

SSDG Uses PKI as a security mechanism. This document provides information about setting up PKI with SSDG.

1. Steps for configuring PKI with SSDG

The following steps are involved in configuring PKI with SSDG

- i. Creating private key and Certificate Signing Request (CSR) – The following procedure is involved in creating a CSR.
 - a. Creating a certificate keystore and private key - This is done using the keytool utility of JDK using the following command.

```
JAVA_HOME\bin>keytool -genkey -alias your_alias_name -keyalg RSA -  
keystore your_keystore_filename
```

Figure 1 shows the snapshot of the above command execution.

```
C:\Program Files\Java\jdk1.5.0_14\bin>keytool -genkey -alias nsdgalias -keyalg  
SA -keystore H:\pkidoc\nsdg.keystore  
Enter keystore password: seng@cdac  
What is your first and last name?  
[Unknown]: www.cdacmumbai.in  
What is the name of your organizational unit?  
[Unknown]: SENG  
What is the name of your organization?  
[Unknown]: C-DAC  
What is the name of your City or Locality?  
[Unknown]: MUMBAI  
What is the name of your State or Province?  
[Unknown]: MAHARASHTRA  
What is the two-letter country code for this unit?  
[Unknown]: IN  
Is CN=www.cdacmumbai.in, OU=SENG, O=C-DAC, L=MUMBAI, ST=MAHARASHTRA, C=IN corre  
ct?  
[no]: Y  
Enter key password for <nsdgalias>  
(RETURN if same as keystore password): seng@cdac  
C:\Program Files\Java\jdk1.5.0_14\bin>_
```

Figure 1 : CSR Generation Snapshot 1

On execution of this command following steps need to be taken.

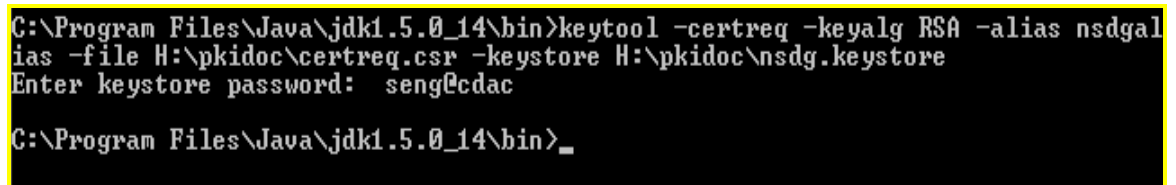
- The system will prompt for a password. Provide a password that is at least 6 characters long.
- Next, the details regarding the domain or IP address for which the SSL certificate is to be used have to be provided. These details include the first and last name which can be the web portal name serving the requests. Also, details like organisation unit, organisation name, city or locality, state or province etc are to be filled in

Next, the key password is to be provided. If the key password is the same as keystore password, Enter key is to be pressed. Else, the key password should be provided.

- b. Next step involves the generation of the CSR. The following command is used to generate the CSR using the keystore.

```
JAVA_HOME\bin>keytool -certreq -keyalg RSA -alias your_alias_name -file  
certreq.csr -keystore your_keystore_filename
```

Figure 2 gives the CSR snapshot.



```
C:\Program Files\Java\jdk1.5.0_14\bin>keytool -certreq -keyalg RSA -alias nsdgalias -file H:\pkidoc\certreq.csr -keystore H:\pkidoc\nsdg.keystore  
Enter keystore password: seng@cdac  
C:\Program Files\Java\jdk1.5.0_14\bin>_
```

Figure 2 : CSR Generation Snapshot 2

On execution, the system prompts for the keystore password. On providing the same the CSR is generated.

- c. The CSR generated through the above steps is found in file *certreq.csr*. Figure 3 gives screenshot of CSR.

```

-----BEGIN CERTIFICATE-----
MIIFUzCCBDugAwIQAglQNiLGYiQ9FhSvNIsXHPReSzANBkgqhkiG9w0BAQUFADCB
yzELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTDIzlcmITaWduLCBJbmMuMTAwLgYDVQQL
EydGb3lgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV
BAstOVRlcm1zIG9mlHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz
L3Rlc3RjYSAoYykwOTEtMCsGA1UEAxMkVmVyaVNPZ24gVHJpYWVwU2VjdXJlIFNI
cnZlciBDQSAtIEcyMB4XDTA5MDcyMDAwMDAwMFoXDTA5MDgwMzIzNTk1OVowgasx
CzAJBgNVBAYTAklOMRQwEgYDVQQIEwtNQUhBUkFTSFRSQTEPMA0GA1UEBxQGTVVN
QkFJMq4wDAYDVQQKFjAVDLURBQzENMAAsGA1UECxxQUU0VORzE6MDgGA1UECxxQxVGVy
bXMgb2YgdXNlIGF0IHd3dy52ZXJpc2lnbi5jb20vY3BzL3Rlc3RjYSAoYykwNTEa
MBGGA1UEAxQRd3d3LmNkYWVWntdW1iYWkuaW4wgZ8wDQYJKoZIhvcNAQEBBQADgYOA
MIGJAoGBAJG3zTnu+/PqypMb8rJfJ/0FN+gwwykOzh6hGZ22rZDf+6x3DNmfh
jm8iPpiMK7XaQtKds9+CkJGxcyCQZUNAC0RfPb4tnpVegmlZP8jr/6zz+dw+K5I3
HQT+WinNjSGnGJfwEdzwqnGS9k6BfeZHudtyNANoDQczIB8yiMktAgMBAAGjggHT
MIIBzzAJBgNVHRMEAjAAMAsGA1UdDwQEAwIfoDBDBgNVHR8EPDA6MDigNqAdhjJo
dHRwOi8vU1ZSVHJpYWVwtRzltY3J5LnZlcmIzaWduLmNvbS9TVlJUCmlhbEcyLmNy
bDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUwMTAvBggrBgEFBQcCARYjaHR0cHM6
Ly93d3cudmVyaXNPZ24uY29tL2Nwcy90ZXN0Y2EwHQYDVR0IBBYwFAyIKwYBBQUH
AwEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFcGXE4q91qK13AYst7aO2hBmYg7IMHQG
CCsGAQUFBwEBBGgwZjAkBggrBgEFBQcwAYYYaHR0cDovL29jc3AudmVyaXNPZ24u
Y29tMD4GCCsGAQUFBzACHjJodHRwOi8vU1ZSVHJpYWVwtRzltYWVhLnZlcmIzaWdu
LmNvbS9TVlJUCmlhbEcyLmNlcjBuBggrBgEFBQcCBDARIMGChXqBcMFowWDBWFglp
bWFnZS9SnaWYwIAtfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEFGDAmFiRo
dHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZIhvcNAQEF
BQADggEBACmRbGSGjar2r3odBzagUjXQPJf++OQ5QxH7tybjveMI5HPs4/JpnjF
Yv4kVMJF3r02wkHQqPYcLtUrknGkv3jcVWgE09y3p8fNEMJmZNtr0WLphr2DLLz
FtJfHOVddSliSi4nor0srKUp2zhNGMW5R/NuUvl7yltVAhl60DfkUbzoVwa5blWl
mlKt62bTqPp23Voj82qqKTN/BAXm6HdVlcYc0FgH57Een9C5gdUgmLSfcDime9Ht
B+s1XBe+UV+rFxZsbBneumr8hF5+5en1xPdiTQ88pzaR2RUn1g7sTRxCwDgzxP80
5cX+tjD9nYjx2c0JLFAp6Gbr56bz/U4=
-----END CERTIFICATE-----

```

Figure 3 : View of CSR

- ii. **Getting Certificate from the Certifying Authority (CA)** – The CSR generated employing the above procedure needs to be sent to the CA for signature. The CSR file may be either uploaded on the CA website or submitted to CA by alternate means like email etc.

Some CA websites allow the generation of CSR online by filling up online forms.

- iii. **Configure keystore in SSDG** - The CA will return the signed .cer file which contains the signed certificate. This certificate is to be installed in the local keystore. The following command serves the above purpose.

keytool -import -alias <your_alias_name> -file <.cer file signed from CA> -keystore <your_keystore_name> -trustcacerts.

If you get error which states that

'keytool error: java.lang.Exception: Failed to establish chain from reply'.

Include the certificates of your CA in cacerts file present in java. For eg: In this document it is assumed that NIC is CA from whom you have acquired certificate.

- iv. Go to Link of your CA from where you have acquired certificate .For e.g.: NIC is your CA.Go to Web site <http://nicca.nic.in/index.jsp>.Click on Repository. Click on Certificate Chain(CCA,NICCA & NIC sub-CA certs).Click on Certificate Chain Download zip file Download Certificate Chain (.zip format)

Now include all the certs which are present in .zip in your machine where cacerts is present jre/lib/security folder.

- a) Command for importing CCA India 2011.cer in cacerts is
keytool -importcert -alias <aliasname> -file "CCA India 2011.cer" -keystore ../jre/lib/security/cacerts -storepass changeit
- b) Command for importing NIC sub-CA for NIC 2011.cer in cacerts is
keytool -importcert -alias <alaisname> -file "NIC sub-CA for NIC 2011.cer" -keystore ../jre/lib/security/cacerts -storepass changeit
- c) Command for importing NIC CA 2011.cer in cacerts is
keytool -importcert -alias <aliasname> -file "NIC CA 2011.cer" -keystore ../jre/lib/security/cacerts -storepass changeit

Then execute the command

keytool -importcert -alias <aliasname> -file <name of certificate file acquired from CA> -trustcacerts -keystore <name of your keystore>

Your certificate will get imported into keystore.

- v. Copy the keystore in locations specified in the table named *config_para* and change the parameters accordingly listed below :
- a. Alias_name
 - b. javax.net.ssl.keyStore
 - c. javax.net.ssl.keyStorePassword
 - d. KeystorePassword
 - e. KeystorePath
 - f. KeystorePath_Web