**API Overview**

The DigiCert ONE IoT Device Manager application program interface (API) provides a powerful interface for customizing and automating workflows for your certificates and devices.

A RESTful API is an architectural style for an that uses HTTP requests to access and use data. That data can be used to GET, PUT, POST and DELETE data types, which refers to the reading, updating, creating and deleting of operations concerning resources.

REST stands for **Representational State Transfer**. This means that when a client requests a resource using a REST API, the server *transfers* back the current *state* of the resource in a standardized *representation*.

In other words, REST APIs work by fielding requests for a resource and returning all relevant information about the resource, translated into a format that clients can easily interpret (this format is determined by the API receiving requests). Clients can also modify items on the server and even add new items to the server through a REST API.

The base path for all endpoints is: <https://demo.one.digicert.com/iot/api/v1/> and a complete list of API methods with Swagger documentation, including certificate issuance, renewal, etc., is available here <https://demo.one.digicert.com/iot/api-docs/index.html>.

All requests are submitted via RESTful URLs using REST features, including header-based authentication and JSON request types. The Digicert One API methods can be tested using common tools such as the GUI based tool Postman (available for download at <https://www.postman.com/>) or the command line tool *curl* which is pre-installed on current versions of Microsoft Windows but can also be downloaded and installed using this guide [https://www.thewindowsclub.com/how-to-install-curl-on-windows-10](%20https://www.thewindowsclub.com/how-to-install-curl-on-windows-10).

**Authentication**

The DigiCert ONE APIs support header-based API key authentication. Additionally, a subset of the IoT Device Manager APIs support authentication using an enrollment passcode or client certificate.

**API key authentication**

To authenticate with an API key, include the custom HTTP header **x‑api‑key** in your request. Provide your own API key as the value for this header when you submit your request. The API key will be provided to you by the PKI Registration Authority (RA). **NOTE: Store the API key securely and limit access based on need.**

**Enrollment Passcode authentication**

An alternative to an API key is Passcode authentication, which has , more limited functionality. Only the following endpoints in the IoT Device Manager API support the option to authenticate with an enrollment passcode instead of an API key:

* Request certificate
* Renew certificate

To authenticate with an enrollment passcode, use the custom HTTP header **x-passcode**. The value of the **x-passcode** header is the passcode associated with the enrollment profile you specify in the body of the request. Requests that use enrollment passcode authentication do not include the **x-api-key** header.

**What is a CSR (Certificate Signing Request)?**

To generate a certificate, the first step is to create a CSR. A CSR is a text file inthe standard PKCS#10 format that contains information (e.g. common name, organization, country) the Digicert ONE Certification Authority (CA) will use to create your certificate. It also contains the public key that will be included in your certificate and is signed with the corresponding private key.   
  
The CSR itself is usually created in a Base-64 based PEM format. You can open the CSR file using a simple text editor and it will look like the sample below. You must include the header and footer (-----BEGIN CERTIFICATE REQUEST-----) when pasting the CSR. Below is an example of the contents of a CSR file.

|  |
| --- |
| **Sample CSR for API** endpoint https://demo.one.digicert.com /iot/api/v1/certificate |
| *-----BEGIN CERTIFICATE REQUEST-----*  *MIIDZjCCAc4CAQAwITEfMB0GA1UEAwwWRW5yb2xsbWVudCBSZXF1ZXN0IENTUjCC*  *AaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGBAL3mxbVa/cNmJuB5bi3rE/V4*  *3J0xsQaqLCUzME9nBY7DrM6eu2JeNr/S1/OrL2IZtcU1XmiRarFx9B+x9HWygkmw*  *wgakeVF8EFFWDZftIueGusGTf74fRoplJnjHR4X51cYFD047Klirj4FCWPcADYc/*  *Ko+76tZZSOPZz9kAcqMZ2+Hk2xxNhgy/g41oMQOl4r6AMuWF5heVv4gz5SQXI3Vx*  *4Ci35ioneNVjOd0w02y3d7a619WrTjg0mjTsFOzTSqcFWEHSwDvhTDyC9J0jposk*  *KvcPEmTsFlr3y2xtMV7ha6MB3p6AetgHtzDgXrR0ZDieuH8gE+KAnZtmGExA1hwj*  *0NYTbCSM3UztkZTTAoxLKSCCqkmnSQ8jQt6OouXpLr/KhSOUWBUVsIemdDFH+XIs*  *DXzrKrZdsN1vE58PUz9zjBDPi+vpqmst77zbn/GfGCEeEX2KMXKyhwTpNd7Gkc0E*  *inMLB4bMPB5g+6/hKFoDCRRzRsR+TSbP/PZ/mmcS9wIDAQABoAAwDQYJKoZIhvcN*  *AQELBQADggGBABHpauTrfMfmDkHMQzo/UPLnM7HgZ9lmrPLMAEfbSusfw02z0P1O*  *+jOA2WbtiyZ+pPsfBOEjiuud4TDQezGsQqaqCPhG9Yh71aqqZsXA5w1CeWYO3tDA*  *OdphBfH2RvL6Dw7dJQbW6GY5gn7rmjYMt9kW/RDEjg5bL7HkuFtLg+5IFHkZhSw+*  *v+uSptRV/O14LoI1TLdXSL2WgU1K6tz7HR6IsgO5v/2//D99uuQEH0H30PjJanDV*  *qUkKyPbbu3o9/gbWvqfT0eA5hYGvhAb/OGCOW5zY7BCc73pTPP4mgwJcsF5jP9wc*  *GKrH1Dl3JNGw0En62F3d0c10nWU73GD9CdgYhJtGl7sfnv/vx39OOyLMo1mpE8bp*  *t/6pa7lScRJAvQrND6UKMQVBUCTZLA/5MbhpSYUmDbgrXwRFPnV6Qklo5HSSgi38*  */oNXX3vDPJuGjeONzZbI72jkny4vet2usJ6Du25M87O9VlLej730efpefb8bzFS2*  *dez5d3jFinfsxg==*  *-----END CERTIFICATE REQUEST-----* |

There are a variety of software tools that can be used to create a CSR, including OpenSSL, Java Keytool, etc. How this is done is up to your organization and will likely be handled by the AOR (Authorized Organization Representative) or LRA (Local Registration Authority) with the assistance of the PKI RA and possibly your local IT department. Before generating a CSR, a key pair is generated. The key pair contains a public and private key. **The private key must be kept secure as it is used to encrypt and decrypt data, digitally sign code or documents, and authenticate identity.  If your**[**private key**](https://winscp.net/eng/docs/public_key#private)**is stored unprotected on your own computer, then anybody who gains access to that computer will be able to generate signatures as if they were you.** The [CA](https://www.digicert.com/) signing your certificate request (such as DigiCert) does not create or have access to your private key.

**Example of Requesting a New Certificate via API with Postman**

Once you have generated a CSR, you can use Postman to test certificate requests via the API. Below is a screenshot of a sample API request and response using Postman. The CSR text, along with other information such as the Enrollment Profile ID, are included in the Body of the API call. The API Key or Passcode are included in the Headers.

The appropriate Enrollment Profile ID(s) will be provided to you by the RA.

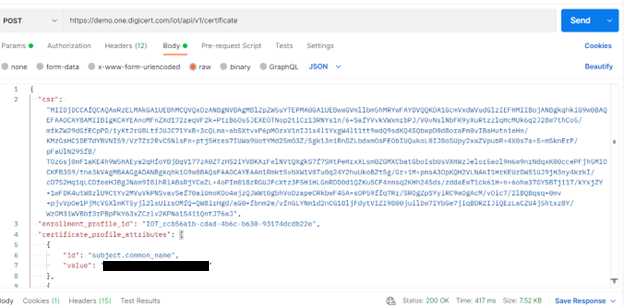


Figure 1 Postman API Body

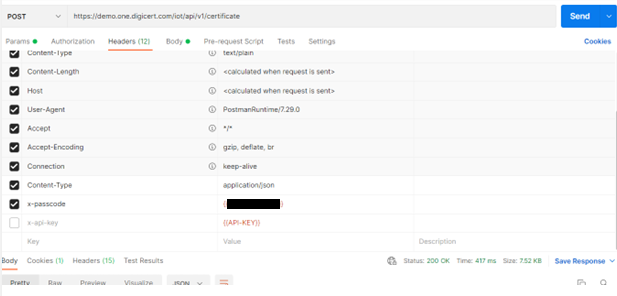


Figure 2 Postman API Headers

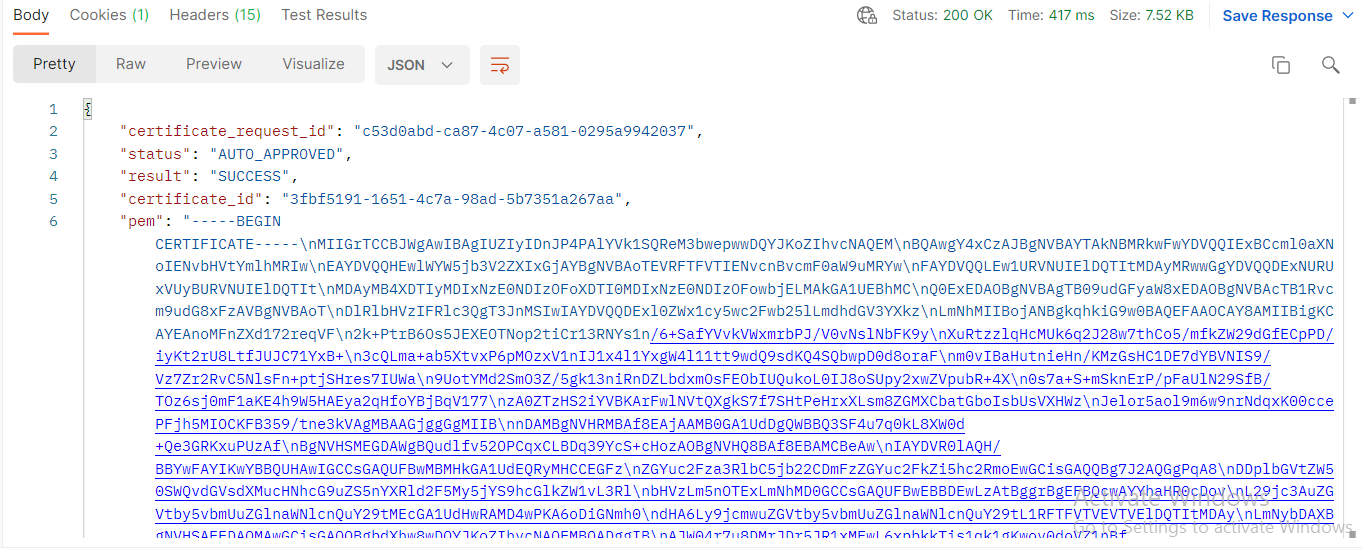


Figure 3 Postman API Response

Once you have configured the correct Body and Headers, clicking Send will initiate the API call, sending the CSR and authentication passcode to the Digicert ONE CA, which will then respond with the newly signed certificate, as seen in the third screenshot. In fact, the response will contain the full “Chain” of certificates, including the new end-entity certificate, the certificate of the Issuing CA, and of the Root CA. The API response will contain multiple data elements including certificate\_request\_id, status, results, Certificate\_id and pem. To create a certificate file to be used, the pem value must be copied and saved as a text file with the appropriate name and file extension (.cer, .crt, .pem etc). These certificates can then be installed for use on a computer, server, network device, USB token etc. as needed for use in your PSAP.

**Overriding CSR values with API Request Body Fields**

For convenience when generating multiple certificates via API, various certificate attributes contained in the CSR can be overridden by specifying those attributes in the Body of the API request along with the CSR and certificate\_enrollment\_profile values. A sample BODY for a certificate request is shown below.

|  |
| --- |
| **Sample Postman Body for API endpoint** https://demo.one.digicert.com /iot/api/v1/certificate |
| **{**  **"csr": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",**  **"enrollment\_profile\_id": "IOT\_XXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXX",**  **"certificate\_profile\_attributes": [{**  **"id": "subject.common\_name",**  **"value": ""**  **},**  **{**  **"id": "subject.organization\_name",**  **"value": ""**  **},**  **{**  **"id": "subject.organization\_unit",**  **"value": ""**  **},**  **{**  **"id": "subject.country",**  **"value": "CA"**  **},**  **{**  **"id": "subject.state",**  **"value": ""**  **},**  **{**  **"id": "subject.locality",**  **"value": ""**  **}**  **]**  **}** |