Generating a CSR with OpenSSL

This procedure is used to generate a digital certificate to be used when transacting across the DBN Alliance's Exchange Framework.

1. Create a file called **openssl.conf** and enter the below information:

```
oid_section = OIDs

[ req ]
distinguished_name = dn
prompt = no

[ OIDs ]

organizationIdentifier=2.5.4.97

[ dn ]
emailAddress=member.rep@my_access_point.com
O=My Access Point LTD
organizationalUnitName=MyAccessPoint AP
C=US
ST=Texas
organizationIdentifier=MYACCESSPOINT
CN=DUNS::012345678
```

The table below shows sample values to use for the opensl.conf data elements:

OPENSSL Key Value	Description	Example
emailAddress	The Member Representative email address where certificate emails will be sent to.	admin@myaccesspoint.com
O (organization)	The Member organization name.	My Access Point LTD
organizationalUnitName	The entity within the Member's organization for this certificate, typically this will be the access point or SMP service.	MyAccessPoint AP
C (Country)	The Member Organizations registered country code.	US
ST (State)	The state or district within the country for the Member Organization.	Texas
organizationIdentifier	The ORG SEAT ID is the name of the Member Organization short name as assigned when the Member joined the DBN Alliance. The SEATID is used to issue certificates for the member organization and is assigned by the DBN Alliance. It is typically the member organization name in short form with spaces removed and all uppercase.	MYACCESSPOINT
CN (Common Name)	The member's unique scheme::identifier used for address routing. Schemes include	DUNS::012345678 GLN::3456789012340

	DUNS, SSN, GLN etc. Identifier is the unique organizations identifier in that scheme, the double colons are the required separator between scheme and identifier.	

2. Open a Command Prompt or Terminal and run the following openssl command:

```
openssl req -newkey rsa:2048 -keyout example.key -out
example.csr -config openssl.conf -nodes
```

3. The input file is ***openssl.conf*** and this generates two output files:

File	Component	Handling
example.csr	The Certificate Signing Request	This file is submitted to the Certificate Authority for signing.
example.key	The Private Key	This file is kept secure.

If an error occurs similar to this:

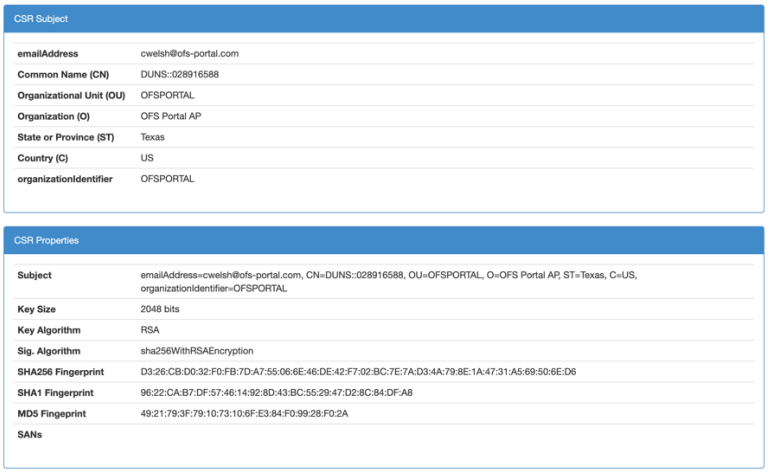
problem creating object organizationIdentifier=2.5.4.97
40970FADA17F0000:error:04000066:object identifier routines:OBJ_create:oid exists:../crypto/objects/obj_dat.c:719:

Remove this line from the openssl.conf file and try the openssl command again:

```
organizationIdentifier=2.5.4.97
```

Certain openssl versions require different OID parameters and this was found to be a common problem on some systems.

4. Inspect the CSR for accuracy prior to submitting to the Certificate Authority.

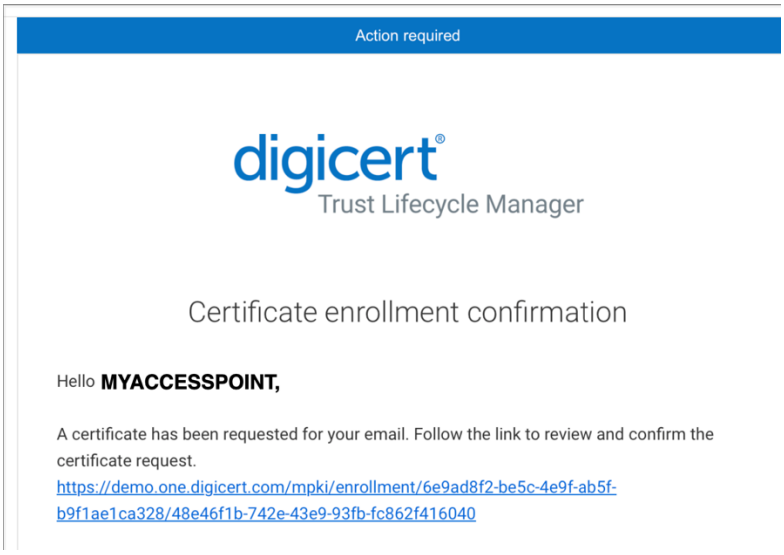


To inspect the CSR, you can use a decoder like https://redkestrel.co.uk/tools/decoder

5. The CSR contents will be used to submit the CSR data to the DigiCert One platform to issue the digital certificate needed to use the exchange framework. The email address entered in the CSR request data value ***emailAddress*** will receive a link to upload the CSR data to.

   The Certificate Administrator will now ENROLL the SEATID to one of the certificate domains (TEST, PILOT or PRODUCTION) as requested and an email will be received at the ***emailAddress*** from the DigiCert One platform.

   Once this link is received and followed, the CSR data can be pasted into the DigiCert One platform to have the digital certificate issued to the organization. The screen shot below shows a sample email received from the DigiCert One platform and the link to follow to reach the CSR upload form.



6. Once the CSR has been uploaded and submitted, a button to download the certificate will be shown in the DigiCert One application, click the button and the certificate will be downloaded through the web browser.