How to create a Customer Certificate

Instruction to create Certificate for the first time.

Step-by-step guide

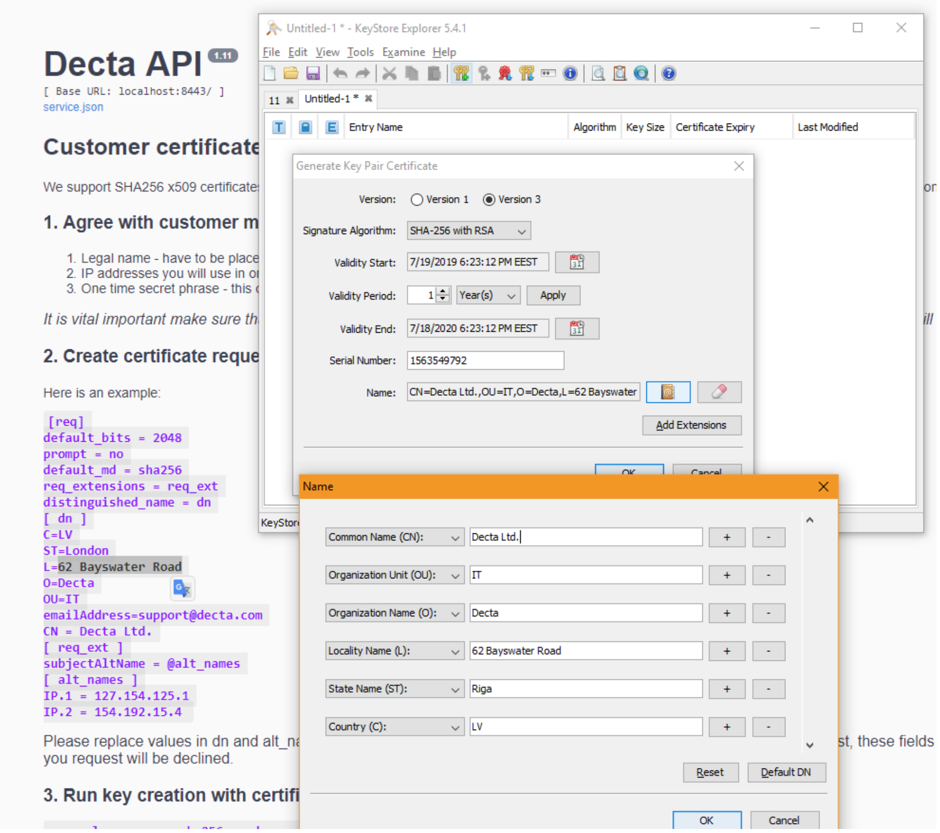
Precondition:

Request to create certificate. Provide "Client Name" and "Secret" values. As a result CN, Secret and IP should be received.

Check Swagger technical instructions here.

After certificate request was processed, certificate should be created.

1. Download and install "KeyStore Explorer" (Download Link)
2. Open "KeyStore Explorer" and add new KeyStore (with type: **PKCS # 12**)
3. Press "Generate Key Pair" button (type: **RSA 2048**)
4. While certificate creation - Fill in required fields in Name section. **Pay attention on fields CN and Email (should be added, absent by default).**



Decta API 1.11

[Base URL: localhost:8443/]

service.json

Customer certificate

We support SHA256 x509 certificate

1. Agree with customer m

1. Legal name - have to be place
2. IP addresses you will use in o
3. One time secret phrase - this

It is vital important make sure th

2. Create certificate reque

Here is an example:

```
[req]
default_bits = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn
[ dn ]
C=LV
ST=London
L=62 Bayswater Road
O=Decta
OU=IT
emailAddress=support@decta.com
CN = Decta Ltd.
[ req_ext ]
subjectAltName = @alt_names
[ alt_names ]
IP.1 = 127.154.125.1
IP.2 = 154.192.15.4
```

Please replace values in dn and alt_na ... st, these fields
you request will be declined.

3. Run key creation with certifi

Untitled-1 * - KeyStore Explorer 5.4.1

Generate Key Pair Certificate

Version: ○ Version 1 ● Version 3

Signature Algorithm: SHA-256 with RSA

Validity Start: 7/19/2019 6:23:12 PM EEST

Validity Period: 1 Year(s)

Validity End: 7/18/2020 6:23:12 PM EEST

Serial Number: 1563549792

Name: CN=Decta Ltd.,OU=IT,O=Decta,L=62 Bayswater

Name

Common Name (CN): Decta Ltd.

Organization Unit (OU): IT

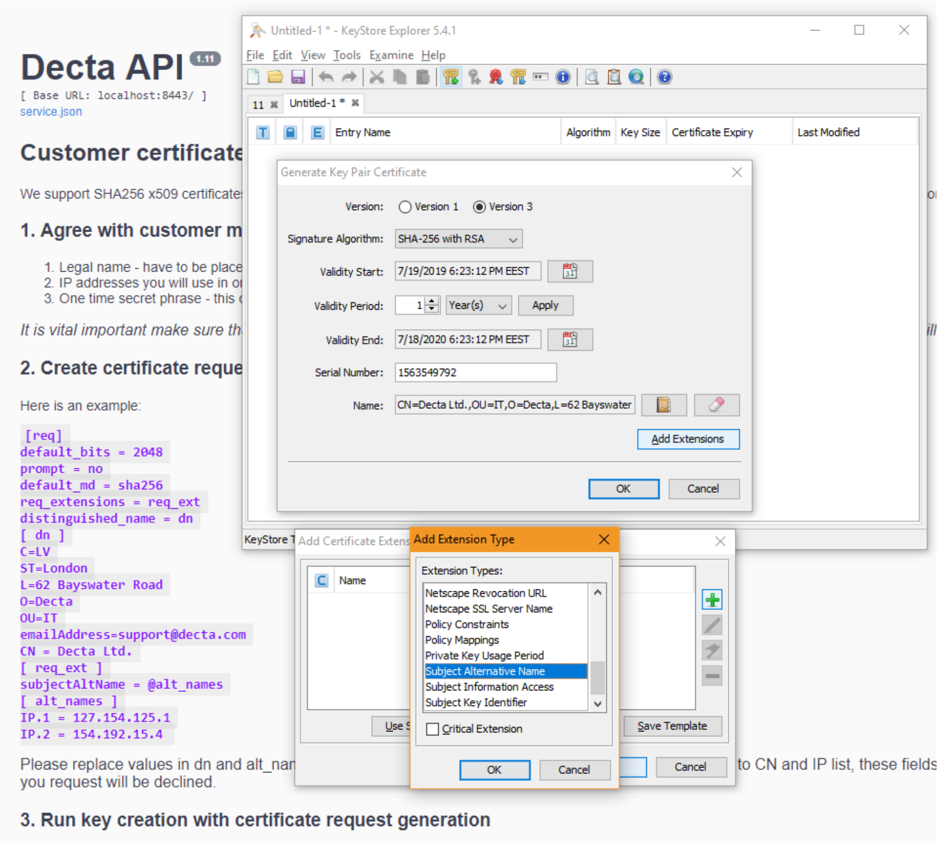
Organization Name (O): Decta

Locality Name (L): 62 Bayswater Road

State Name (ST): Riga

Country (C): LV

5. Add Extensions (**Alternative Name**), add IP



Decta API 1.11

[Base URL: localhost:8443/]

service.json

Customer certificate

We support SHA256 x509 certificate

1. Agree with customer m

1. Legal name - have to be place
2. IP addresses you will use in o
3. One time secret phrase - this

It is vital important make sure th

2. Create certificate reque

Here is an example:

```
 [req]
default_bits = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn
[ dn ]
C=LV
ST=London
L=62 Bayswater Road
O=Decta
OU=IT
emailAddress=support@decta.com
CN = Decta Ltd.
[ req_ext ]
subjectAltName = @alt_names
[ alt_names ]
IP.1 = 127.154.125.1
IP.2 = 154.192.15.4
```

Please replace values in dn and alt_nan … to CN and IP list, these fields … you request will be declined.

3. Run key creation with certificate request generation

Untitled-1 * - KeyStore Explorer 5.4.1

Generate Key Pair Certificate

Version: ○ Version 1 ● Version 3

Signature Algorithm: SHA-256 with RSA

Validity Start: 7/19/2019 6:23:12 PM EEST

Validity Period: 1 Year(s) Apply

Validity End: 7/18/2020 6:23:12 PM EEST

Serial Number: 1563549792

Name: CN=Decta Ltd.,OU=IT,O=Decta,L=62 Bayswater

Add Extensions

OK Cancel

Add Extension Type

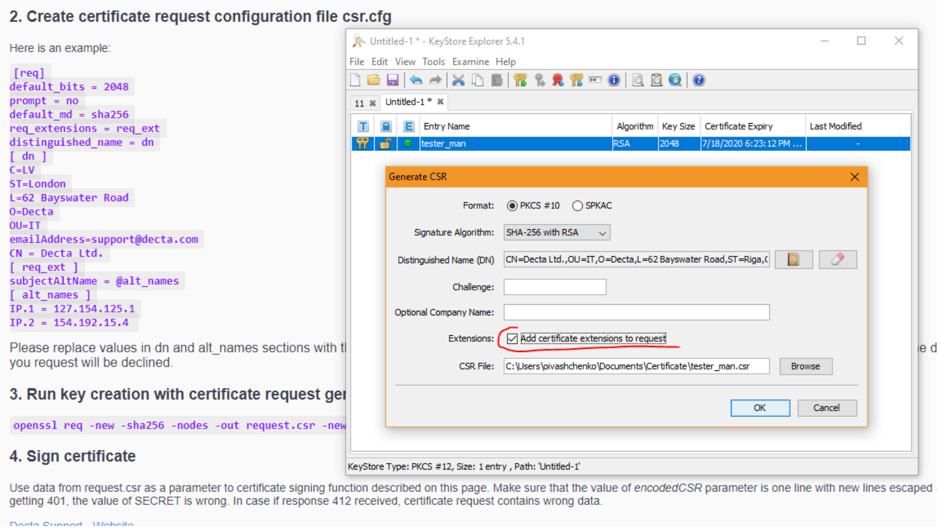
Extension Types:

- Netscape Revocation URL
- Netscape SSL Server Name
- Policy Constraints
- Policy Mappings
- Private Key Usage Period
- Subject Alternative Name
- Subject Information Access
- Subject Key Identifier

□ Critical Extension

OK Cancel

6. After all information added and certificate is saved. CSR file should be generated. Select "Generate CSR" from dropdown menu on certificate. **Tick "Add certificate extensions to request"**



2. Create certificate request configuration file csr.cfg

Here is an example:

```
 [req]
default_bits = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn
[ dn ]
C=LV
ST=London
L=62 Bayswater Road
O=Decta
OU=IT
emailAddress=support@decta.com
CN = Decta Ltd.
[ req_ext ]
subjectAltName = @alt_names
[ alt_names ]
IP.1 = 127.154.125.1
IP.2 = 154.192.15.4
```

Please replace values in dn and alt_names sections with t… e d … you request will be declined.

3. Run key creation with certificate request ge

```
openssl req -new -sha256 -nodes -out request.csr -new
```

4. Sign certificate

Use data from request.csr as a parameter to certificate signing function described on this page. Make sure that the value of *encodedCSR* parameter is one line with new lines escaped getting 401, the value of SECRET is wrong. In case if response 412 received, certificate request contains wrong data.

Untitled-1 * - KeyStore Explorer 5.4.1

Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
tester_man	RSA	2048	7/18/2020 6:23:12 PM ...	-

Generate CSR

Format: ● PKCS #10 ○ SPKAC

Signature Algorithm: SHA-256 with RSA

Distinguished Name (DN) CN=Decta Ltd.,OU=IT,O=Decta,L=62 Bayswater Road,ST=Riga,C

Challenge:

Optional Company Name:

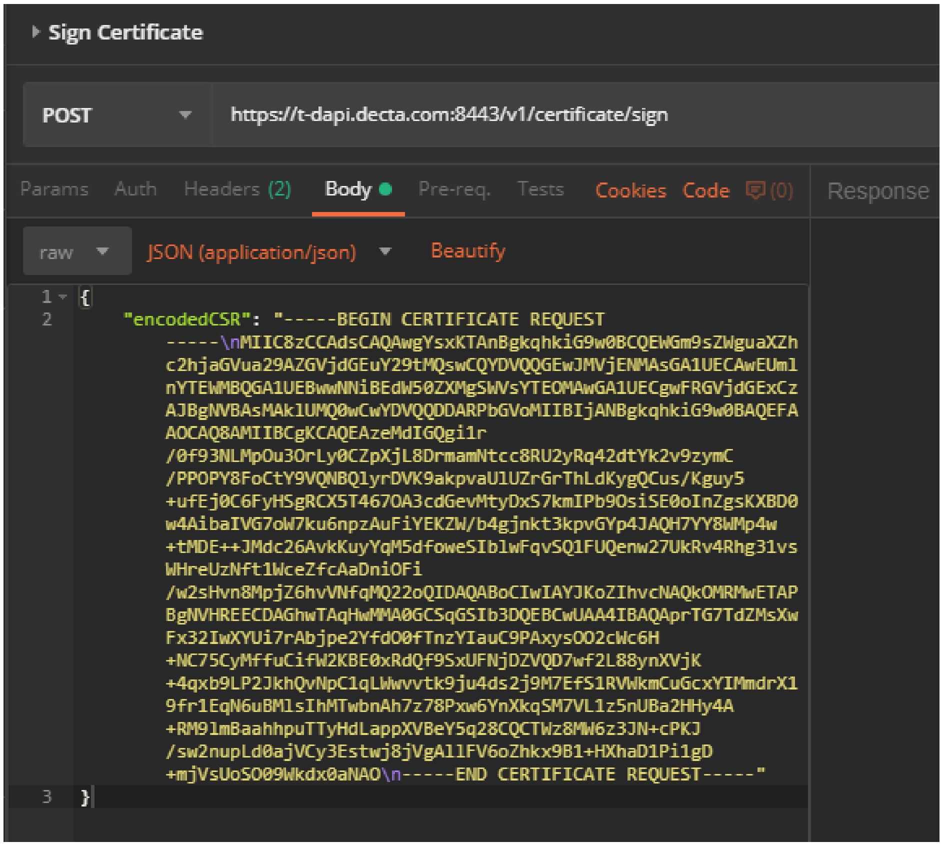
Extensions: ☑ Add certificate extensions to request

CSR File: C:\Users\pivashchenko\Documents\Certificate\tester_man.csr Browse

OK Cancel

KeyStore Type: PKCS #12, Size: 1 entry , Path: 'Untitled-1'

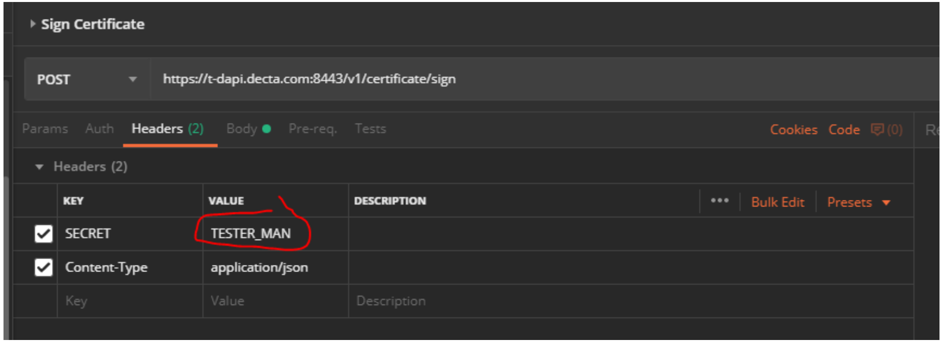
7. Sign certificate using POSTMAN, with CSR from file (add CSR without spaces and add \n after header, and before footer) and secret in header.



Sign Certificate

POST https://t-dapi.decta.com:8443/v1/certificate/sign

```
{
    "encodedCSR": "-----BEGIN CERTIFICATE REQUEST
        -----\nMIIC8zCCAdsCAQAwgYsxKTAnBgkqhkiG9w0BCQEWGm9sZWguaXZh
        c2hjaGVua29AZGVjdGEuY29tMQswCQYDVQQGEwJMVjENMAsGA1UECAwEUml
        nYTEWMBQGA1UEBwwNNiBEdW50ZXMgSWVsYTEOMAwGA1UECgwFRGVjdGExCz
        AJBgNVBAsMAk1UMQ0wCwYDVQQDDARPbGVoMIIBIjANBgkqhkiG9w0BAQEFA
        AOCAQ8AMIIBCgKCAQEAzeMdIGQgi1r
        /0f93NLMpOu3OrLy0CZpXjL8DrmamNtcc8RU2yRq42dtYk2v9zymC
        /PPOPY8FoCtY9VQNBQlyrDVK9akpvaU1UZrGrThLdKygQCus/Kguy5
        +ufEj0C6FyHSgRCX5T467OA3cdGevMtyDxS7kmIPb9OsiSE0oInZgsKXBD0
        w4AibaIVG7oW7ku6npzAuFiYEKZW/b4gjnkt3kpvGYp4JAQH7YY8WMp4w
        +tMDE++JMdc26AvkKuyYqM5dfoweSIblwFqvSQ1FUQenw27UkRv4Rhg31vs
        WHreUzNft1WceZfcAaDniOFi
        /w2sHvn8MpjZ6hvVNfqMQ22oQIDAQABoCIwIAYJKoZIhvcNAQkOMRMwETAP
        BgNVHREECDAGhwTAqHwMMA0GCSqGSIb3DQEBCwUAA4IBAQAprTG7TdZMsXw
        Fx32IwXYUi7rAbjpe2YfdO0fTnzYIauC9PAxysOO2cWc6H
        +NC75CyMffuCifW2KBE0xRdQf9SxUFNjDZVQD7wf2L88ynXVjK
        +4qxb9LP2JkhQvNpClqLWwvvtk9ju4ds2j9M7EfS1RVWkmCuGcxYIMmdrX1
        9fr1EqN6uBMlsIhMTwbnAh7z78Pxw6YnXkqSM7VL1z5nUBa2HHy4A
        +RM91mBaahhpuTTyHdLappXVBeY5q28CQCTWz8MW6z3JN+cPKJ
        /sw2nupLd0ajVCy3Estwj8jVgAllFV6oZhkx9B1+HXhaD1Pi1gD
        +mjVsUoSO09Wkdx0aNAO\n-----END CERTIFICATE REQUEST-----"
}
```

- 

  Sign Certificate

  POST https://t-dapi.decta.com:8443/v1/certificate/sign

	KEY	VALUE	DESCRIPTION
☑	SECRET	TESTER_MAN	
☑	Content-Type	application/json	
	Key	Value	Description

8. Check and Save response. If you are getting 401, the value of SECRET is wrong. In case if response 412 received, certificate request contains wrong data.

Information received from Response will be used in each request to DAPI.