SECTIGO

Sectigo Digital Certificate APIs

An Overview

Sectigo offer a series of HTTPS POST-based APIs that are incredibly simple to work with to provision and manage all types of digital certificate. They can be used from any language or script which can perform a HTTPS POST request, and can even be tested from simple HTML forms.

All available types of certificates can be requested and provisioned via these APIs, allowing you to offer a completely custom interface to your users, or to integrate the provisioning of certificates into existing systems and workflows.

All aspects of the certificate lifecycle can be performed using the APIs - request and issuance, validation, re-issuance/re-keying, revocation.

A number of 'helper' APIs are also provided to assist with other aspects of the certificate provisioning process - CSR decoders, DCV (Domain Control Validation) APIs, management of multi-domain certificates, and reporting APIs.

Sectigo also offer a 'push' mechanism for updating callers on the status of requested certificates, whereby the Sectigo system will make a call to a specified endpoint via HTTP(S) when a certificate changes state. This can also include the full, signed certificate and certificate chain once issued.

SSL/TLS Server Certificates

Sectigo offers a complete range of SSL server certificates - single domain, wildcard and multi-domain - in all industry-allowed validation options of DV, OV and EV. These certificates can be requested, collected and fully managed via our APIs.

Each API has a specific function, and a list of the most common APIs and their function can be found below.

DecodeCSR
This API can be used to verify and decode a CSR (Certificate Signing Request) and extract information from within it. While there are many pieces of software and libraries available to do this, our API uses the same decoder as our main CA system, and so CSRs that verify and decode with this will be accepted by our system.
(https://secure.Sectigo.net/api/pdf/latest/DecodeCSR.pdf)

AutoApplySSL
This is the main API for requesting certificates. To it you will pass your login credentials (either a username/password pair, or via a client-authentication certificate) and a CSR. In addition, you will pass a series of other parameters to determine the certificate type, duration, domain names in the certificate, and the information requested within the certificate. You will also pass details of the DCV (Domain Control Validation) process to confirm control over the domain the certificate is requested for (https://secure.Sectigo.net/api/pdf/latest/AutoApplySSL.pdf)

WebHostReport
This API can provide detailed status on one or more orders previously placed through your account. This includes simple order information, but also can extend to very detailed information about the order and where it is in the Validation process.
(https://secure.Sectigo.net/api/pdf/latest/WebHostReport.pdf)

CollectSSL
This API is used for checking the status of requested certificates and also downloading the signed certificate once it is issued. The certificate can be downloaded in a number of formats, and can include or exclude all of the certificates in the issuing chain.
(https://secure.Sectigo.net/api/pdf/latest/CollectSSL.pdf)

Other management APIs

DCV Process: Not an API, but an overview guide to the DCV process, and the options available.
(https://secure.Sectigo.net/api/pdf/latest/Domain%20Control%20Validation.pdf)

This document will link to other APIs, such as:
GetDCVEmailAddressList
(https://secure.Sectigo.net/api/pdf/latest/GetDCVEmailAddressList.pdf)

AutoUpdateDCV
(https://secure.Sectigo.net/api/pdf/latest/AutoUpdateDCV.pdf)

AutoReplaceSSL: Used to replace/reissue certificates.
(https://secure.Sectigo.net/api/pdf/latest/AutoReplaceSSL.pdf)

AutoRevokeSSL: Used to revoke a certificate.
(https://secure.Sectigo.net/api/pdf/latest/AutoRevokeSSL.pdf)

AutoRemoveMDCDomain: Used to remove un-validated names on a multi-domain certificate, before issuance. If the removed name is the only remaining un-validated name on the request, then certificate issuance will be triggered.
(https://secure.Sectigo.net/api/pdf/latest/AutoRemoveMDCDomain.pdf)

UpdateUserOVCallback: Used to help automate the OV telephone call-back process. With this you can submit a time and date for an automated call-back to a customer, or suggest a new phone number for us to verify.
(https://secure.Sectigo.net/api/pdf/latest/UpdateUserOvCallback.pdf)

UpdateUserEVClickThrough: Used to send a link to a customer email address, which contains a click-through agreement and the ability to fill out the required EV information without any paperwork.
(https://secure.Sectigo.net/api/pdf/latest/UpdateUserEvClickThrough.pdf)

Example SSL Server Certificate Provisioning Flow

DV Certificate

Domain Validated certificates require only verification of the control over the requested domain name(s) in the certificate.

The certificates can be issued very rapidly.

1) Gather request information from the customer:
   a. CSR
   b. Product type and duration

2) Check the CSR for validity – use DecodeCSR API or other x.509 parsing library.

3) Use the CSR to gather DCV details – possible email addresses for DV, hash values for alternative DCV. Present to the customer for selection or setup the alternative DCV methods (HTTP file, DNS record) on behalf of the customer

4) Submit request to Sectigo – use AutoApplySSL API.
   a. Your reseller credentials
   b. CSR
   c. Product type and duration
   d. DCV information
   e. [Optional] A caCertificateID value
   f. [Optional] Increment the 'days' parameter to account for early renewal.

Save the resulting orderNumber, certificateID and other return values.

5) Await completion of DCV or checking of the DCV process if using the non-email methods.

6) Call CollectSSL API to receive signed certificate or receive the certificate pushed via the push certificate mechanism.

OV and EV Certificates

Organisation Validated (OV) and Extended Validation (EV) certificates follow the same basic process flow as the DV certificates above. However, additional information must be submitted as part of step 4) and step 5) is expanded to cover the validation of this additional information, and a telephone callback. These validation steps are handled directly by Sectigo, and in some cases the telephone call-back can be customer driven by an automated system.

