Business Practices Disclosure

1 INTRODUCTION

1.1 Overview

This document defines the business activities performed by PSW as Registration Authority (RA) of the Sectigo Web PKI of Sectigo Limited. The Sectigo Web PKI regulates the issuance of digital certificates that are to be trusted on the public Internet.

PSW GROUP trades with digital certificates of the Sectigo Web PKI and takes over registrations for Sectigo as Registration Authority of Sectigo.

In doing so, PSW GROUP acts in accordance with the current specifications of the CA/B Forum

- **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-securityrequirements/#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-CodeSigningCertificate-Guidelines

And according to the requirements of the certification authority (CA) Sectigo about the documents

- Sectigo WebPKI Certificate Policy - Link: https://sectigo.com/legal
- Sectigo Certification Practice Statement - Link: https://sectigo.com/legal
- Sectigo WebPKI S/MIME Certificate Practice Statement - Link: https://sectigo.com/legal

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:
WebTrust for Registration Authorities

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

Sectigo Limited
Unit 7, Campus Road, Listerhills Science
Park, Bradford, BD7 1HR, United Kingdom
Email: legalnotices@sectigo.com
Tel: +44 (0) 161 874 7070
Documents: https://sectigo.com/legal

1.2 Document name and identification

This document is the "Business Practice Disclosure" of PSW GROUP as RA of Sectigo. This document, in conjunction with the information provided in 1.1 Overview listed, this document discloses the business practices (i.e., the identification and authentication process related to the binding of the individual subscriber to the certificate) with reference to the relevant provisions of Sectigo's Business Practice Disclosure in Sectigo's Certification Practices Statement. In addition, PSW GROUP discloses with this document its business practices in accordance with the relevant provisions of the Sectigo Business Practices Disclosure in the CA's Certification Policy (if applicable).

In addition, PSW GROUP discloses, where applicable, additional business practices not included in Sectigo's CP and CPS that are relevant activities performed on behalf of Sectigo.

In sections that do not concern PSW GROUP as RA, No Stipulation. is made to CP and CPS of Sectigo. In these sections, "No Stipulation." noted.

1.2.1 Document version

Document version	Changes
09/05/2023	1.1: Added S/MIME CPS
03/05/2024	• 1.1: New location of Sectigo • Update titles of sections 9.2.3 and 9.14 • 1.6.2: replaced by a reference to the Sectigo CPS
03/18/2024	Corrected version 03/05/2024: Corrected date format

1.3 PKI participants

In this section the participants of the Sectigo Web PKI are identified.

1.3.1 Certification Authorities

No Stipulation.

1.3.1.1 Policy Authority

No Stipulation.

1.3.2 Registration authorities

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

- the registration process

- the identification and authentication process.

PSW GROUP acts locally in its own context of geographic or business partnerships upon approval and authorization by Sectigo in accordance with Sectigo's practices and procedures.

PSW GROUP does not issue SSL certificates itself and does not arrange for their issuance. PSW GROUP performs pre-validation of some or all of the subject's identity information, but is not capable of performing domain control validation.

PSW GROUP performs its validation tasks only from pre-approved systems that are identified to Sectigo through various means, which always include, but are not limited to, the white list of the IP address from which PSW GROUP operates.

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

RA PSW GROUP employees: RA PSW GROUP employees are the holders of Trusted Roles according to Sectigo's specifications.

1.3.3 Subscribers

No Stipulation.

1.3.4 Relying parties

No Stipulation.

1.3.5 Other participants

No Stipulation.

1.4 Certificate usage

1.4.1 Appropriate Certificate uses

No Stipulation.

1.4.2 1.4.2 Prohibited Certificate uses

No Stipulation.

1.5 Policy administration

No Stipulation.

1.5.1 Organization administering the document

No Stipulation.

1.5.2 Contact person

PSW GROUP can be contacted as follows:

PSW GROUP GmbH & Co. KG
Flemingstraße 20-22
36041 Fulda
Hesse, Germany

TEL: +49 661 480 276 10
E-MAIL: info@psw.de
URL: https://www.psw-group.de

1.5.3 Person determining CP suitability for the policy

No Stipulation.

1.5.4 CP approval procedures

No Stipulation.

1.6 Definitions and acronyms

1.6.1 Definitions

As defined in the Sectigo CPS.

1.6.2 Acronyms

As defined in the Sectigo CPS.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

PSW GROUP publishes the documents of Sectigo in the download folder of the website. There Sectigo makes available the CP, the CPS, the Subscriber Agreement, the Document Signing CPS, the EV Certificate Request and the Vulnerability Scanning Subscriber Agreement in the current version.

2.1 Repositories

PSW GROUP publishes the documents at https://www.psw-group.de/downloads/. There, the relevant documents are published by all CAs from which PSW GROUP sells digital certificates.

Sectigo documents are alternatively available from Sectigo at www.sectigo.com/legal.

2.2 Publication of certification information

No Stipulation.

2.3 Time or frequency of publication

The documents are updated in the repository when the CAs are reported. In addition, the documents are regularly checked by PSW GROUP for new versions and updated in the repository when new versions are available.

2.4 Access controls on repositories

The documents published in the repository are for public information and are freely accessible. Sectigo has logical and physical access control measures in place to prevent unauthorized changes to the repository.

2.5 Accuracy of Information

PSW GROUP has taken measures to regularly check this information for up-to-dateness and to check the content for accuracy. If these provisions contradict the CP or CPS of Sectigo, the provisions from the CP or CPS shall apply.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

No Stipulation.

3.1.2 Need for names to be meaningful

No Stipulation.

3.1.3 Anonymity or pseudonymity of Subscribers

No Stipulation.

3.1.4 Rules for interpreting various name forms

No Stipulation.

3.1.5 Uniqueness of names

No Stipulation.

3.1.6 Recognition, authentication, and role of trademarks

No Stipulation.

3.2 Initial identity validation

No Stipulation.

3.2.1 Method to prove possession of Private Key

No Stipulation.

3.2.2 Authentication of Organization Identity

No Stipulation.

3.2.3 Authentication of Individual Identity

No Stipulation.

3.2.4 Non-verified Subscriber Information

No Stipulation.

3.2.5 Validation of authority

No Stipulation.

3.2.6 Criteria for interoperation

No Stipulation.

3.3 Identification and authentication for re-key requests

No Stipulation.

3.3.1 Identification and authentication for routine re-key

No Stipulation.

3.3.2 Identification and authentication for re-key after revocation

No Stipulation.

3.4 Identification and authentication for revocation request

No Stipulation.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

No Stipulation.

4.1 Certificate Application

The conditions required to apply for a Sectigo certificate with PSW GROUP can be viewed in each case on the product page of the website www.psw-group.de under "Validation".

4.1.1 Who can submit a Certificate application

No Stipulation.

4.1.2 Enrollment process and responsibilities

No Stipulation.

4.2 Certificate application processing

No Stipulation.

4.2.1 Performing identification and authentication functions

PSW GROUP takes over the identification and authentication functions partly as RA from Sectigo according to the specifications from the CPS.

4.2.2 Approval or rejection of certificate applications

No Stipulation.

4.2.3 Time to process Certificate applications

No Stipulation.

4.3 Certificate issuance

4.3.1 CA actions during Certificate issuance

PSW GROUP takes over the tasks of an RA for Sectigo certificate applications.

This includes:

- Verify the identity of the requester as specified in Section 3.2 in the CP.
- Verify the authority of the requester and the integrity of the information in the Certificate request as specified in Section 4.1 in the CP.
- Have Sectigo sign a Certificate if all Certificate requirements have been met.
- Make the Certificate available to the Subscriber after confirming that the Subscriber has formally acknowledged their obligations as described in Section 9.6.3 in the CP.

4.3.2 Notification to Subscriber by the CA of issuance of Certificate

No Stipulation.

4.3.3 Refusal to Issue a Certificate

No Stipulation.

4.4 Certificate acceptance

No Stipulation.

4.4.1 Conduct constituting Certificate acceptance

No Stipulation.

4.4.2 Publication of the Certificate by the CA

No Stipulation.

4.4.3 Notification of Certificate issuance by the CA to other entities

No Stipulation.

4.5 Key pair and Certificate usage

4.5.1 Subscriber Private Key and Certificate usage

No Stipulation.

4.5.2 Relying party Public Key and Certificate usage

No Stipulation.

4.6 Certificate renewal

No Stipulation.

4.6.1 Circumstance for Certificate renewal

No Stipulation.

4.6.2 Who MAY request renewal

No Stipulation.

4.6.3 Processing Certificate renewal requests

No Stipulation.

4.6.4 Notification of new Certificate issuance to Subscriber

No Stipulation.

4.6.5 Conduct constituting acceptance of a renewal Certificate

No Stipulation.

4.6.6 Publication of the renewal Certificate by the CA

No Stipulation.

4.6.7 Notification of Certificate issuance by the CA to other entities

No Stipulation.

4.7 Certificate re-key

No Stipulation.

4.7.1 Circumstance for Certificate re-key

No Stipulation.

4.7.2 Who MAY request certification of a new Public Key

No Stipulation.

4.7.3 Processing Certificate re-keying requests

No Stipulation.

4.7.4 Notification of new Certificate issuance to Subscriber

No Stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed Certificate

No Stipulation.

4.7.6 Publication of the re-keyed Certificate by the CA

No Stipulation.

4.7.7 Notification of Certificate issuance by the CA to other entities

No Stipulation.

4.8 Certificate modification

No Stipulation.

4.8.1 Circumstance for Certificate modification

No Stipulation.

4.8.2 Who MAY request Certificate modification

No Stipulation.

4.8.3 Processing Certificate modification requests

No Stipulation.

4.8.4 Notification of new Certificate issuance to Subscriber

No Stipulation.

4.8.5 Conduct constituting acceptance of modified Certificate

No Stipulation.

4.8.6 Publication of the modified Certificate by the CA

No Stipulation.

4.8.7 Notification of Certificate issuance by the CA to other entities

No Stipulation.

4.9 Certificate revocation and suspension

No Stipulation.

4.9.1 Circumstances for revocation

No Stipulation.

4.9.2 Who can request revocation

No Stipulation.

4.9.3 Procedure for revocation request

PSW GROUP accepts revocation requests for certificates which have been applied for at PSW GROUP. Revocation requests for Sectigo certificates are forwarded to Sectigo.

4.9.4 Revocation request grace period

No Stipulation.

4.9.5 Time within which CA MUST process the revocation request

No Stipulation.

4.9.6 Revocation checking requirement for relying parties

No Stipulation.

4.9.7 CRL issuance frequency (if applicable)

No Stipulation.

4.9.8 Maximum latency for CRLs (if applicable)

No Stipulation.

4.9.9 On-line revocation/status checking availability

No Stipulation.

4.9.10 On-line revocation checking requirements

No Stipulation.

4.9.11 Other forms of revocation advertisements available

No Stipulation.

4.9.12 Special requirements related to key compromise

No Stipulation.

4.9.13 Circumstances for suspension

No Stipulation.

4.9.14 Who can request suspension

No Stipulation.

4.9.15 Procedure for suspension request

No Stipulation.

4.9.16 Limits on suspension period

No Stipulation.

4.10 Certificate status services

4.10.1 Operational characteristics

No Stipulation.

4.10.2 Service availability

No Stipulation.

4.10.3 Optional features

No Stipulation.

4.11 End of subscription

No Stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

No Stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

No Stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

No Stipulation.

5.1.1 Site location and construction

No Stipulation.

5.1.2 Physical access

5.1.2.1 Physical Access for CA Equipment

No Stipulation.

5.1.2.2 Physical Access for RA Equipment

PSW GROUP protects equipment and systems for RA activity through special measures and reviews risks annually and after major changes.

5.1.3 Power and air conditioning

No Stipulation.

5.1.4 Water exposures

No Stipulation.

5.1.5 Fire prevention and protection

No Stipulation.

5.1.6 Media storage

No Stipulation.

5.1.7 Waste disposal

No Stipulation.

5.1.8 Off-site backup

No Stipulation.

5.2 Procedural controls

5.2.1 Trusted roles

No Stipulation.

5.2.1.1 CA Administrators

No Stipulation.

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

No Stipulation.

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

No Stipulation.

5.2.1.4 Internal Auditors

No Stipulation.

5.2.1.5 RA Staff

No Stipulation.

5.2.2 Number of persons required per task

No Stipulation.

5.2.3 Identification and authentication for each role

No Stipulation.

5.2.4 Roles requiring separation of duties

No Stipulation.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

No Stipulation.

5.3.2 Background check procedures

PSW GROUP performs background checks for all Trusted Roles holders.

5.3.3 Training requirements

Training for employees is conducted and reviewed according to a training plan. Separate documented checks are performed for Trusted Roles.

5.3.4 Retraining frequency and requirements

No Stipulation.

5.3.5 Job rotation frequency and sequence

No Stipulation.

5.3.6 Sanctions for unauthorized actions

No Stipulation.

5.3.7 Independent contractor requirements

No Stipulation.

5.3.8 Documentation supplied to personnel

No Stipulation.

5.4 Audit logging procedures

No Stipulation.

5.4.1 Types of events recorded

No Stipulation.

5.4.2 Frequency of processing log

No Stipulation.

5.4.3 Retention period for audit log

No Stipulation.

5.4.4 Protection of audit log

No Stipulation.

5.4.5 Audit log backup procedures

No Stipulation.

5.4.6 Audit collection system (internal vs. external)

No Stipulation.

5.4.7 Notification to event-causing subject

No Stipulation.

5.4.8 Vulnerability assessments

No Stipulation.

5.5 Records archival

No Stipulation.

5.5.1 Types of records archived

No Stipulation.

5.5.2 Retention period for archive

No Stipulation.

5.5.3 Protection of archive

No Stipulation.

5.5.4 Archive backup procedures

No Stipulation.

5.5.5 Requirements for time-stamping of records

No Stipulation.

5.5.6 Archive collection system (internal or external)

No Stipulation.

5.5.7 Procedures to obtain and verify archive information

No Stipulation.

5.6 Key changeover

No Stipulation.

5.7 Compromise and disaster recovery

No Stipulation.

5.7.1 Incident and compromise handling procedures

No Stipulation.

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

No Stipulation.

5.7.3 Entity Private Key compromise procedures

No Stipulation.

5.7.4 Business continuity capabilities after a disaster

No Stipulation.

5.8 CA or RA termination

No Stipulation.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

No Stipulation.

6.1.2 Private key delivery to Subscriber

No Stipulation.

6.1.3 Public key delivery to Certificate issuer

No Stipulation.

6.1.4 CA Public Key delivery to relying parties

No Stipulation.

6.1.5 Key sizes

No Stipulation.

6.1.6 Public key parameters generation and quality checking

No Stipulation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

No Stipulation.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

No Stipulation.

6.2.2 Private key (n out of m) multi-person control

No Stipulation.

6.2.3 Private key escrow

No Stipulation.

6.2.4 Private key backup

No Stipulation.

6.2.5 Private key archival

No Stipulation.

6.2.6 Private key transfer into or from a cryptographic module

No Stipulation.

6.2.7 Private key storage on cryptographic module

No Stipulation.

6.2.8 Method of activating Private Key

No Stipulation.

6.2.8.1 CA Administrator Activation

No Stipulation.

6.2.8.2 Offline CAs Private Key

No Stipulation.

6.2.8.3 Online CAs Private Keys

No Stipulation.

6.2.8.4 Device Private Keys

No Stipulation.

6.2.9 Method of deactivating private key

No Stipulation.

6.2.10 Method of destroying Private Key

No Stipulation.

6.2.11 Cryptographic Module Rating

No Stipulation.

6.3 Other aspects of key pair management

6.3.1 Public key archive

No Stipulation.

6.3.2 Certificate operational periods and key pair usage periods

No Stipulation.

6.4 Activation data

No Stipulation.

6.4.1 Activation data generation and installation

No Stipulation.

6.4.2 Activation data protection

No Stipulation.

6.4.3 Other aspects of activation data

No Stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

No Stipulation.

6.5.2 Computer security rating

No Stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

No Stipulation.

6.6.2 Security management controls

No Stipulation.

6.6.3 Life cycle security controls No Stipulation.

6.7 Network security controls

No Stipulation.

6.8 Time stamping

No Stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

No Stipulation.

7.1.1 Version number(s)

No Stipulation.

7.1.2 Certificate extensions

No Stipulation.

7.1.3 Algorithm object identifiers

No Stipulation.

7.1.4 Name forms

No Stipulation.

7.1.5 Name constraints

No Stipulation.

7.1.6 Certificate policy object identifier

No Stipulation.

7.1.7 Usage of Policy Constraints extension

No Stipulation.

7.1.8 Policy qualifiers syntax and semantics

No Stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No Stipulation.

7.2 CRL profile

No Stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

No Stipulation.

8.1 8.1 Frequency or circumstances of assessment

No Stipulation.

8.2 8.2 Identity/qualifications of assessor

No Stipulation.

8.3 Assessor's relationship to assessed entity

No Stipulation.

8.4 Topics covered by assessment

No Stipulation.

8.5 Actions taken as a result of deficiency

No Stipulation.

8.6 Communication of results

No Stipulation.

8.7 Self audits

No Stipulation.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No Stipulation.

9.1.1 Certificate issuance or renewal fees

No Stipulation.

9.1.2 Certificate access fees

No Stipulation.

9.1.3 Revocation or status information access fees

No Stipulation.

9.1.4 Fees for other services

No Stipulation.

9.1.5 Refund policy

No Stipulation.

9.2 Financial responsibility

9.2.1 Insurance coverage

No Stipulation.

9.2.2 Other assets

No Stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No Stipulation.

9.3 Confidentiality of business information

No Stipulation.

9.3.1 Scope of confidential information

No Stipulation.

9.3.2 Information not within the scope of confidential information

No Stipulation.

9.3.3 Responsibility to protect confidential information

No Stipulation.

9.4 Privacy of personal information

9.4.1 Privacy plan

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

9.4.2 Information treated as private

No Stipulation.

9.4.3 Information not deemed private

No Stipulation.

9.4.4 Responsibility to protect private information

No Stipulation.

9.4.5 Notice and consent to use private information

No Stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No Stipulation.

9.4.7 Other information disclosure circumstances

No Stipulation.

9.5 Intellectual property rights

No Stipulation.

9.6 Representations and warranties

9.6.1 CA representations and warranties

No Stipulation.

9.6.2 RA representations and warranties

No Stipulation.

9.6.3 Subscriber representations and warranties

No Stipulation.

9.6.4 Relying party representations and warranties

No Stipulation.

9.6.5 Representations and warranties of other participants

No Stipulation.

9.7 Disclaimers of warranties

9.7.1 Fitness for a Particular Purpose

No Stipulation.

9.7.2 Other Warranties

No Stipulation.

9.8 Limitations of liability

No Stipulation.

9.8.1 Damage and Loss Limitations

No Stipulation.

9.8.2 Exclusion of Certain Elements of Damages

No Stipulation.

9.9 Indemnities

9.9.1 Indemnification by Sectigo

No Stipulation.

9.9.2 Indemnification by Subscriber

No Stipulation.

9.9.3 Indemnification by Relying Parties

9.10 Term and termination

9.10.1 Term

No Stipulation.

9.10.2 Termination

No Stipulation.

9.10.3 Effect of termination and survival

No Stipulation.

9.11 Individual notices and communications with participants

No Stipulation.

9.12 Amendments

No Stipulation.

9.12.1 Procedure for amendment

No Stipulation.

9.12.2 Notification mechanism and period

No Stipulation.

9.12.3 Circumstances under which OID MUST be changed

No Stipulation.

9.13 Dispute resolution provisions

No Stipulation.

9.14 Governing law

9.14.1 Governing Law

No Stipulation.

9.14.2 Interpretation

No Stipulation.

9.14.3 Jurisdiction

No Stipulation.

9.15 Compliance with applicable law

No Stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No Stipulation.

9.16.2 Assignment

No Stipulation.

9.16.3 Severability No Stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No Stipulation.

9.16.5 Force Majeure

No Stipulation.

9.16.6 Conflict of Rules

No Stipulation.

9.17 Other provisions

9.17.1 Subscriber Liability to Relying Parties No Stipulation.

9.17.2 Duty to Monitor Agents

No Stipulation.

9.17.3 Ownership

No Stipulation.

9.17.4 Interference with Sectigo Implementation

No Stipulation.

9.17.5 Choice of Cryptographic Method

No Stipulation.

9.17.6 Sectigo Partnerships Limitations

No Stipulation.

9.17.7 Subscriber obligations

No Stipulation.