Sectigo eIDAS PKI Disclosure Statement

Sectigo
Version 1.3
Effective: August 29, 2025
Rambla Catalunya, 86 3 1,
08008 Barcelona, Spain
www.sectigo.com

SECTIGO

Contents

Introduction

This document is the Sectigo´s PKI Disclosure Statement (PDS).

This declaration is not a substitute for the combined CP/CPS (Certificate Policy/Certification Practice Statement) of Sectigo under which digital certificates are issued by Sectigo. The CP/CPS of Sectigo is available at https://sectigo.com/legal and https://sectigo.com/eidascps

The PKI Disclosure Statement summarizes the terms and conditions of the certification services offered by Sectigo in a more readable and understandable format for the benefit of our subscribers and relying parties.

Qualified certificates are certificates issued in accordance with the eIDAS regulation: "eIDAS Regulation (eIDAS)" means REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Certificates issued in accordance with the eIDAS regulation are issued by Sectigo.

Contact info

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

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

  Sectigo
  Attention: Legal Practices,
  Unit 7, Campus Road, Listerhills Science Park, Bradford, BD7 1HR, United Kingdom
  Tel: +44 (0) 161 874 7070

Certificate type, validation procedure and usage of certificates

Sectigo issues qualified certificates (including PSD2) that enable identifying the subscriber who uses them to create an electronic signature or seal or to protect the communication between a subscriber and a web site.

Sectigo validates the information and supporting documents comprising the certification request sent by the subscriber. The identity verification of the future subscriber occurs via a physical face-to-face meeting, or a method known to be equivalent for issuing certificates in compliance with the latest version of the ETSI EN 319 411-2:

- legal persons, level QCP-l, QCP-l-qscd or QEVCP-w (QCP-w-psd2 optionally for PSD2)
- Natural persons, level QCP-n, QCP-n-qscd or QNCP-w

The identifiers of the different certificate policies are specified in specific documents with the certificate profiles.

Limits of use of the certificate

Sectigo cannot be held liable for any use of the certificate that does not comply with the CP/CPS.

The certificates are not designed, provided or combined with any authorization to use them in any context other than those defined by the CP/CPS, i.e. as an electronic signature and/or an electronic seal.

The certificates issued by Sectigo cannot be used as identity proof within the meaning of Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 (amended by regulation 1183/2024 of May 20th, 2024).

Sectigo is not responsible for evaluating the appropriate nature of use of a certificate.

Additional limits of use may be defined by the subscriber agreement signed between Sectigo and the subscriber or by the relying party agreement.

Obligations of subscribers

The subscriber acknowledges that it has all the necessary information before using its certificate.

The subscriber pledges to:

- provide a registration file with accurate and complete information;
- immediately inform Sectigo if the information contained in the registration file and/or the certificate is incorrect and/or modified;
- only use the key pair in accordance with any limitations notified to subscriber, and the subject if the subject is a natural or legal person;
- adopt suitable measures to prevent unauthorized use of the private key;
- when the subject is a natural and/or legal person, maintain the private key under the subject's personal control;
- notify Sectigo immediately if any of the following occur, up to the end of the validity period indicated in the certificate:
    - if the private key has been lost, stolen, or potentially compromised;

    - control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons;
    - inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject;
- following the compromise of the subject's private key, immediately and permanently discontinue the use of the key, except for key decipherment;
- in the case of being informed that the subject's certificate has been revoked, or that the issuing CA has been compromised, ensure that the private key is no longer used by the subject
- where applicable, hold the intellectual property rights on the information transmitted in the registration file;
- use the certificate only for the purposes authorised by the CP/CPS, by the relying party agreement and by the regulations applicable in general;
- comply with all the requirements defined by the CP/CPS and especially generate and use cryptographic keys in a device and with algorithms that comply with the CP/CPS;
- refrain from reverse-engineering or attempting to take control of the software tools used by Sectigo in the context of the certification service;
- ensure the security of its authentication means in order to prevent the use of the key pair by unauthorised third parties; it particularly pledges to take all measures necessary to guarantee the confidentiality of the key pair activation means and to implement all measures for keeping the key pair under the exclusive control of authorised persons, where applicable.

Additional obligations may be defined by the subscriber agreement signed between Sectigo and the subscriber.

Obligations of relying parties

The relying parties are required to ensure the appropriate use of the information contained in the certificates, especially by:

- verifying the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying party;
- take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or the terms and conditions supplied;
- verifying the consistency between their requirements and the conditions and limits of use of the certificate defined by the relying party agreement and by the CP/CPS;
- verifying whether the certificate is compliant with legal, regulatory or normative requirements required for the desired use;
- verifying the status of the certificate that they wish to use, as well as the validity of all certificates of the chain of trust;
- using the appropriate software and hardware for verifying the validity of the signatures or seals associated with the certificates;

- ensuring the conditions and limits of use of the electronic signatures or electronic seals associated with the certificates;
- take any other precautions prescribed in agreements or elsewhere.

Certificate status checking by relying parties

An information service provided by Sectigo enables:

- using the OCSP (Online Certificate Status Protocol) to verify the status of a certificate;
- using the certificate revocation lists of the CA.

Under normal operation, it is available 24/7 pursuant to the conditions defined by the CP/CPS.

The service allows obtaining information on the revocation of certificates of levels QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd, QNCP-w and QEVCP-w even after their expiry. In case of the discontinuation of the TSP ’s activity, the obligations related to the provision of information on the certificate status are transferred in accordance with the stipulations of the CP/CPS.

The Certificate Revocation Lists (CRLs) can be downloaded from the Sectigo´s site. The CRLs (Certificate Revocation Lists) are compliant with standard IETF RFC 5280. The information required for using the OCSP protocol to verify the status of certificates is contained in the certificate fields and their extensions. The protocol is implemented as per standard IETF RFC 6960.

Limited warranty and limitations of liabilities

For warranty and liability limitations, please refer to the provisions of the eIDAS Service Portal Terms and Conditions and the CP/CPS (in particular, see Subscriber Agreement Sections 13-14 and CP/CPS Sections 9.7 - 9.9).

Applicable documentation

The applicable documents are published at https://sectigo.com/legal and https://sectigo.com/eidascps

Privacy policy

Sectigo complies with the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the Sectigo Privacy Policy at https://sectigo.com/privacy-policy. All records relating to certificates and qualified time-stamps issued by Sectigo (e.g. evidence of the identity of subscribers; certificate issuance requests, including acceptance of the terms and conditions; certificate revocation requests; etc.) are retained by Sectigo for fifteen (15) years.

Refund policy

Sectigo´s refund policy is defined in the correspondent clause of the CP/CPS and offers a 30-day period (beginning when a certificate is first issued) in where the subscriber may request a full refund for their certificates.

Applicable law, complaints and dispute resolution

Complaints from customers or other parties related to Sectigo qualified certificates or any services provided in respect to these certificates will be handled without any unreasonable delay and the complaining party will receive an answer to the complaint within 14 calendar days from reception of the complaint.

In case of a dispute arising, the parties shall try to settle the dispute through negotiations and conciliation.

Sectigo repository, trust marks and audit

Sectigo and their CAs are regularly audited for compliance with the requirements stated in ETSI EN 319 411-2 by an accredited body in accordance with standard ETSI EN 319 403 when related to certificates issued according to Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 (amended by regulation 1183/2024 of May 20th, 2024).