emudhra
Trust Delivered

# Generating CSR

fido ALLIANCE MEMBER
CAB CA/BROWSER FORUM
WebTrust Accredited
AATL
CLOUD SIGNATURE CONSORTIUM
Asia PKI Consortium

## What is a CSR?

A CSR or Certificate Signing Request is a block of encoded text (encoded using ASN.1 according to the PKCS #10 specification) that contains information a Certificate Authority (CA) needs to create your SSL certificate. Usually generated on the server where the certificate will be installed, it contains three crucial parts, which includes:

- Your Public Key
- The fully-qualified domain name(s) you want your certificate to be used with
- Other information about you and your organization/website (including the legally registered name and the city/state/country where it is registered)

Note that a key pair is generated at the same time you create a CSR. The first half of the key pair, the public key, which is included in the CSR that you share with the CA and the SSL certificate that you receive in response, is used to encrypt the data sent by the user to your server, thereby facilitating secure data transmission. While the other half of the key pair, the private key, which is not a part of the CSR nor shared with the CA or anyone else, is used at a later stage — when the SSL Certificate is installed — to decrypt the data that the public key encrypted.

Also a SSL certificate that is created using a CSR will only work with the private key that was generated in conjunction with that particular CSR. So if you lose the Private Key, the SSL certificate will no longer work.

## What is contained in a CSR?

| Name | Explaination | Examples |
|---|---|---|
| **Common Name** | The Fully Qualified Domain Name (FQDN) of your server. This must match exactly what you type in your web browser or you will receive a name mismatch error | *.google.com<br>mail.google.com |
| **Organization** | The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC | Google Inc. |
| **Organizational Unit** | The division of your organization handling the certificate | Information Technology<br>IT Department |
| **City/Locality** | The city where your organization is located | Mountain View |
| **State/County/Region** | The state/region where your organization is located. This shouldn't be abbreviated | California |
| **Country** | The two-letter ISO code for the country where your organization is location | US<br>GB |
| **Email address** | An email address used to contact your organization. | webmaster@google.com |
| **Public Key** | The Public Key that will go into the certificate. | The Public Key is created automatically |

## What does a CSR look like?

Created in the Base-64 encoded PEM format that can be opened in a text editor, most CSRs start with "-----BEGIN CERTIFICATE REQUEST-----" and end with "-----END CERTIFICATE REQUEST-----" as illustrated in the below example:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIByjCCATMCAQAwgYkxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MRYwFAYDVQQHEw1Nb3VudGFpbiBWaWV3MRMwEQYDVQQKEwpHb29nbGUgSW5jMR8w
HQYDVQQLExZJbmZvcm1hdGlvbiBUZWNobm9sb2d5MRcwFQYDVQQDEw53d3cuZ29v
Z2xlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEApZtYJCHJ4VpVXHfV
IlstQTlO4qC03hjX+ZkPyvdYd1Q4+qbAeTwXmCUKYHThVRd5aXSqlPzyIBwieMZr
WFlRQddZ1IzXAlVRDWwAo60KecqeAXnnUK+5fXoTI/UgWshre8tJ+x/TMHaQKR/J
cIWPhqaQhsJuzZbvAdGA80BLxdMCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GBAIhl
4PvFq+e7ipARgI5ZM+GZx6mpCz44DTo0JkwfRDf+BtrsaC0q68eTf2XhYOsq4fkH
Q0uA0aVog3f5iJxCa3Hp5gxbJQ6zV6kJ0TEsuaaOhEko9sdpCoPOnRBm2i/XRD2D
6iNh8f8z0ShGsFqjDgFHyF3o+lUyj+UC6H1QW7bn
-----END CERTIFICATE REQUEST-----
```

## How to Generate a CSR?

- **Tools Used to Generate CSR:**

  Here are some of the tools that you can use to generate the key pair and export CSR file -

  1. Open SSL downloaded from website
  2. IIS Server in Windows
  3. Java Keytool utility installed with JRE

  Below are step-by-step instructions that you have to follow to generate CSR using each of the above tools:

## CSR Generation Using OpenSSL

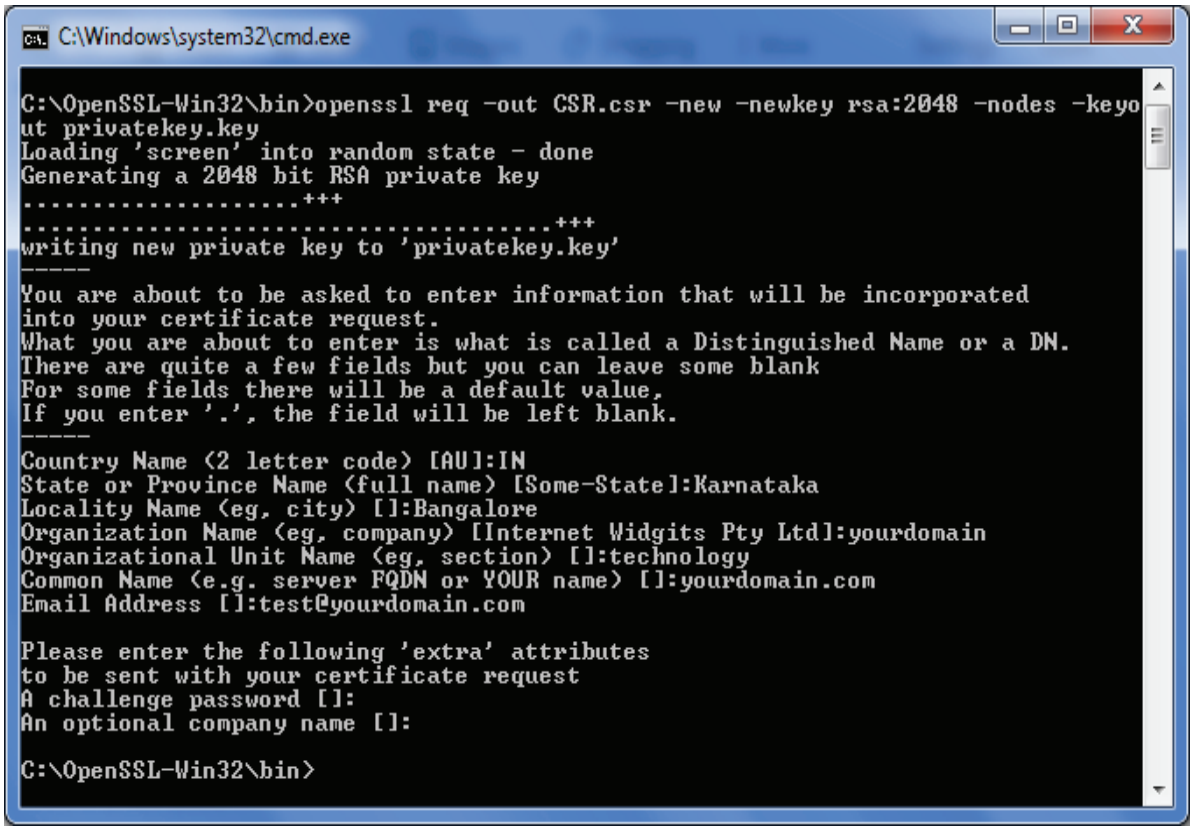
- Go to the bin folder in Openssl, Open Command Prompt.
- Run the command

***" openssl req -out CSR.csr -new -sha256 -newkey rsa:2048 -nodes -keyout privatekey.key -config openssl.cnf "***

Where CSR.csr - csr for the domain.
privatekey.key - Private key of the new certificate.
rsa: 2048 - rsa 2048 bit key is the key size of the CSR.(2048 to 8192 is allowed for RSA 2048 key Size is not allowed.)

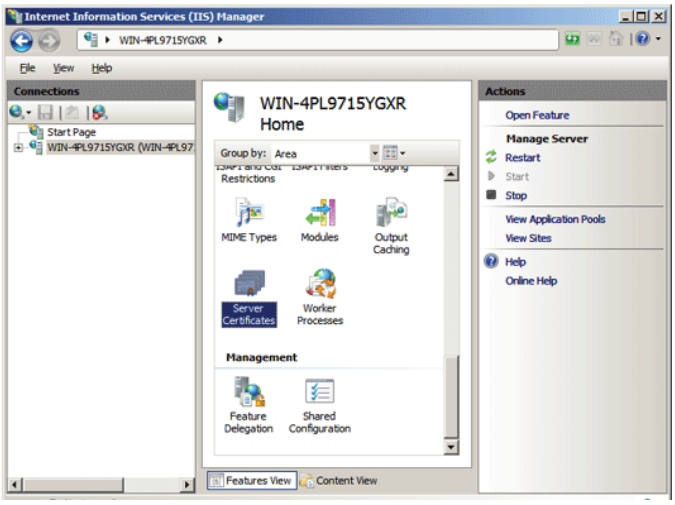
- Allowed Signature Algorithm- md5 with RSA, SHA(1/224/256/384/512) with RSA encryption.
- On running the above command, it will prompt asking the details ,
  - Country Name – 2 digit country code is required. *(eg- 'IN' for India).*
  - State /Province Name – State or Province Full Name *(eg- Karnataka )*
  - Locality Name- City Name *(eg- Bangalore)*
  - Organization Name- - Company Name *(eg- emudhra limited)*
  - Organization Unit Name- Section Name *(eg- technology)*
  - Common Name- Server Fully Qualified Name *(eg – www.yourdomain.com)*. For Wildcard Certificate before domain name '*' shall be included. (eg- *.yourdomain.com)
  - Email ID- Email ID of the requester.*(Not Mandatory)*
  - A challenge Password- *(Not Mandatory)*.
  - An Optional Company Name- *(Not Mandatory)*
- For DV certificate only Common Name and Country Code is sufficient .

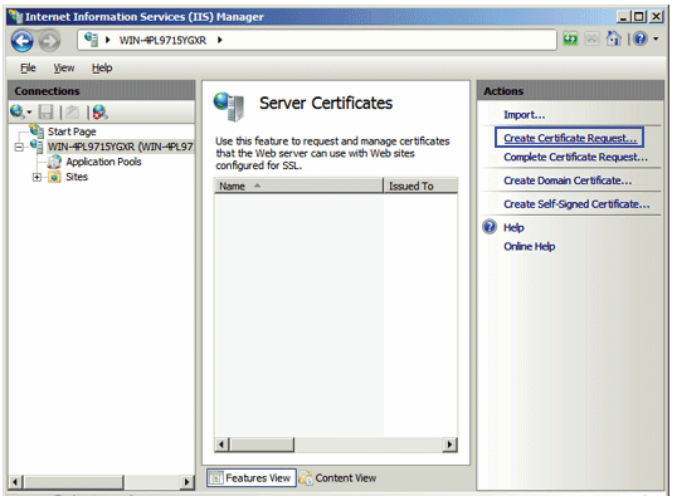
- Find below OpenSSL CSR generation for RSA



## CSR Generation in IIS

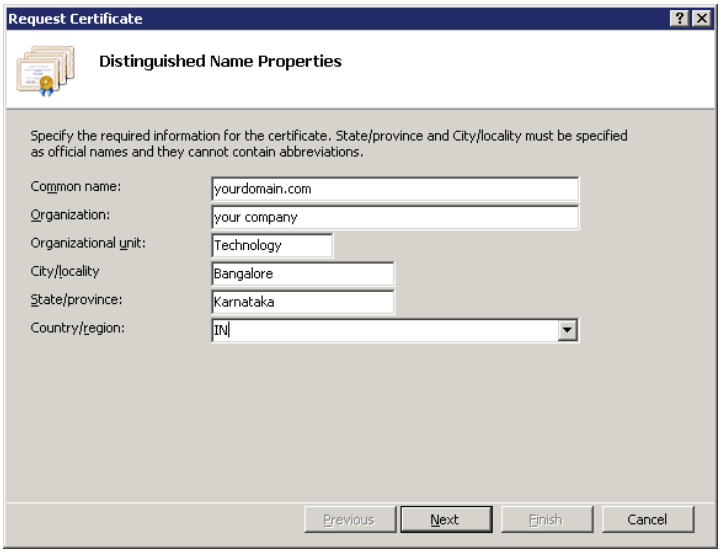
- Open IIS and select a 'Server', Double Click on 'Server Certificates'.

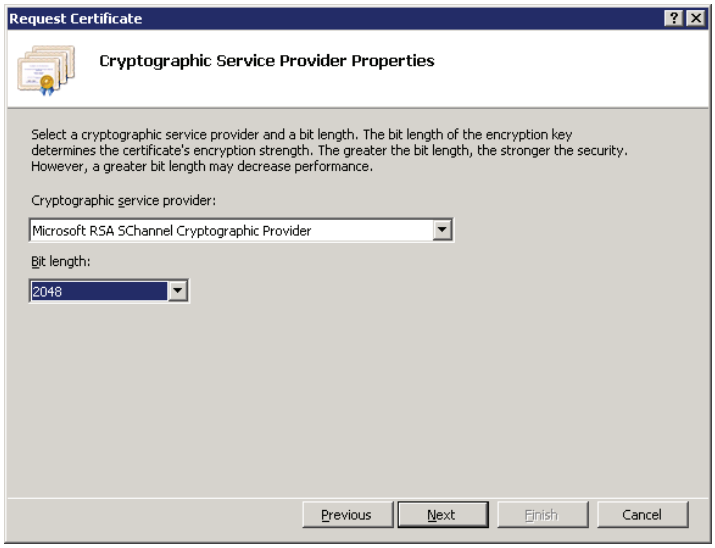



- Click on 'Create Certificate Request', a new window opens , enter the CSR details and click on 'Next', Select the Cryptographic Service Provider and Key Length. Click 'Next ' and provide the path to save the CSR.

- Provide the CSR details



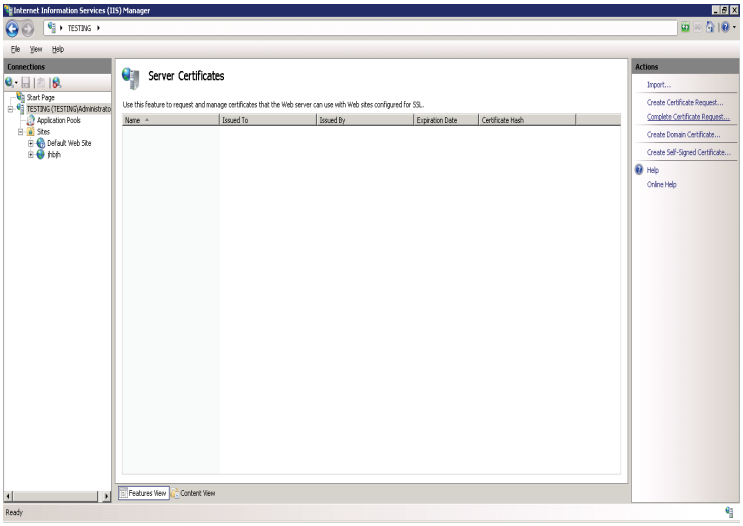



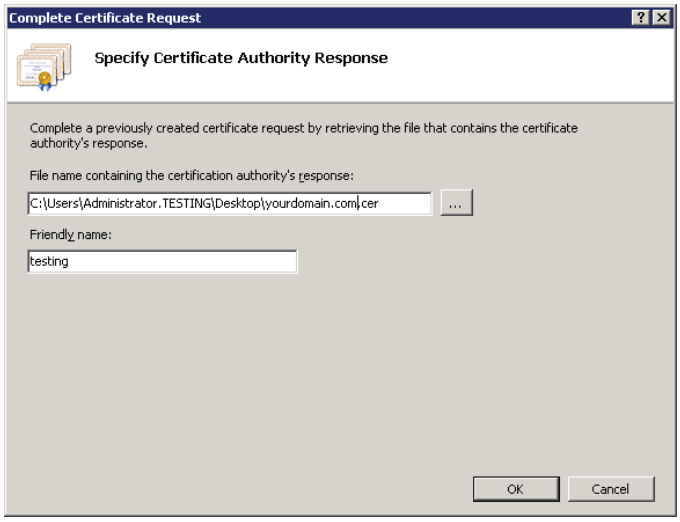

- Click ON 'Next' . Select 'Microsoft RSA SChannel Cryptographic Provider' and select Key Size between (2048 to 8192).

- Provide the path and save the CSR file

## Importing CER in IIS

- Go to the Sever and Click on 'Server Certificate' and click on 'Complete Certificate Request'.

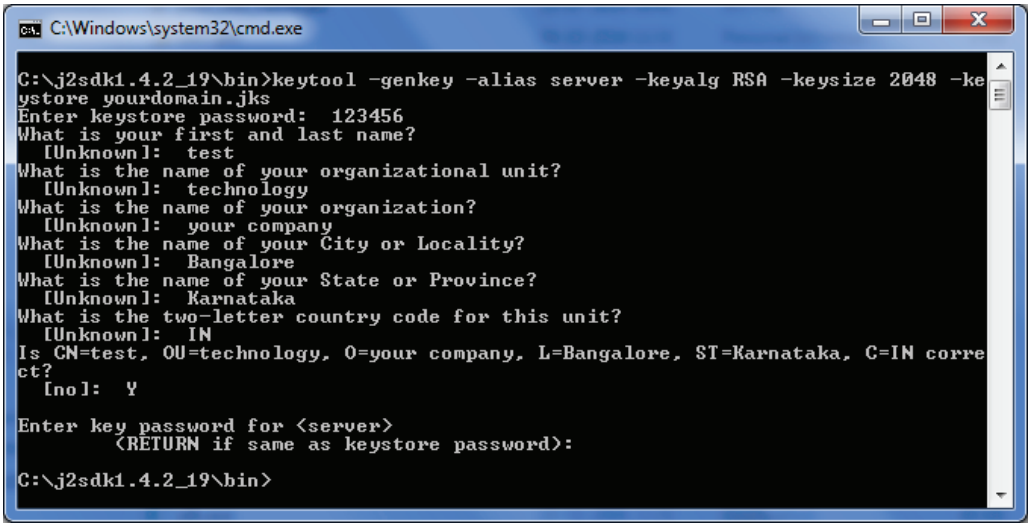



- Select the File Path and provide a friendly name and click on 'Ok'. The Certificate will display in the Server Certificates

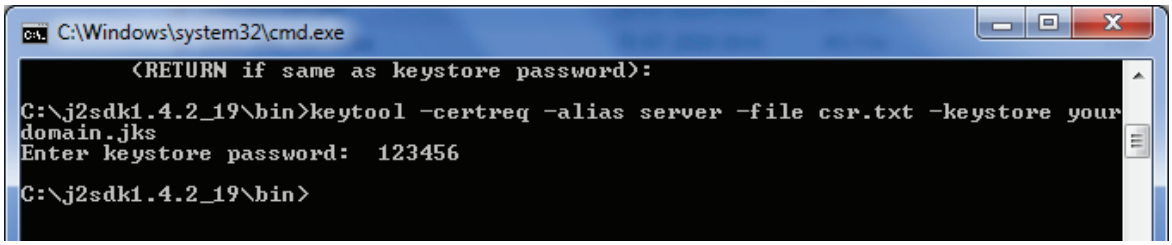
## Generating the Key pairs in JKS

- Navigate to Java Bin Path, and Run the below command
  Keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore yourdomain.jks –
  Provide the password and provide the CSR details- This will create New jks File and Private Key inside the jks(java key store)
- Where yourdomain.jks – java key store file where the Private Key is stored



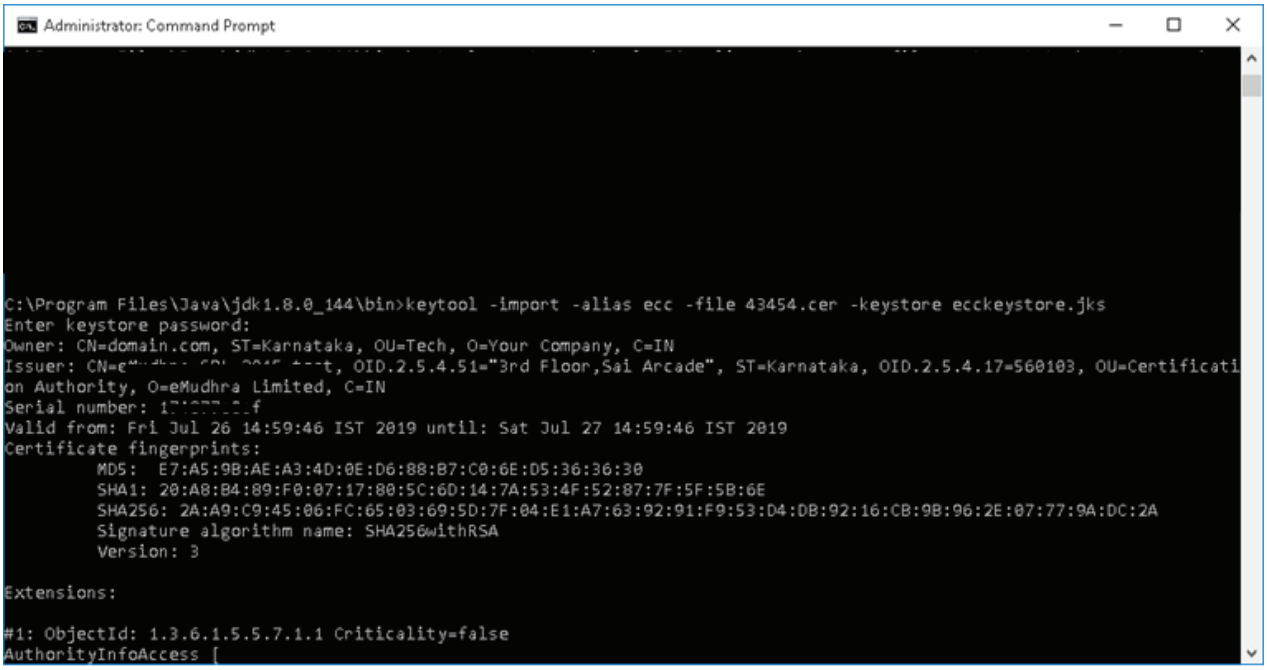
## Generating CSR in JKS

- Keytool -certreq -alias server -file csr.txt -keystore yourdomain.jks - Enter the previous password and create a CSR.
- Where csr.txt – is the CSR file
- On running the command a CSR is generated in the bin folder by name CSR.txt.




## Importing the CER in JKS

- Keytool -import -alias ecc -file domain.cer -keystore ecckeystore.jks to Import the .cer file into keystore.



## About eMudhra:

Much like the name, which is an embodiment of the seal of authenticity in the electronic or digital world, eMudhra is a cyber security solutions company and a trust service provider that is focused on accelerating the world's transition to a secure integrated digital society. With presence in 5 continents and a global delivery center in Bengaluru, India, eMudhra is empowering secure digital transformation of over 45 global banks, several Fortune 100 customers and thousands of SMEs.

emudhra
Trust Delivered

USA | India | Malaysia| UAE