for the Policy**  
No stipulation.

**1.5.4 CP/CPS approval procedures**  
No stipulation.

## **1.6 Definitions and Acronyms**

No stipulation.

### **1.6.1 Definitions**

As defined in the Sectigo combined CP/CPS.

### **1.6.2 Acronyms**

As defined in the Sectigo combined CP/CPS.

### **1.6.3 Conventions**

As defined in the Sectigo combined CP/CPS.

## **2 PUBLICATION AND REPOSITORY RESPONSIBILITIES**

Sectigo publishes its documents at <https://www.sectigo.com/legal>. There Sectigo makes available the combined CP/CPS documents, the Subscriber Agreement and the EV Certificate requests in the current version.

### **2.1 Repositories**

PSW GROUP provides links to all relevant documents of the Certification Authorities whose digital certificates are offered by PSW GROUP at <https://www.psw-group.de/downloads>. In particular, all CP, CPS, and Subscriber Agreements of these Certification Authorities are linked there, where possible.

Sectigo documents are alternatively available at <https://www.sectigo.com/legal>.

### **2.2 Publication of Certification Information**

No stipulation.

### **2.3 Time or Frequency of Publication**

The documents are reviewed and updated at least annually, without a fixed date. In the event of relevant changes in the Sectigo CP/CPS or other material changes, this document will be updated and republished.

### **2.4 Access Controls on Repositories**

The documents published in the repository are for public information and are freely accessible.

### **2.5 Accuracy of Information**

PSW GROUP has taken measures to regularly check this information being up to date and to check the content for accuracy. This document will be reviewed at least annually. If Sectigo CP/CPS have relevant changes then this document will be updated accordingly. If information in this document contradicts the CP/CPS of Sectigo, the provisions from the CP/CPS shall apply.

## **3 IDENTIFICATION AND AUTHENTICATION**

No stipulation.

### **3.1 Naming**

No stipulation.

#### **3.1.1 Types of Names**

No stipulation.

#### **3.1.2 Need for Names to be Meaningful**

No stipulation.

#### **3.1.3 Anonymity or Pseudonymity of Subscribers**

No stipulation.

#### **3.1.4 Rules for Interpreting Various Name Forms**

No stipulation.

##### **3.1.4.1 Non ASCII character substitution**

No stipulation.

##### **3.1.4.2 Geographic names**

No stipulation.

#### **3.1.5 Uniqueness of Names**

No stipulation.

#### **3.1.6 Recognition, Authentication, and Role of Trademarks**

No stipulation.

## **3.2 Initial Identity Validation**

No stipulation.

### **3.2.1 Method to Prove Possession of Private Key**

No stipulation.

### **3.2.2 Validation of mailbox authorization or control**

No stipulation.

#### **3.2.2.1 Validating authority over mailbox via domain**

No stipulation.

#### **3.2.2.2 Validating control over mailbox via email**

No stipulation.

#### **3.2.2.3 Validating applicant as operator of associated mail server(s)**

No stipulation.

#### **3.2.2.4 Validating control over mailbox usingACME extensions**

No stipulation.

### **3.2.3 Authentication of Organization Identity**

No stipulation.

### **3.2.3.1 Attribute collection of organization identity**

No stipulation.

### **3.2.3.2 Validation of organization identity**

No stipulation.

### **3.2.3.3 Disclosure of verification sources**

No stipulation.

## **3.2.4 Authentication of Individual Identity**

No stipulation.

### **3.2.4.1 Attribute collection and validation of individual identity**

No stipulation.

## **3.2.5 Non-Verified Subscriber Information**

No stipulation.

## **3.2.6 Validation of Authority**

No stipulation.

## **3.2.7 Criteria for Interoperation**

No stipulation.

## **3.2.8 Reliability of verification sources**

No stipulation.

## **3.3 Identification and Authentication for Re-Key Requests**

No stipulation.

### **3.3.1 Identification and Authentication for Routine Re-Key**

No stipulation.

### **3.3.2 Identification and Authentication for Re-Key after Revocation**

No stipulation.

## **3.4 Identification and Authentication for Revocation Request**

No stipulation.

## **4 CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS**

No stipulation.

### **4.1 Certificate Application**

The requirements for applying for a Sectigo certificate via PSW GROUP can be found for each product on the respective product page at <https://www.psw-group.de>, under the "Validierung" tab. This information is currently available in German.

The specifications in the combined CP/CPS for S/MIME certificates of Sectigo apply.

#### **4.1.1 Who can Submit a Certificate Application**

No stipulation.

##### **4.1.1.1 EPKI Manager Account Holder Certificate Applications**

No stipulation.

##### **4.1.1.2 Reseller Partner Certificate Applications**

No stipulation.

#### **4.1.2 Enrollment Process and Responsibilities**

No stipulation.

### **4.2 Certificate Application Processing**

No stipulation.

#### **4.2.1 Performing Identification and Authentication Functions**

PSW GROUP performs identification and authentication functions, in part, as an RA for Sectigo, in accordance with the specifications of the S/MIME CP/CPS.

This includes:

- Verify the identity of the requester as specified in the combined CP/CPS.
- Verify the authority of the requester and the integrity of the information in the Certificate request as specified in the combined CP/CPS.
- Ask Sectigo to sign a Certificate if all Certificate requirements have been met.

#### **4.2.2 Approval or Rejection of Certificate Applications**

No stipulation.

#### **4.2.3 Time to Process Certificate Applications**

No stipulation.

#### **4.2.4 Certificate Authority Authorization**

No stipulation.

##### **4.2.4.1 DNSSEC Validation of CAA records**

No stipulation.

### **4.3 Certificate Issuance**

No stipulation.

#### **4.3.1 CA Actions during Certificate Issuance**

No stipulation.

## **4.3.2 Notification to Subscriber by the CA of Issuance of Certificate**

PSW GROUP provides the certificate to the Subscriber and notifies the Subscriber via e-mail after confirming that the Subscriber has formally acknowledged their obligations as described in the combined CP/CPS.

## **4.3.3 Refusal to Issue a Certificate**

No stipulation.

## **4.4 Certificate Acceptance**

No stipulation.

### **4.4.1 Conduct Constituting Certificate Acceptance**

No stipulation.

### **4.4.2 Publication of the Certificate by the CA**

No stipulation.

### **4.4.3 Notification of Certificate Issuance by the CA to Other Entities**

No stipulation.

#### **4.4.3.1 Reseller Partner**

No stipulation.

#### **4.4.3.2 EPKI Manager Account Holder**

No stipulation.

## **4.5 Key Pair and Certificate Usage**

No stipulation.

### **4.5.1 Subscriber Private Key and Certificate Usage**

No stipulation.

### **4.5.2 Relying Party Public Key and Certificate Usage**

No stipulation.

## **4.6 Certificate Renewal**

No stipulation.

### **4.6.1 Circumstance for Certificate Renewal**

No stipulation.

### **4.6.2 Who May Request Renewal**

No stipulation.

### **4.6.3 Processing Certificate Renewal Requests**

No stipulation.

### **4.6.4 Notification of New Certificate Issuance to Subscriber**

No stipulation.

### **4.6.5 Conduct Constituting Acceptance of a Renewal Certificate**

No stipulation.

### **4.6.6 Publication of the Renewal Certificate by the CA**

No stipulation.

## **4.6.7 Notification of Certificate Issuance by the CA to Other Entities**

No stipulation.

## **4.7 Certificate Re-key**

No stipulation.

### **4.7.1 Circumstances for Certificate Re-Key**

No stipulation.

### **4.7.2 Who May Request Certificate Re-key**

No stipulation.

### **4.7.3 Processing Certificate Rekeying Requests**

No stipulation.

### **4.7.4 Notification of Re-key to Subscriber**

No stipulation.

### **4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate**

No stipulation.

### **4.7.6 Publication of the Re-Keyed Certificate by the CA**

No stipulation.

### **4.7.7 Notification of Certificate Issuance by the CA to Other Entities**

No stipulation.

## **4.8 Certificate Modification**

No stipulation.

### **4.8.1 Circumstance for Certificate Modification**

No stipulation.

### **4.8.2 Who May Request Certificate Modification**

No stipulation.

### **4.8.3 Processing Certificate Modification Requests**

No stipulation.

### **4.8.4 Notification of New Certificate Issuance to Subscriber**

No stipulation.

### **4.8.5 Conduct Constituting Acceptance of Modified Certificate**

No stipulation.

### **4.8.6 Publication of the Modified Certificate by the CA**

No stipulation.

### **4.8.7 Notification of Certificate Issuance by the CA to Other Entities**

No stipulation.

## **4.9 Certificate Revocation and Suspension**

No stipulation.

#### **4.9.1 Circumstances for Revocation**

No stipulation.

#### **4.9.2 Who Can Request Revocation**

No stipulation.

#### **4.9.3 Procedure for Revocation Request**

No stipulation.

#### **4.9.4 Revocation Request Grace Period**

PSW GROUP processes revocation requests for certificates which have been applied for at PSW GROUP.

Revocation requests for Sectigo certificates are forwarded to Sectigo.

PSW GROUP ensures that the revocation request is made by the organization or individual entity that has made the Certificate application.

#### **4.9.5 Time Within which CA Must Process the Revocation Request**

No stipulation.

#### **4.9.6 Revocation Checking Requirement for Relying Parties**

No stipulation.

#### **4.9.7 CRL Issuance Frequency**

No stipulation.

#### **4.9.8 Maximum Latency for CRLs**

No stipulation.

#### **4.9.9 On-Line Revocation/Status Checking Availability**

No stipulation.

#### **4.9.10 On-Line Revocation Checking Requirements**

No stipulation.

#### **4.9.11 Other Forms of Revocation Advertisements Available**

No stipulation.

#### **4.9.12 Special Requirements for Key Compromise**

No stipulation.

#### **4.9.13 Circumstances for Suspension**

No stipulation.

#### **4.9.14 Who can Request Suspension**

No stipulation.

#### **4.9.15 Procedure for Suspension Request**

No stipulation.

#### **4.9.16 Limits on Suspension Period**

No Stipulation.

### **4.10 Certificate Status Services**

No Stipulation.

## **4.10.1 Operational Characteristics**

No Stipulation.

## **4.10.2 Service Availability**

No Stipulation.

## **4.10.3 Optional Features**

No stipulation.

## **4.11 End of Subscription**

No Stipulation.

## **4.12 Key Escrow and Recovery**

No Stipulation.

### **4.12.1 Key Escrow and Recovery Policy and Practices**

No stipulation.

### **4.12.2 Session Key Encapsulation and Recovery Policy and Practices**

No stipulation.

## **5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS**

No stipulation.

### **5.1 Physical Controls**

PSW GROUP protects equipment and systems used for RA activities through specific measures, and reviews associated risks annually and after significant changes.

#### **5.1.1 Site Location and Construction**

No stipulation.

#### **5.1.2 Physical Access**

No stipulation.

##### **5.1.2.1 Physical Access for CA Equipment**

No stipulation.

##### **5.1.2.2 Physical Access for RA Equipment**

No stipulation.

#### **5.1.3 Power and Air Conditioning**

No stipulation.

#### **5.1.4 Water Exposures**

No stipulation.

#### **5.1.5 Fire Prevention and Protection**

No stipulation.

#### **5.1.6 Media Storage**

No stipulation.

#### **5.1.7 Waste Disposal**

No stipulation.

#### **5.1.8 Off-Site Backup**

No stipulation.

## **5.2 Procedural Controls**

### **5.2.1 Trusted Roles**

PSW GROUP appoints individuals to trusted roles after evaluating their suitability for registration tasks and ensuring process security. Trusted roles are reviewed annually, and status is revoked immediately in the event of changes or a negative suitability assessment.

Individuals in trusted roles are granted access to Sectigo software for the registration process, relevant documentation, and secure areas as necessary.

#### **5.2.1.1 CA Administrators**

No stipulation.

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

No stipulation.

### **5.2.1.3 Operator (e.g., System Administrators/ System Engineers)**

No stipulation.

### **5.2.1.4 Internal Auditors**

No stipulation.

## **5.2.2 Number of Persons Required per Task**

No stipulation.

## **5.2.3 Identification and Authentication for Each Role**

No stipulation.

## **5.2.4 Roles Requiring Separation of Duties**

No stipulation.

## **5.3 Personnel Controls**

No stipulation.

### **5.3.1 Qualifications, Experience, and Clearance Requirements**

No stipulation.

### **5.3.2 Background Check Procedures**

PSW GROUP conducts background checks for all individuals assigned to trusted roles.

### **5.3.3 Training Requirements**

Employee training is conducted and reviewed in accordance with a defined training plan. Separate documented assessments are performed for trusted roles, and passing these assessments is mandatory for appointment to a trusted role.

### **5.3.4 Retraining Frequency and Requirements**

No stipulation.

### **5.3.5 Job Rotation Frequency and Sequence**

No stipulation.

### **5.3.6 Sanctions for Unauthorized Actions**

No stipulation.

### **5.3.7 Independent Contractor Requirements**

No stipulation.

### **5.3.8 Documentation Supplied to Personnel**

No stipulation.

## **5.4 Audit Logging Procedures**

No stipulation.

### **5.4.1 Types of Events Recorded**

No stipulation.

#### **5.4.1.1 Router and firewall activities log**

No stipulation.

## **5.4.2 Frequency of Processing Log**

No stipulation.

## **5.4.3 Retention Period for Audit Log**

No stipulation.

## **5.4.4 Protection of Audit Log**

No stipulation.

## **5.4.5 Audit Log Backup Procedures**

No stipulation.

## **5.4.6 Audit Collection System (Internal vs. External)**

No stipulation.

## **5.4.7 Notification to Event-Causing Subject**

No stipulation.

## **5.4.8 Vulnerability Assessments**

No stipulation.

## **5.5 Records Archival**

No stipulation.

### **5.5.1 Types of Records Archived**

No stipulation.

### **5.5.2 Retention Period for Archive**

No stipulation.

### **5.5.3 Protection of Archive**

No stipulation.

### **5.5.4 Archive Backup Procedures**

No stipulation.

### **5.5.5 Requirements for Time-Stamping of Records**

No stipulation.

### **5.5.6 Archive Collection System (Internal or External)**

No stipulation.

### **5.5.7 Procedures to Obtain and Verify Archive Information**

No stipulation.

## **5.6 Key Changeover**

No stipulation.

## **5.7 Compromise and Disaster Recovery**

No stipulation.

## **5.7.1 Incident and Compromise Handling Procedures**

No stipulation.

## **5.7.2 Computing Resources, Software, and/or Data are corrupted**

No stipulation.

## **5.7.3 Entity Private Key Compromise Procedures**

No stipulation.

## **5.7.4 Business Continuity Capabilities after a Disaster**

No stipulation.

## **5.8 CA or RA Termination**

No stipulation.

## **6 TECHNICAL SECURITY CONTROLS**

No stipulation.

### **6.1 Key Pair Generation and Installation**

#### **6.1.1 Key Pair Generation**

##### **6.1.1.1 Subscriber Key Pairs**

No stipulation.

##### **6.1.1.2 CA and subCA Key Pairs**

No stipulation.

#### **6.1.2 Private Key Delivery to Subscriber**

No stipulation.

#### **6.1.3 Public Key Delivery to Certificate Issuer**

No stipulation.

#### **6.1.4 CA Public Key Delivery to Relying Parties**

No stipulation.

#### **6.1.5 Key Sizes**

No stipulation.

#### **6.1.6 Public Key Parameters Generation and Quality Checking**

No stipulation.

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

No stipulation.

### **6.2 Private Key Protection and Cryptographic Module Engineering Controls**

No stipulation.

#### **6.2.1 Cryptographic Module Standards and Controls**

No stipulation.

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

No stipulation.

#### **6.2.3 Private Key Escrow**

No stipulation.

#### **6.2.4 Private Key Backup**

No stipulation.

#### **6.2.5 Private Key Archival**

No stipulation.

#### **6.2.6 Private Key Transfer into or from a Cryptographic Module**

No stipulation.

## **6.2.7 Private Key Storage on Cryptographic Module**

No stipulation.

## **6.2.8 Method of Activating Private Key**

No stipulation.

### **6.2.8.1 CA Administrator Activation**

No stipulation.

### **6.2.8.2 Offline CAs Private Key**

No stipulation.

### **6.2.8.3 Online CAs Private Keys**

No stipulation.

## **6.2.9 Method of Deactivating Private Key**

No stipulation.

## **6.2.10 Method of Destroying Private Key**

No stipulation.

## **6.2.11 Cryptographic Module Rating**

No stipulation.

## **6.3 Other Aspects of Key Pair Management**

No stipulation.

### **6.3.1 Public Key Archival**

No stipulation.

### **6.3.2 Certificate Operational Periods and Key Pair Usage Periods**

No stipulation.

## **6.4 Activation Data**

No stipulation.

### **6.4.1 Activation Data Generation and Installation**

No stipulation.

### **6.4.2 Activation Data Protection**

No stipulation.

### **6.4.3 Other Aspects of Activation Data**

No stipulation.

## **6.5 Computer Security Controls**

### **6.5.1 Specific Computer Security Technical Requirements**

No stipulation.

### **6.5.2 Computer Security Rating**

No stipulation.

## **6.6 Lifecycle Technical Controls**

### **6.6.1 System Development Controls**

No stipulation.

### **6.6.2 Security Management Controls**

No stipulation.

### **6.6.3 Lifecycle Security Controls**

No stipulation.

## **6.7 Network Security Controls**

No stipulation.

### **6.7.1 Network Segmentation**

No stipulation.

### **6.7.2 CA Infrastructure Security**

No stipulation.

## **6.8 Time-Stamping**

No stipulation.

## **7 CERTIFICATE, CRL, AND OCSP PROFILES**

No stipulation.

### **7.1 Certificate Profile**

No stipulation.

#### **7.1.1 Version Number(s)**

No stipulation.

#### **7.1.2 Certificate Extensions**

No stipulation.

##### **7.1.2.1 Root CAs**

No stipulation.

##### **7.1.2.2 Subordinate CAs**

No stipulation.

##### **7.1.2.3 Subscriber Certificates**

No stipulation.

##### **7.1.2.4 All Certificates**

No stipulation.

#### **7.1.3 Algorithm Object Identifiers**

No stipulation.

#### **7.1.4 Name Forms**

No stipulation.

##### **7.1.4.1 Encoding**

No stipulation.

##### **7.1.4.2 Subject Information – Subscriber Certificates**

No stipulation.

##### **7.1.4.3 Subject Information – Root Certificates and Subordinate CA Certificates**

No stipulation.

###### **7.1.4.3.1 Subject Distinguished Name Fields**

No stipulation.

#### **7.1.5 Name Constraints**

No stipulation.

##### **7.1.5.1 E-mail Protection**

No stipulation.

#### **7.1.6 Certificate Policy Object Identifier**

No stipulation.

## **7.1.7 Usage of Policy Constraints Extension**

No stipulation.

## **7.1.8 Policy Qualifiers Syntax and Semantics**

No stipulation.

## **7.1.9 Processing Semantics for the Critical Certificate Policies Extension**

No stipulation.

## **7.2 CRL Profile**

No stipulation.

### **7.2.1 Version Number(s)**

### **7.2.2 CRL and CRL Entry Extensions**

No stipulation.

## **7.3 OCSP Profile**

No stipulation.

### **7.3.1 Version Number(s)**

No stipulation.

### **7.3.2 OCSP Extensions**

No stipulation.

## **8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS**

All RAs must undergo an annual independent WebTrust for RA assessment, covering all relevant processes and controls.

### **8.1 Frequency or Circumstances of Assessment**

No stipulation.

### **8.2 Identity/Qualifications of Assessor**

No stipulation.

### **8.3 Assessor's Relationship to Assessed Entity**

No stipulation.

### **8.4 Topics Covered by Assessment**

No stipulation.

### **8.5 Actions Taken as a Result of Deficiency**

No stipulation.

### **8.6 Communication of Results**

No stipulation.

### **8.7 Self-Audits**

No stipulation.

### **8.8 Review of delegated parties**

No stipulation.

## **9 OTHER BUSINESS AND LEGAL MATTERS**

No stipulation.

### **9.1 Fees**

No stipulation.

#### **9.1.1 Certificate Issuance or Renewal Fees**

No stipulation.

#### **9.1.2 Certificate Access Fees**

No stipulation.

#### **9.1.3 Revocation or Status Information Access Fees**

No stipulation.

#### **9.1.4 Fees for Other Services**

No stipulation.

#### **9.1.5 Refund Policy**

No stipulation.

#### **9.1.6 Reissue Policy**

No stipulation.

## **9.2 Financial Responsibility**

### **9.2.1 Insurance Coverage**

No stipulation.

### **9.2.2 Other Assets**

No stipulation.

### **9.2.3 Insurance or extended Warranty Coverage**

No stipulation.

## **9.3 Confidentiality of Business Information**

No stipulation.

### **9.3.1 Scope of Confidential Information**

No stipulation.

### **9.3.2 Information Not Within the Scope of Confidential Information**

No stipulation.

### **9.3.3 Responsibility to Protect Confidential Information**

No stipulation.

### **9.3.4 Publication of Certificate Revocation Data**

No stipulation.

## **9.4 Privacy of Personal Information**

### **9.4.1 Privacy Plan**

PSW GROUP follows the specifications of Sectigo and the legal requirements in Germany and the EU.

### **9.4.2 Information Treated as Private**

No stipulation.

### **9.4.3 Information not Deemed Private**

No stipulation.

### **9.4.4 Responsibility to Protect Private Information**

No stipulation.

### **9.4.5 Notice and Consent to Use Private Information**

No stipulation.

### **9.4.6 Disclosure Pursuant to Judicial or Administrative Process**

No stipulation.

### **9.4.7 Other Information Disclosure Circumstances**

No stipulation.

## **9.5 Intellectual Property Rights**

No stipulation.

## **9.6 Representations and Warranties**

### **9.6.1 CA Representations and Warranties**

No stipulation.

### **9.6.2 RA Representations and Warranties**

The RA warrants ongoing compliance with WebTrust for RAs and agrees to immediately inform Sectigo of any incidents that may impact the integrity or trustworthiness of the registration process.

### **9.6.3 Subscriber Representations and Warranties**

No stipulation.

### **9.6.4 Relying Party Representations and Warranties**

No stipulation.

### **9.6.5 Representations and Warranties of other Participants**

No stipulation.

## **9.7 Disclaimers of Warranties**

### **9.7.1 Fitness for a Particular Purpose**

No stipulation.

### **9.7.2 Other Warranties**

No stipulation.

## **9.8 Limitations of Liability**

No stipulation.

### **9.8.1 Damage and Loss Limitations**

No stipulation.

### **9.8.2 Exclusion of Certain Elements of Damages**

No stipulation.

## **9.9 Indemnities**

### **9.9.1 Indemnification by Sectigo**

No stipulation.

### **9.9.2 Indemnification by Subscriber**

No stipulation.

### **9.9.3 Indemnification by Relying Parties**

No stipulation.

## **9.10 Term and Termination**

### **9.10.1 Term**

No stipulation.

### **9.10.2 Termination**

No stipulation.

### **9.10.3 Effect of Termination and Survival**

No stipulation.

## **9.11 Individual Notices and Communications with Participants**

No stipulation.

## **9.12 Amendments**

No stipulation.

### **9.12.1 Procedure for Amendment**

No stipulation.

### **9.12.2 Notification Mechanism and Period**

No stipulation.

### **9.12.3 Circumstances Under Which OID Must be Changed**

No stipulation.

## **9.13 Dispute Resolution Provisions**

No stipulation.

## **9.14 Governing Law, Interpretation, and Jurisdiction**

### **9.14.1 Governing Law**

No stipulation.

### **9.14.2 Interpretation**

No stipulation.

### **9.14.3 Jurisdiction**

No stipulation.

## **9.15 Compliance with Applicable Law**

No stipulation.

## **9.16 Miscellaneous Provisions**

### **9.16.1 Entire Agreement**

No stipulation.

### **9.16.2 Assignment**

No stipulation.

### **9.16.3 Severability**

No stipulation.

### **9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)**

No stipulation.

### **9.16.5 Force Majeure**

No stipulation.

### **9.16.6 Conflict of Rules**

No stipulation.

## **9.17 Other Provisions**

### **9.17.1 Subscriber Liability to Relying Parties**

No stipulation.

### **9.17.2 Duty to Monitor Agents**

No stipulation.

### **9.17.3 Ownership**

No stipulation.

### **9.17.4 Interference with Sectigo Implementation**

No stipulation.

### **9.17.5 Choice of Cryptographic Method**

No stipulation.

### **9.17.6 Sectigo Partnerships Limitations**

No stipulation.

## 9.17.7 Subscriber Obligations

No stipulation.