**Cloud monetization API (CMAPI)**

**How to Request User License using /access\_request API with example**

**Step 1. Create Public/Private Key Pair**

* A Private and Public key are required to use the REST-driven licensing APIs (CMAPI)
* Many publicly available tools, one example below:
* Download and Install OpenSSL “Light” for Windows @ <https://slproweb.com/products/Win32OpenSSL.html>
* Open command prompt in C:\Program Files\OpenSSL-Win64\bin (or OpenSSL installed location)
* Run the following commands:

*openssl genrsa -out SaaSDemoPrivate.pem 2048*

*openssl rsa -inform PEM -outform DER -in SaaSDemoPrivate.pem -pubout*

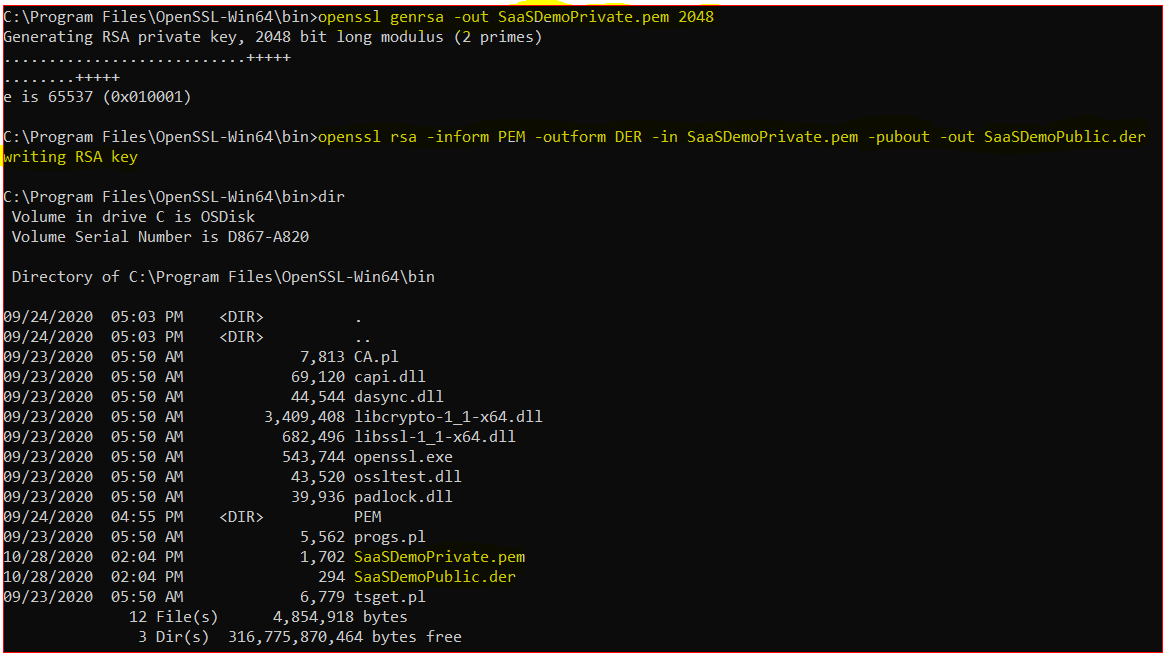
*-out SaaSDemoPublic.der*

* It Generates:

Private Key: *SaaSDemoPrivate.pem*

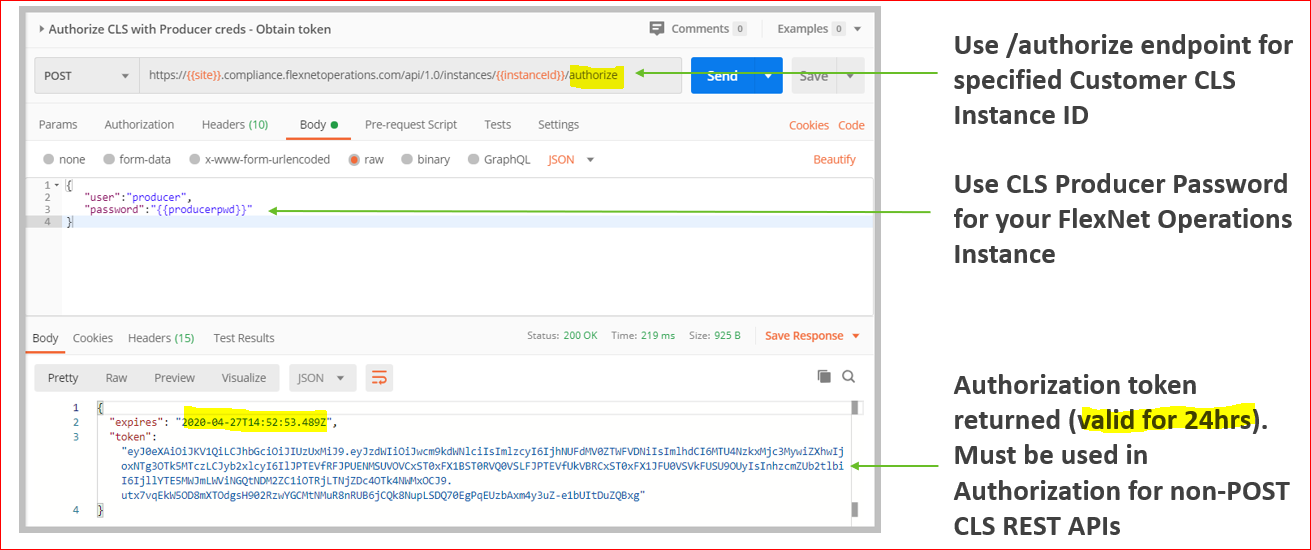
Public Key : *SaaSDemoPublic.der*

will be created in C:\Program Files\OpenSSL-Win64\bin



**Step 2: Get CLS Authorization Token**

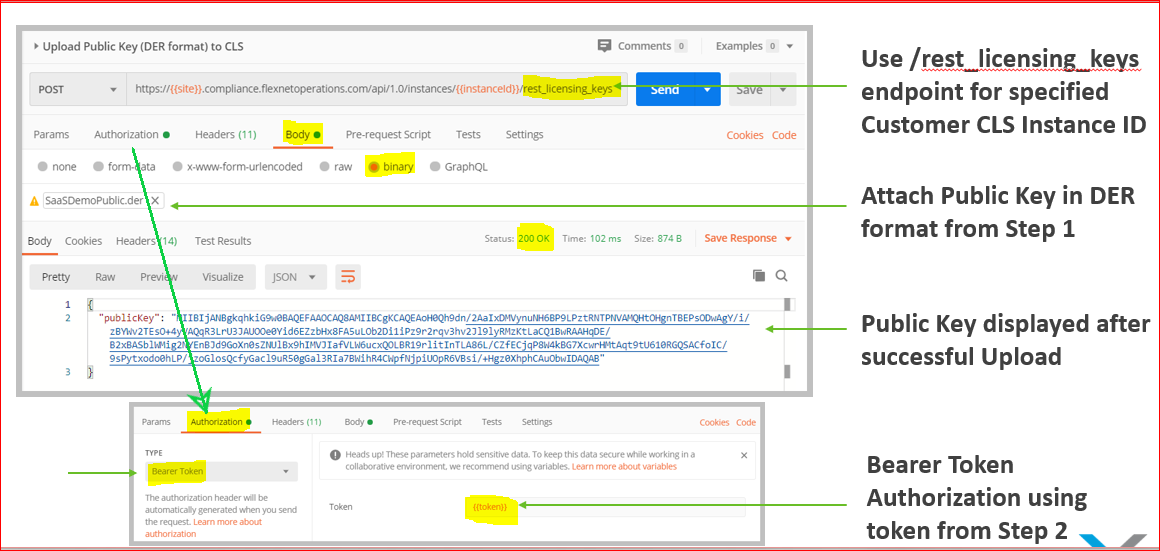
* In the Customer Portal set the admin password on target Cloud Server (CLS). The Producer password (for all Cloud Servers) can also be used
* Use /authorize REST endpoint to get the authorization token



Documentation Reference: ***License Server Producer Guide***

**Step 3: Upload Public Key to Customer CLS Instance using /rest\_licensing\_keys**

* Add Authorization with token generated from **step 2**
* Add Body - Attach *SaaSDemoPublic.der* Public Key from C:\Program Files\OpenSSL-Win64\bin



* Add Content-Type: application/octet stream to Headers
* Send POST to rest\_licensing\_keys endpoint. Status should be “200 OK” and then we will get **Public key** with a successful upload.

**Step 4. Create JSON Web Token (JWT) from Private Key**

* JWT Creation example we can use online tools such as [**https://jwt.io/**](https://jwt.io/)are readily available.
* Select the **RS256** Algorithm and enter the following Payload Data:

{

"sub": "1234567890",

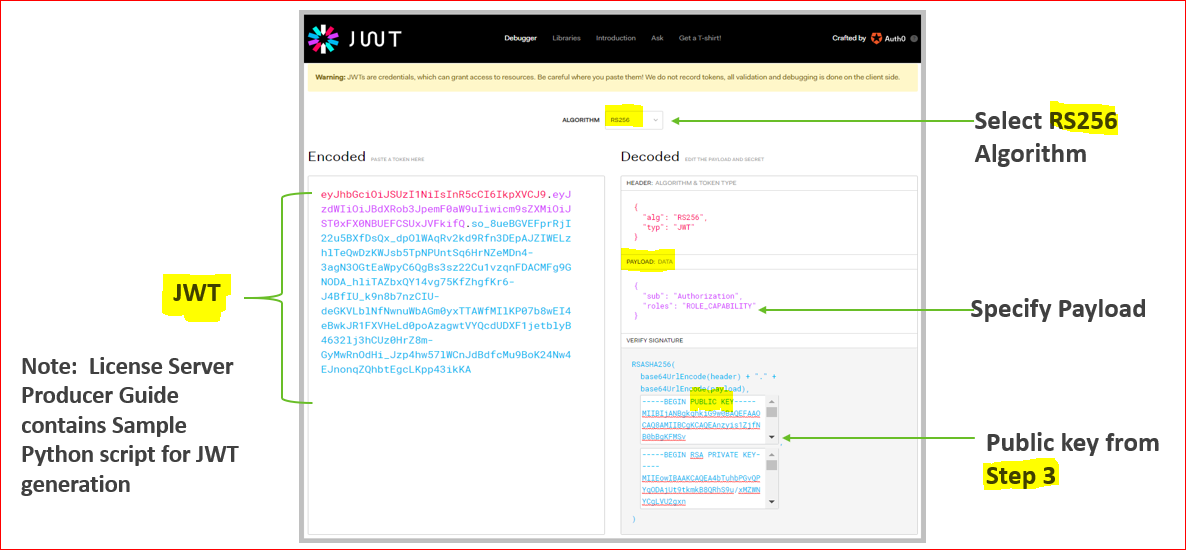
"roles": "ROLE\_CAPABILITY"

}

* Copy contents of *SaaSDemoPrivate.pem* from *C:\Program Files\OpenSSL-Win64\bin* into the Verify Signature Private Key Section

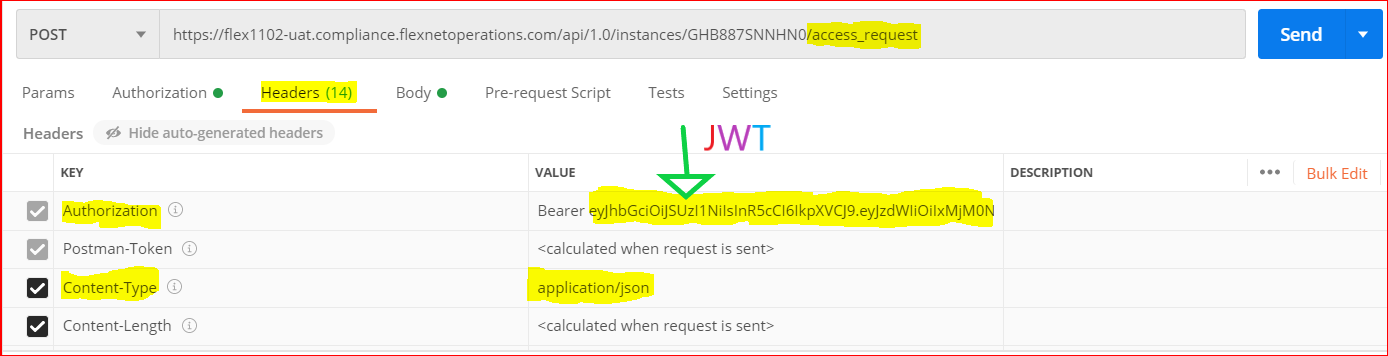


* Copy **Public key** from **Step 3** and paste it below “Begin Public key” line, then we will get JWT Token on the left side like below



**Step 5. Request User License using /access\_request**

* Add the newly created JWT token to the Header



* Create the desired license request in the Body, for an example request under raw section

{

    "hostId" : {

        "type" : "string",

        "value" : " **Access\_Request**"

    },

    "incremental" : **true**,

    "borrow-interval" : "0",

    "partial" : **true**,

    "features" : [

        {

            "count" : 1,

            "name" : "0000Test",

            "version" : "1"

        },

        {

         "count" : 1,

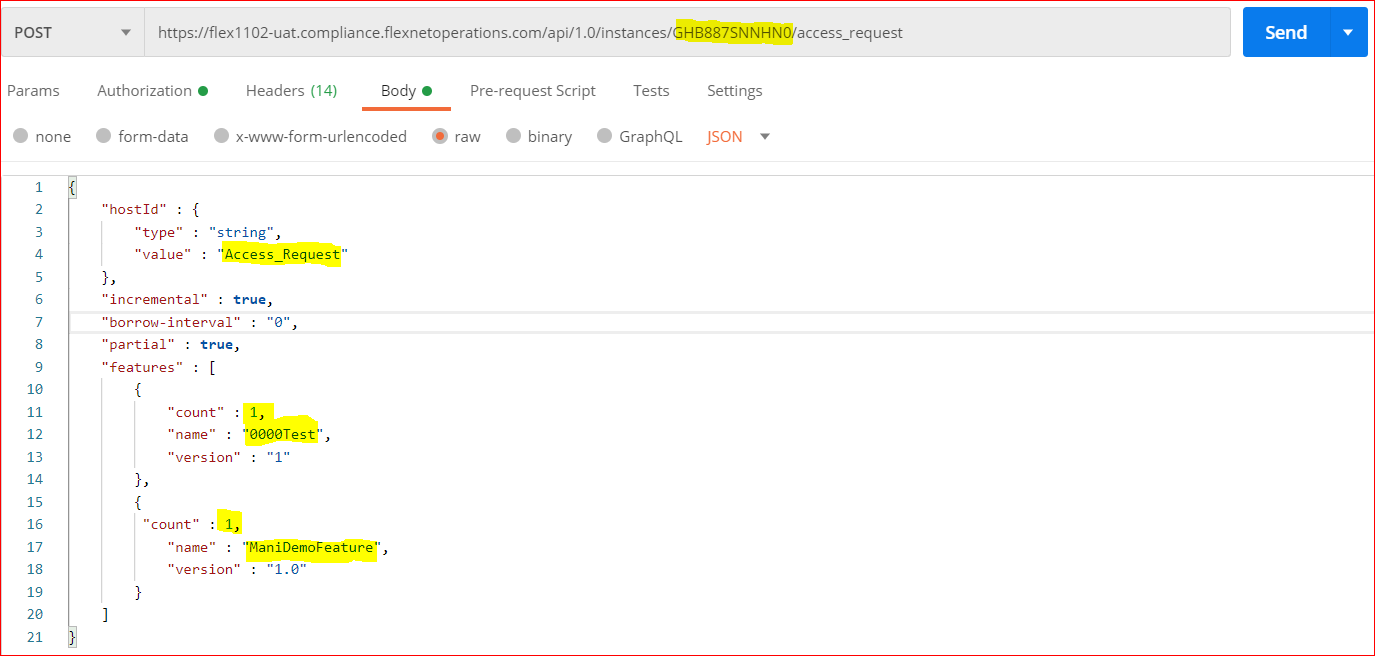
            "name" : "ManiDemoFeature",

            "version" : "1.0"

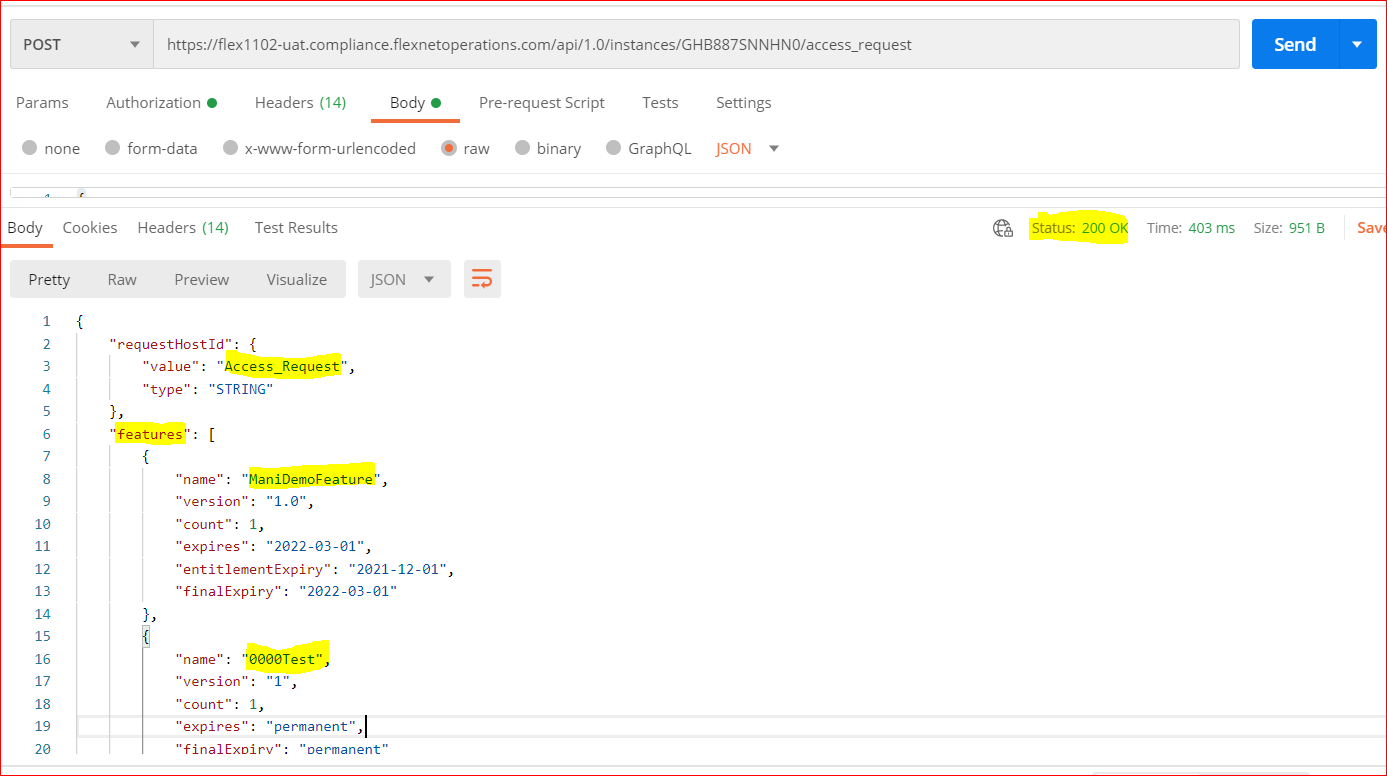
        }

    ]

}



* Send the POST request (/access\_request) and view the response for the above request with two features and one count for each.



* **Served Device** Details can then be viewed in the Producer/Customer Portals:



* We can see the requested features with number of counts for each.

**Step6: View Available Licenses in the CLS**

* One method to see all licenses (with available quantities) is to use /preview\_request. The /features endpoint can also be used (verbose). Sample request for preview

{

    "hostId": {

"type": "string",

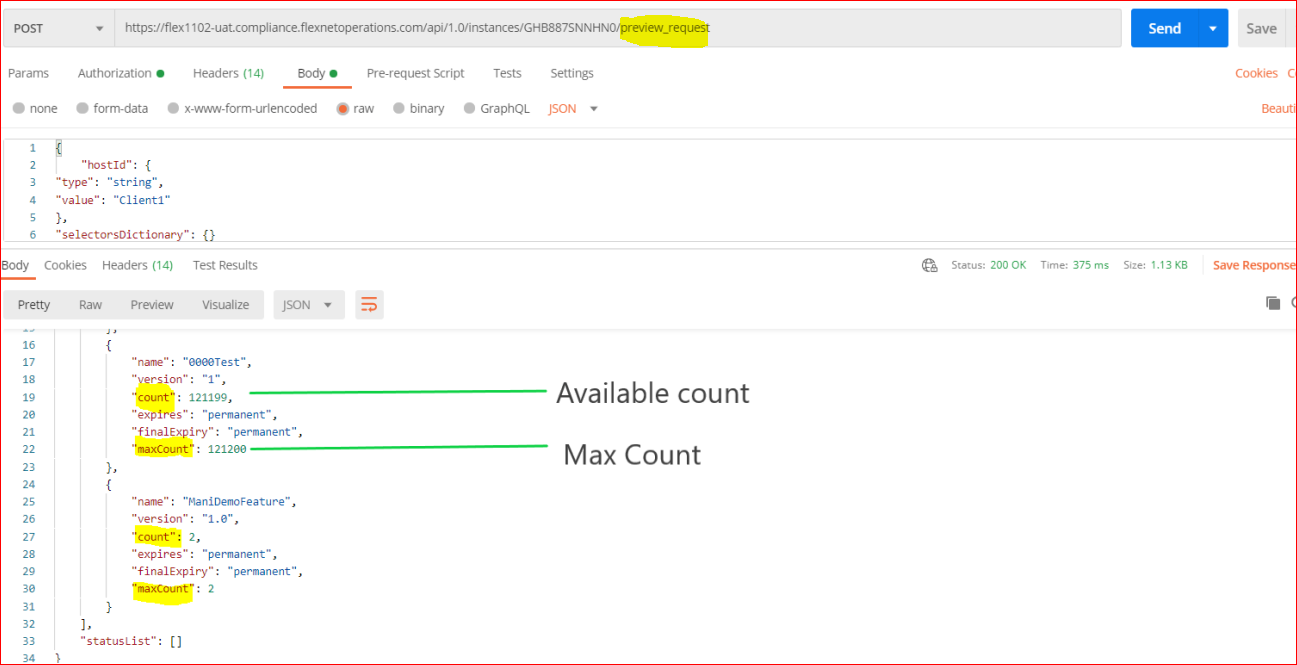
"value": "Client1"

},

"selectorsDictionary": {}

}

* Preview response contains available count “**count**” and Maximum Entitled count “**maxCount**” for each feature



**Thanks**