Sectigo eIDAS PKI Disclosure Statement

Sectigo
Version 1.1
Rambla Catalunya, 86 3 1,
08008 Barcelona, Spain
www.sectigo.com

Copyright Notice

Sectigo
Rambla Catalunya, 86 3 1,
08008 Barcelona, Spain

Contents

Introduction

This document is the Sectigo´s PKI Disclosure Statement (PDS).
This declaration is not a substitute for the Certification Policy (CP) or for the Certification Practice Statement (CPS) of Sectigo. The CP and the CPS of Sectigo are available at https://sectigo.com/legal

The PKI Disclosure Statement summarises 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.

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 Ltd.
  Attention: Legal Practices,
  3rd Floor, Building 26 Exchange Quay, Trafford Road
  Salford, Greater Manchester, M5 3EQ, United Kingdom
  Tel: + 44(0) 161 874 7070
  Fax: + 44(0) 161 877 1767

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 EN 319 411-2 level QCP-l, QCP-n or QCP-w.

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 authorisation to use them in any context other than those defined by the Certification Policy, i.e. as an electronic signature and/or an electronic seal.
The certificates issued by Sectigo cannot be used as identity proof or as a means of electronic identification within the meaning of Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014.
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 information;
- immediately inform Sectigo if the information contained in the registration file and/or the certificate is incorrect and/or modified;
- 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 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.

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 and QCP-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

Except for the guarantees expressly defined in the relying party agreement applicable to the relying parties and those defined in the subscriber agreement applicable to the subscriber, all other express or implicit guarantees are not applicable, especially any guarantee of suitability for a specific use or of compliance with special requirements of the relying parties and the subscribers.
Therefore, the provision of the certification service does not discharge the subscriber and the relying parties from analysing and verifying the legal or regulatory requirements applicable to it.

Sectigo cannot be held liable:

- in case of an unauthorised or non-compliant use (with the legal and contractual requirements) of the certificates, the revocation information as well as the

equipment or software made available for the provision of the certification service.
- for any damages resulting from errors or inaccuracies in the information contained in the certificates, when these errors or inaccuracies result directly from the erroneous nature of the information communicated by the subscriber.
- under any circumstance in case of any use that is not compliant with the uses defined in the CP/CPS or in the relying party agreement.
- under any circumstance in case of breach of obligations by the Subscriber and/or the Relying Parties.
- for indirect damages resulting from the use of a certificate.

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

Applicable documentation

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

Privacy policy

The privacy policy is published at https://sectigo.com/privacy-policy

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 the 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 EN 319 411-2 by an accredited body in accordance with standard 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.