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/webtrust-principles-and-criteria-for-registration-authorities-v10.pdf

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/uploads/files/WebPKI-COP-v1.0.pdf

Sectigo Certification Practice Statement
Link: https://sectigo.com/uploads/files/Sectigo-CPS-v5.1.7.pdf

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. If a telephone number is listed there, 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/uploads/files/EV-Certificate-Request-short-form-v1.1.pdf
Sectigo Certificate Subscriber Agreement
https://comodoca.my.salesforce.com/sfc/p/#1N000002Ljih/a/1N000000gHyK/v9LCRR6EMgcShpdiZNQxBOv7uR.zhoSpEwalpPruRjs

STATEMENT

Sectigo WebPKI Certificate Policy
Link: https://sectigo.com/uploads/files/WebPKI-COP-v1.0.pdf

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.

Authorized Organizational Representative (AOR): A person (potentially among several) within an organization who is authorized to vouch for person and non-person identities. Any particular AOR is not permanently linked to any particular non-person identity; the CA MUST only ascertain that the AOR is legitimately associated with the organization, and that the AOR is identified as having authority to request certificates for the organization.

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

Baseline Requirements: The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, published at http://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 Status Server (CSS): A trusted entity that provides on-line verification to a relying party of a subject certificate's revocation status, and may also provide additional attribute information for the subject certificate.

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

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

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).

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

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

Grace Period: Means the period during which the Subscriber MUST make a revocation request.
Issuing System: Means a system used to sign Certificates or validity status information.

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

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.

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

Replacement: Requesting the issuance of a new certificate to replace a current valid certificate issued by **Sectigo** without placing a new order.Repository: Means **Sectigo**'s repository, available at https://www.sectigo.com/legal/.

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

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

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

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

Subscriber Agreement: Means an agreement that MUST be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the digital Certificate product type as presented during the product online order process and is available for reference in the Repository.

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

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

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

1.6.2. Acronyms

AICPA: American Institute of Certified Public Accountants
AOR: Authorized Organization Representative
BR: Baseline Requirements
CA: Certificate Authority
CICA: Canadian Institute of Chartered Accountants
PAC: Personal Authentication Certificate
CPS: Certification Practice Statement
CRL(s): Certificate Revocation List(s)
CSR: Certificate Signing Request
CSS: Certificate Status Server
CVC: Content Verification Certificate
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
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

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 some part of the validation has been performed by a Registration Authority. Some of the intermediate CAs are dedicated to the work of a single RA, whilst others are dedicated to the work of multiple related RAs

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

3.2.3. Authentication of Individual Identity

If the Applicant is a natural person, **Sectigo** SHALL verify the Applicant's name, Applicant's address, and the authenticity of the certificate request.

3.2.5. Validation of authority

Before issuing CA certificates or signature certificates that assert organizational authority, **Sectigo** SHALL validate the subscriber's authority to act in the name of the organization. An example of signature certificates that assert organizational authority is code signing certificates

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.

4.3.1. CA actions during Certificate issuance

Upon receiving the request, the CAs/RAs shall:

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

Sectigo's automated systems receive and collate:

- Evidence gathered during the verification process, and/or
- Assertions that the verification has been completed according to the policy and internal documentation that sets out the acceptable means of verifying subject information.

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

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

Certificate issuance by the Root CA SHALL require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation. The correct authentication of verification evidence provided by external RAs is required before that evidence will be considered for Certificate issuance.

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.

5.2.1.4. 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

5.3.2. 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 crossreference to disqualified directors.

5.3.3. Training requirements

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

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

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

Sectigo Certification Practice Statement
Link: https://sectigo.com/uploads/files/Sectigo-CPS-v5.1.7.pdf

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

„**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 (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."

We, **PSW GROUP** („Registration Authority", „RA"), 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:

"3.2.2.2 Authentication of Organization Identity for OV TLS Secure Server, Object 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), 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;

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 Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates 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

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)
- Proof of right to use name
- Proof of existence and organizational status of the Organization
- Subscriber Agreement, signed (if applying out of bands)

3.2.5. Validation of Authority

Validation of authority involves a determination of whether a person has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a Certificate. Validation of authority is dependent on the type of Certificate requested and is performed in accordance with section 3.2.7 of this CPS.

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.

3.2.5.4. EV TLS Server and Code Signing Certificates

The request is verified in accordance with the CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates section 11.5.

3.2.7. Application Validation

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

3.3. Identification and Authentication for Re-Key Requests

Sectigo supports rekeys on:

- Replacement, which is when a Subscriber wishes to change some (or none) of the subject details in an already issued Certificate and may (or may not) also wish to change the key associated with the new Certificate; and
- Renewal, which is when a Subscriber wishes to extend the lifetime of a Certificate which has been issued they may at the same time vary some (or none) of the subject details and may also change the key associated with the Certificate.

In both cases, Sectigo requires the Subscriber to use the same authentication details (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 then the subject must be reverified.

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) which were used to purchase the Certificate originally OR the Subscriber must be able to send an S/MIME email signed with the Private Key associated with the Certificate.

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

Sectigo employs the following procedure for authenticating a revocation request:

- The revocation request must be sent by the administrator contact associated with the Certificate application. Sectigo may, if necessary, also request that the revocation request be made by either / or the organizational contact and billing contact.

- Upon receipt of the revocation request Sectigo will request confirmation from the known administrator out of bands contact details, either by telephone or by fax.
- Sectigo validation personnel will then command the revocation of the Certificate and logging of the identity of validation personnel and reason for revocation will be maintained in accordance with the logging procedures covered in this CPS.

4. CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS

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

The validity period of Sectigo Certificates varies dependent on the Certificate type, but typically, a Certificate will be valid for either 1 year, 2 years, or 3 years. Sectigo reserves the right to, at its discretion, issue Certificates that may fall outside of these set periods.

The following steps describe the milestones to issue a Secure Server Certificate:

1. The Applicant fills out the online request on Sectigo's web site and the Applicant submits the required information: Certificate Signing Request (CSR), e-mail address, common name, organizational information, country code, verification method and billing information.
2. The Applicant accepts the online Subscriber Agreement.
3. The Applicant submits the required information to Sectigo.
4. The Applicant pays the Certificate fees.
5. Sectigo verifies the submitted information using third party databases and Government records
6. Upon successful validation of the application information, Sectigo may issue the Certificate to the Applicant or should the application be rejected, Sectigo will alert the Applicant that the application has been unsuccessful.
7. Renewal is conducted as per the procedures outlined in this CPS and the official Sectigo websites.
8. Revocation is conducted as per the procedures outlined in this CPS.

4.1.1.2. 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 as per section 2.4.1 of this CPS	End Entity Subscriber	Sectigo	Sectigo

Secure Server Certificate - all types as per section 2.4.1 of this CPS	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 Entity Subscriber	**Sectigo**	**Sectigo**

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.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

Sectigo provides notification of Certificate issuance to the following entities by the following means:

Web Host Reseller Partner:
Issued Subscriber Secure Server Certificates applied for through a Web Host Reseller Partner on behalf of the Subscriber are emailed to the administrator contact of the Web Host Reseller Partner account. For Web Host Reseller Partners using the "auto-apply" interface, Web Host Resellers have the added option of collecting an issued Certificate from a Web Host Reseller account specific URL.

EPKI Manager Account Holder:
Issued Subscriber Secure Server Certificates applied for through an EPKI Manager Account are emailed to the administrator contact of the account.

4.7. Certificate Re-Key

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

4.7.1. Circumstances for Certificate Re-Key

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

4.7.2. Who May Request Certificate Re-Key

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

4.7.3. Processing Certificate Re-key Requests

Depending on the circumstances, the procedure to process a Certificate rekey may be the same as issuing a new Certificate. Under other circumstances, **Sectigo** may process a rekey request by having the Subscriber authenticate its identity.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

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

5.2.3. Identification and Authentication for Each Role

All personnel are required to authenticate themselves to CA and RA systems before they may perform the duties of their role involving those systems.

5.2.4. Roles Requiring Separation of Duties

No Trusted Roles can assume any other role, except Operator

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.

5.3.2. 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 crossreference to disqualified directors.

7.1.4.2. Subject Information – Subscriber Certificates

Sectigo represents that it followed the procedure set forth in its Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

Sectigo does not include Domain Names or IP Addresses in a Subject attribute except as specified in Section 3.2.2. of this CPS.

7.1.4.2.2. Subject Distinguished Name Fields

1. commonName If present in serverAuthentication certificates, this field contains a single IP address or FullyQualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension (see above).

2. organizationName If present in serverAuthentication certificates, this field contains the Subject's name and/or DBA as verified under Section 3.2.2.2 or 3.2.2.3.
Sectigo may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", we may use "Company Name Inc." or "Company Name". Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, we may use the subject:organizationName field to convey a natural person Subject's name or DBA.

3. (omitted)

4. streetAddress If present in serverAuthentication certificates, this field contains the Subject's street address information as verified under Section 3.2.2.2 or 3.2.2.3.

5. localityName If present in serverAuthentication certificates, this field contains the Subject's locality information as verified under Section 3.2.2.2 or 3.2.2.3. Where the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(h), the localityName field may contain the Subject's locality and/or state or province information as verified under Section 3.2.2.2 or 3.2.2.3.

6. stateOrProvinceName If present in serverAuthentication certificates, this field contains the Subject's state or province information as verified under Section 3.2.2.2 or 3.2.2.3. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(h), the subject:stateOrProvinceName field may contain the full name of the Subject's country information as verified under Section 3.2.2.2 or 3.2.2.3.

7. postalCode If present in serverAuthentication certificates, this field contains the Subject's zip or postal code information as verified under Section 3.2.2.2 or 3.2.2.3.

8. countryName If present in serverAuthentication certificates, this field contains the Subject's two-letter ISO 3166-1 country code information as verified under Section 3.2.2.2 or 3.2.2.3. If a Country is not represented by an official ISO 3166-1 country code, Sectigo will specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

9. organizationalUnitName Sectigo implements processes that prevent an organizationalUnitName attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the we have verified this information in accordance with Section 3.2.2.2 or 3.2.2.3 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in under Section 3.2.2.2 or 3.2.2.3.

10. EV and EV Codesigning Certificates SHALL also include the following fields as per Section 9.2 of the EVG:

a. Subject Business Category
   i. subject:businessCategory (OID: 2.5.4.15)

b. Subject Jurisdiction of Incorporation or Registration
   i. subject:jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1) (if required)
   ii. subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2) (if required)
   iii. subject:jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)

c. Subject Registration Number i. Subject:serialNumber (OID: 2.5.4.5)

11. Other Subject Attributes If present in serverAuthentication certificates, all other optional attributes, will contain information that has been verified by **Sectigo**. Optional attributes will not contain metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

8.7. Self-Audits
Sectigo performs regular self-audits and audits of Registration Authorities in accordance with Section 8.7 of the Baseline Requirements.

9.6.2. RA Representations and Warranties
A **Sectigo** RA operates under the policies and practices detailed in this CPS and also the associated Web Host Reseller agreement, Powered SSL agreement and EPKI Manager Account agreement. The RA is bound under contract to:

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

This document and the documents to which reference is made are subject to a regular review process.