PSW GROUP

BUSINESS PRACTICES DISCLOSURE

Since the year 2000, well-known companies have relied on the expertise, services and solutions of **PSW GROUP**. During these times we have developed into one of the leading service providers for certificate solutions in Germany. We successfully cooperate with the largest certification authorities worldwide. Our goal is to provide our customers with the best possible service and to offer them exactly the product that meets their requirements.

An important part is the pre-validation of organization-validated and extended validated SSL and Code Signing certificates. For the CAs for which we perform these validation activities, we verify the identity of the subscriber/certificate holder and usually perform the validation call in German. Our customers in the German-speaking countries greatly appreciate this service.

In accordance with Webtrust requirements for Registration Authorities (RA), we provide the following information about the services we provide as part of our work for **Sectigo**. The requirements can be found under the following link:

https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/wt148webtrust-for-ra--110120-finalaoda.pdf?la=en&hash=34D210225C03FC6436FA0074585CA60C0A3DCD91

Our Business Practices Disclosure addresses our collaboration with **Sectigo** in the validation of SSL and code signing certificates.

Sectigo Limited
3rd Floor, Building 26 Exchange Quay
Trafford Road
Salford
Greater Manchester, M5 3EQ
United Kingdom
Email: legalnotices@sectigo.com
Documents: https://sectigo.com/legal

The **PSW GROUP** takes over the verification of the identity of the subscriber for **Sectigo**. We strictly follow **Sectigo**'s guidelines, which are based on the rules of the CA/Browser Forum

Sectigo WebPKI Certificate Policy
Link: https://sectigo.com/legal

Sectigo Certification Practice Statement
Link: https://sectigo.com/legal

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
Link: https://cabforum.org/baseline-requirements-documents/#Current-Version

Network Security Requirements
Link: https://cabforum.org/network-security-requirements/#Current-Version

Guidelines For The Issuance And Management Of Extended Validation Certificates
Link: https://cabforum.org/extended-validation/#Current-Version

Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates
Link: https://cabforum.org/ev-code-signing-certificate-guidelines/#EV-Code-Signing-Certificate-Guidelines

In the following, we provide information about the services and the relevant sections of the certificate policy and the certificate practice statement that are applicable to us and thus comply with the requirements of the WebTrust principles and criteria for Registration Authorities.

OUR VALIDATION PROCESS

Identity of the Organization

1. Checking die organization name and address

A) i. We check whether the organization is registered in a database approved for examination by **Sectigo**. Both the organization name and the address must match completely.
ii. We also check in the allowed data sources if a telephone number is listed. It will be used for the validation call; OR

B) iii. If there is no database entry for the organization, we check the company's entry in the commercial register and look in addition for a telephone directory entry in an approved register.

Identity of the Subscriber

2. Checking the identity of the subscriber

The subscriber must be listed either
i. in the commercial register; or
ii. in an approved database.
iii. Alternatively, the confirmation of the authorization can also be done via a further validation call with the human resources department or management of the organization. This verification must also be made using the telephone number published in an approved database.

Sectigo EV Certificate Request
https://sectigo.com/legal

Sectigo Certificate Subscriber Agreement
https://sectigo.com/legal

STATEMENT

Sectigo Certification Practice Statement
Link: https://sectigo.com/legal

The **PSW GROUP** is a Registration Authority defined as follows in die CPS from **Sectigo**:

We, **PSW GROUP,** maintain effective controls and measures to assure that we provide our services in accordance with the applicable sections of the Certification Authority's Certificate Practice Statement and Certificate Policy for the following CA:

1.6. Definitions and acronyms

1.6.1. Definitions

"Applicant: Means the natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate request.

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

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 WebTrust for CAs requirements.

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://www.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.

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

Certificate Systems: Means the system used by **Sectigo** or a delegated third party in providing identity verification, registration and enrollment, Certificate approval, issuance, validity status, support, and other PKI-related services.

Certificate Transparency: Means the protocol described in RFC 6962 for publicly logging the existence of Transport Layer Security (TLS) certificates as they are issued or observed.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Authority Authorization: Means a DNS domain holder specify one or more CAs authorized to issue certificates for that domain name. This is described in RFC 8659.

Code: A contiguous set of bits that has been or can be digitally signed with a Private Key that corresponds to a Code Signing Certificate

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

Code Signing Certificate: A digital certificate issued by a CA that contains a code Signing EKU, contains the anyExtendedKeyUsage EKU, or omits the EKU extension and is trusted in an Application Software Supplier's root store to sign software objects.
Note: this can be also named as OV Code Signing Certificate

Common Criteria: is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) in a Security Target (ST), and may be taken from Protection Profiles (PPs). It is an international standard (ISO/IEC 15408) for computer security certification

Critical Vulnerability: A system vulnerability that has a CVSS v2.0 score of 7.0 or higher according to the NVD or an equivalent to such CVSS rating (see http://nvd.nist.gov/home.cfm https://nvd.nist.gov/vuln-metrics/cvss), or as otherwise designated as a Critical Vulnerability by the CA or the CA/Browser Forum.

Demand Deposit Account: a deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as: a checking account, a share draft account, or a current account

Domain Contact: Means the Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a 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).

Dual Use Certificate: Dual Use Certificates are identity verified client certificates used as email and identification certificates that are issued through the Certificate Manager software to the end users of the Certificate Manager subscriber. These certificates are used for secure remote access to the subscriber's computer networks by its employees, agents, and contractors as well as providing these individuals with secure email services.

EV Guidelines (EVG): The CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates, published at http://www.cabforum.org

EV Code Signing Certificate: A Code Signing Certificate validated and issued in accordance the EV Code Signing requirements.

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

Grace Period: Means the period during which the Subscriber MUST make a revocation request.

IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

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

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

Precertificate: Means a certificate that is constructed from the certificate to be issued by adding a special critical poison extension for the purpose of submission to a CT log in accordance with RFC 6962

Privacy Policy: Means the latest version of **Sectigo**'s published document titled as such, which describes **Sectigo**'s policies and practices in collecting, using, and safeguarding personal information, and which is accessible at the following website: https://www.sectigo.com/privacy-policy/.

Private Key: Means the key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: Means the key of a key pair that MAY be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Random Value: Means a value specified by **Sectigo** to the Applicant that exhibits at least 112 bits of entropy.

Reliable Method of Communication: Means a method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Means an entity that relies upon the information contained within the Certificate.

Relying Party Agreement: means an agreement between **Sectigo** and a Relying Party that MUST be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference in the Repository.

Repository: Means **Sectigo's** repository, available at *www.sectigo.com/legal*.

Request Token: Means a value derived in a method specified by **Sectigo** which binds a demonstration of control to the Certificate request.

Root CA System: Means a system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.

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

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

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

Subscriber Agreement: Means an agreement that MUST be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the digital Certificate

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

Verified Method of Communication: Method of communication as defined and verified in conformance with Section 11.5 of the EVG

WebTrust for Certification Authorities: Means the current program for CAs located at http://www.webtrust.org/homepage-documents/item27839.aspx.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the FQDNs contained in the Certificate Subject

Wildcard Domain Name: A Domain Name consisting of a single asterisk character followed by a single full stop character (*.) followed by a FQDN

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

1.6.2. Acronyms

AATL: Adobe Approved Trust List
ADN: Authorization Domain Name
BR: Baseline Requirements
CA: Certificate Authority
CAA: Certification Authority Authorization
CA/B (or CAB): Certificate Authority/Browser (Forum)
CMS: Certificate Management System
CPS: Certification Practice Statement
CRL(s): Certificate Revocation List(s)
CSR: Certificate Signing Request
CT: Certificate Transparency
DN: Distinguished Name
DSA: Digital Signature Algorithm
EPKI: Enterprise Public Key Infrastructure Manager
ECDSA: Elliptic Curve Digital Signature Algorithm
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
PA: Policy Authority
PIN: Personal Identification Number

PKI: Public Key Infrastructure
PKIX: Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS: Public Key Cryptography Standard
RA(s): Registration Authority(ies)
RFC: Request for Comments
RSA: Rivest Shamir Adleman
SAN: Subject Alternate Name
SHA: Secure Hash Algorithm
SGC: Server Gated Cryptography
S/MIME: Secure/Multipurpose Internet Mail Extension(s)
SSL: Secure Sockets Layer
TLS: Transport Layer Security
TSA: Time Stamping Authority
UTC: Coordinated Universal Time
URL: Uniform Resource Locator

1.3.2. Registration authorities

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

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

RAs act locally within their own context of geographical or business partnerships on approval and authorization by **Sectigo** in accordance with **Sectigo** practices and procedures.
Sectigo MAY extend the use of RAs for its Web Host Reseller and Enterprise Public Key Infrastructure (EPKI) Manager. Upon successful approval to join the respective programs the Web Host Reseller Subscriber or EPKI Manager Subscriber MAY be permitted to act as an RA on behalf of **Sectigo**. RAs are required to conform to this CPS, the BR and/or the EVG.
RAs do not issue or cause the issuance of Secure Server Certificates. Some RAs MAY be enabled to perform validation of some or all of the subject identity information but are not able to undertake domain control validation.
RAs MAY only undertake their validation duties from pre-approved systems which are identified to the CA by various means that always include but are not limited to the white-listing of the IP address from which the RA operates.

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

1.3.2.2. External Registration Authority

Some resellers, Powered SSL Partners or enterprise customers may be authorized by **Sectigo** to act as external RAs. As such they MAY be granted RA functionality which MAY include the validation of some or all of the subject identity information for Secure Server Certificates. The external RA is obliged to conduct validation in accordance with this CPS, the BR and/or the EVG prior to issuing a Certificate and acknowledges that they have sufficiently validated the Applicant's identity. This acknowledgement may be via an online process (for example by checking the "I have sufficiently validated this application" checkbox when applying for a Certificate), or via API parameters that sufficient validation has taken place prior to **Sectigo** issuing a Certificate.
External RAs do not validate domain control for Secure Server Certificates. This element of the validation of Secure Server Certificates is always performed by **Sectigo's** internal RA as described in this CPS.
Some of these external RAs have their own practice statement for RAs and are duly audited and certified.

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

In addition to the verification of domain control using the procedures listed above in section 3.2.2.1, Sectigo verifies the identity and address of the Applicant in accordance with the *CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* (commonly referred to as the Baseline Requirements) for Secure Server certificates and in accordance with the Code Signing BRs for code signing certificates, using documentation that is provided by, or through communication with at least one of the following:
1. A government agency in the jurisdiction of the Applicant's legal creation, existence or recognition;

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

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

4. An attestation letter;

For the other certificate types, Sectigo MAY use the same documentation (BRs and Code Signing BRs) or additional documentation like the AATL from Adobe.
Sectigo MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address. Alternatively, Sectigo MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that Sectigo determines to be reliable.
If the Subject Identity Information in the certificate is to include a DBA or Trade Name, Sectigo shall verify the Applicant's right to use such DBA/Trade Name using number 1, 2, or 4 above, or:
1. Communication directly with a government agency responsible for the management of such DBAs or trade names, or;
2. A utility bill, bank statement, credit card statement, government issued tax document, or other form of identification that Sectigo determines to be reliable.

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

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

Requirements *For The Issuance And Management Of Publicly Trusted Code Signing Certificates (commonly referred to as Code Signing BR)* as applicable.
Sectigo will verify:

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

For purposes of verifying the Applicant's Legal Existence/Jurisdiction of Incorporation or Registration information Sectigo uses the data sources as published at *https://sectigo.com/legal*.

3.2.2.5. Data source accuracy

All data sources are evaluated for reliability, accuracy, and for their protection from alteration and falsification before they are used for any identification or authentication purposes. Data sources are revalidated in accordance with the CAB Forum BR for secure server or code signing certificates or EVG documentation or other best practices documentation.

3.2.3. Authentication of Individual Identity

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

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

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

In addition to the verification of domain control using the procedures listed above in section 3.2.2.1 of this CPS, if the Applicant is a natural person, Sectigo verifies the identity and address of the Applicant in accordance with the Baseline Requirements (BRs for Secure Server certificates and Code Signing BRs for Code Signing certificates), using:
1. Verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government issued photo ID (passport, driver's license, military ID, national ID or equivalent document type) notary public or equivalent. Such face-to-face verification SHALL be required prior to issuance of a Document Signing Certificate.

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

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

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

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

If the Applicant for a Certificate containing Subject Identity Information is an organization, then Sectigo SHALL use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.
Sectigo MAY use the sources listed in section 3.2.2.2 to verify the Reliable Method of Communication. Provided that a Reliable Method of Communication is used, Sectigo MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that Sectigo deems appropriate.
In addition, Sectigo SHALL establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then Sectigo SHALL NOT accept any certificate requests that are outside this specification. Sectigo SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.4. Identification and Authentication for Revocation Request

Revocation at the Subscriber's request:
The Subscriber must either be in possession of the authentication details (typically username and password) to log in the correspondent site which were used to purchase the Certificate originally OR the Subscriber must be able to send an email to our abuse accounts which will be authenticated in a later stage (for example, this email can be signed with the Private Key associated with the Certificate).
Revocation at the RA's request:
The RA must be in possession of the authentication details used to effect the original Certificate request to the CA.
Revocation at the CA's request: **Sectigo** does not revoke Certificates at the request of other CAs. **Sectigo** can and does revoke Subscriber Certificates for cause as set out in section 4.9 of this CPS, but identification and authentication is not required in these cases.
Sectigo employs the following procedure for authenticating a revocation request:

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

4.1.1.2. Web Host Reseller Partner Certificate Applications

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

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

4.2. Certificate Application Processing

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

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

Sectigo performs the applicable certificate validation procedures and as required verifies the completeness, accuracy and authenticity of the information provided by the Applicant prior to issuing a Certificate. The procedure includes:

- Verifying that the Applicant is permitted to obtain a Certificate under the relevant stipulations of the CP and this CPS.
- For those requests where the Applicant generates its own key pair:
    - Verifying that the Applicant has provided a well-formed, valid certificate signing request, containing a valid signature;
    - Obtaining a Public Key from the Applicant;
- Verifying that the Applicant has executed the Subscriber Agreement;
- Validating that the requested Certificate meets the requirements in section 3.1;
- Performing the validation procedures set out in section 3.2 and the relevant subsections

In the case of a Secure Server Certificate, Sectigo checks the DNS for the existence of a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, as specified in RFC 8659, and in accordance with section 3.2.2.8 of the Baseline Requirements for publicly issued SSL/TLS Certificates.

4.2.1. Performing Identification and Authentication Functions

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

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

Sectigo MAY use the services of a third party to confirm information on a business entity that applies for a digital Certificate. Sectigo accepts confirmation from third party organizations, other third party databases, and government entities.
Sectigo's controls MAY also include trade registry transcripts that confirm the registration of the Applicant company and state the members of the board, the management and directors representing the company.
Sectigo MAY use any means of communication at its disposal to ascertain the identity of an organizational or individual Applicant. Sectigo reserves right of refusal in its absolute discretion.
Sectigo has a system in place which examines subject details, including domain names, for matches or near matches to some known high profile or pre-notified names that may indicate that a certificate is at a higher than normal risk of fraudulent applications being made and in those cases the certificate application is flagged for manual review.

4.2.2. Approval or Rejection of Certificate Applications

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

If the validation of a Certificate application fails, Sectigo rejects the Certificate application. Sectigo reserves its right to reject applications to issue a Certificate to Applicants if, on its own assessment, by issuing a Certificate to such parties the good and trusted name of Sectigo might get tarnished, diminished or have its value reduced and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal.
Applicants whose applications have been rejected may subsequently reapply.
Certificate applications that contain a new gTLD are not approved while the gTLD is still under consideration by ICANN.

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

4.9. Certificate Revocation and Suspension

Revocation of a Certificate is to permanently end the operational period of the Certificate prior to reaching the end of its stated validity period. In other words, upon revocation of a Certificate, the operational period of that Certificate is immediately considered terminated. The serial number of the revoked Certificate will be placed within the CRL and remains on the CRL until sometime after the end of the Certificate's validity period.
Sectigo does not utilize Certificate suspension.

4.9.1. Circumstances for Revocation

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

- The Subscriber requests in writing that the CA revoke the Certificate;
- The Subscriber notifies Sectigo that the original Certificate request was not authorized and does not retroactively grant authorization;
- Sectigo reasonably believes there has been loss, theft, modification, unauthorized disclosure, or other compromise of the Private Key associated with the Certificate;
- Sectigo is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);

Sectigo reasonably believes that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon;

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

- The Subscriber or Sectigo has breached a material obligation under this CPS or the relevant Subscriber Agreement;
- The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the Baseline Requirements;
- Sectigo is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- Sectigo is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- Either the Subscriber's or Sectigo's obligations under this CPS or the relevant Subscriber Agreement are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
-
- There has been a modification of the information pertaining to the Subscriber that is contained within the Certificate;
- Sectigo is made aware of a material change in the information contained in the Certificate, or the information contained in the Certificate is inaccurate;
- A personal identification number, Private Key or password has, or is likely to become known to someone not authorized to use it, or is being or is likely to be used in an unauthorized way
- The Certificate has not been issued in accordance with the policies set out in this CPS;
- The Subscriber has used the Certificate contrary to law, rule or regulation, or Sectigo reasonably believes that the Subscriber is using the Certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The Certificate was issued as a result of fraud or negligence;
- Sectigo is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key, or if there is clear evidence that the specific method used to generate the Private Key was flawed;

- Sectigo right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless Sectigo has made arrangements to continue maintaining the CRL/OCSP Repository; or
- The Certificate, if not revoked, will compromise the trust status of Sectigo.

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

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

4.9.2. Who Can Request Revocation

A Subscriber or another appropriately authorized party can request revocation of a Certificate. An authorized party includes an RA, regardless of whether on behalf of the Subscriber may request revocation through their account. Sectigo MAY revoke a Certificate without receiving a request and without reason. Other parties may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, using the contact details set out in section 1.5.2.1 of this CPS.

5.2. Procedural Controls

5.2.1. Trusted Roles

Trusted roles are assigned by senior members of the management team who decide permissions with signed authorizations being archived.
The list of personnel appointed to trusted roles is maintained and reviewed annually.
The functions and duties performed by persons in trusted roles are distributed so that a lone person cannot subvert the security and trustworthiness of PKI operations. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of Sectigo PKI operations.

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

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

The CA Officer role is responsible for issuing and revoking certificates, the verification of identity, and compliance with the required issuance steps including those defined in this CPS and recording the details of approval and issuance steps taken identity vetting tasks are completed.
CA Officers must identify and authenticate themselves to systems before access is granted. Identification is via a username, with authentication requiring a password and digital Certificate.

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

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

5.2.1.4. Internal Auditors

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

5.3. Personnel Controls

Access to the secure parts of Sectigo's facilities is limited using physical and logical access controls and is only accessible to appropriately authorized individuals filling trusted roles for which they are properly qualified and to which they have been appointed by management.
Sectigo requires that all personnel filling trusted roles are properly trained and have suitable experience before being permitted to adopt those roles.

5.3.1. Qualifications, Experience, and Clearance Requirements

Consistent with this CPS, Sectigo follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties.
The Operator Role is only granted on Sectigo IT systems when there is a specific business need. New Operators are not given full administrator rights until they have demonstrated a detailed knowledge of Sectigo IT systems & policies and that they have reached a suitable skill level satisfactory to the Server Systems Manager/Administrator or CEO. New administrators are closely monitored by the Server Systems Manager/Administrator for the first three months. Where systems allow, administrator access authentication is via a public/Private Key specifically issued for this purpose. This provides accountability of individual administrators and permits their activities to be monitored.
The CA Officer Role is granted certificate issuance privileges only after sufficient training in Sectigo's validation and verification policies and procedures. This training period MUST be at least six months before issuance privileges will be granted for EV SSL or Code Signing certificates.

5.3.2. Background Check Procedures

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

5.3.3. Training Requirements

Sectigo provides suitable training to all staff before they take on a Trusted Role should they not already have the complete skill-set required for that role. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached.
CA Administrators are trained in the operation and installation of CA software.
Operators are trained in the maintenance, configuration, and use of the specific software, operating systems, and hardware systems used by Sectigo. Internal Auditors are trained to proficiency in the general principles of systems and process audit as well as familiarity with Sectigo's policies and procedures.
CA Officers are trained in Sectigo's validation and verification policies and procedures and are required to pass an examination on the applicable information validation and verification requirements.
Sectigo maintains records of who received training.

5.3.4. Retraining Frequency and Requirements

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

5.4.8. Vulnerability Assessments

A vulnerability is a weakness in the organization or in an information system that might be exploited by a threat, with the possibility of causing harm to assets. In order to mitigate the risk or possibility of causing harm to assets, Sectigo performs regular vulnerability assessment by taking a two-pronged approach. Sectigo assesses vulnerabilities by (1) making an assessment of the threats to, impacts on, and the vulnerabilities of assets and the likelihood of their occurrence, and (2) by developing a process of selecting and implementing security controls in order to reduce the risks identified in the risk assessment to an acceptable level. Sectigo routinely performs vulnerability assessments by identifying the vulnerability categories that face an asset. Some of the vulnerability categories that Sectigo evaluates are technical, logical, human, physical, environmental, and operational.
Vulnerability scans are run by Sectigo trusted staff on a weekly schedule. Additional scans are run following system updates, changes, or when deemed necessary.
If a Critical Vulnerability is discovered, not previously addressed, Sectigo will do in the next 96 hours one of the following:

- remediate the Critical Vulnerability
- If not possible in the 96 hours assigned, create and implement a plan to mitigate this Critical Vulnerability
- document the factual basis for which Sectigo thinks that the Critical Vulnerability does not require remediation

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

5.5.1. Types of Records Archived

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

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

5.5.2. Retention Period for Archive

The retention period for archived information depends on the type of information, the information's level of confidentiality, and the type of system the information is stored on.
Sectigo retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof for a term of not less than 7 years after any Certificate based on that documentation ceases to be valid, or as necessary to comply with applicable laws. The retention term begins on the date of expiration or revocation. Copies of Certificates are held, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that Sectigo MAY see fit.
User data backed up from a workstation is retained for a minimum period of 6 months.

Sectigo WebPKI Certificate Policy
Link: https://sectigo.com/legal

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

RAs may only undertake their validation duties from pre-approved systems which are identified to the CA by various means that always include but are not limited to the white-listing of the IP address from which the RA operates.
Sectigo operates a number of intermediate CAs from which it issues certificates for which a Registration Authority has performed some part of the validation. Some of the intermediate CAs are dedicated to the work of a single RA, whilst others are dedicated to the work of multiple related RAs
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.

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.

3.2.2. Authentication of Organization Identity

Requests for CA certificates shall include the CA name, address, and documentation of the existence of the CA. Before issuing CA certificates, an authority for the issuing CA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA.
Verification practices are detailed in the CPS.

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 825 days (domain name or IP address validation for SSL certificates will be set to 398 days or less according to the BRs effective dates), then the subject must be reverified.

3.3.1. Identification and authentication for routine re-key

CA and Subscriber Certificate re-key SHALL follow 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

Requests to revoke a Certificate have different options, for example, MAY be authenticated using that Certificate's Public Key, regardless of whether the associated Private Key has been compromised.
See CPS section 3.4 for the different requirements for the revocation requesters.

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 SHALL be identified in the CPS.
For server certificate applications the maximum age of data used for verification SHALL NOT exceed 825 days and 398 days for Domain or IP Address validation according to the BRs effective dates.

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 SHALL be 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 SHALL be commensurate with the level of threat in the RA equipment environment.

5.1.5. Fire prevention and protection

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

5.1.6. Media storage

CA media SHALL be 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 SHALL be 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 SHALL be consistent with stipulations in Section 5.1.2.

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 frequency, retention, and extent of the backup is determined by the infrastructure team, taking into account the criticality and security requirements of the information. Backup of critical CA software is performed weekly and is stored offsite. Backup of critical business information is performed daily and is stored offsite. Access to backup servers/media is restricted to authorized personnel only. Backup media is regularly tested through restoration to ensure it can be relied on in the event of a disaster. Backup servers/media 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 MUST be free from conflicts of interest that might prejudice the impartiality of Sectigo PKI operations.

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

5.2.1.2. 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.

5.2.3. Identification and authentication for each role

The CA SHALL confirm 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 SHALL include 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 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 SHALL be selected based on loyalty, trustworthiness, and integrity, and SHALL be 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 cross-reference to disqualified directors.

5.3.6. Sanctions for unauthorized actions

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

5.4.8. Vulnerability assessments

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

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.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices specified in this CP have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the WebTrust for Certification Authorities ("WebTrust for CAs") and other industry standards related to the operation of CAs.
A regular audit is performed by an independent external auditor to assess Sectigo's compliancy with the WebTrust for CAs.

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 one year in duration.

8.3. Assessor's relationship to assessed entity

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

8.5. Actions taken as a result of deficiency

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

8.6. Communication of results

The audit requires that Sectigo make the Audit Report available to the public no later than 3 months after of the audit period. Sectigo is not required to make publicly available any general audit finding that does not impact the overall audit opinion.

8.7. Self Audits

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