Kent State PKI:
Sign-up Instructions for Kent CA SSL Certificate

1. If you have not done so already, visit http://cert.kent.edu and follow the instructions to install the KSU CA certificate on your computer.

2. Create a Certificate Signing Request (CSR) according to your web server's instructions. If prompted for key length, be sure to specify **1024-bits** (or higher, if required by your application). Use the following values when filling out the form:
    a. Common name: **The fully qualified domain name (FQDN) of the website,** as accessed by your users (i.e. server.dept.kent.edu)
    b. Organization: **Kent State University**
    c. Organizational unit: **The name of your division** (i.e. Information Services)
    d. City/Locale: **Kent**
    e. State: **Ohio**
    f. Country: **US**

    The CSR will look like this:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDYTCCAsoCAQAwgYUxGTAXBgNVBAMTEHdmc3Rlc3Qua2VudC5lZHUxHTAbBgNV
BAsTFEluZm9ybWF0aW9uIFNlcnZpY2VzMR4wHAYDVQQKExVLZW50IFN0YXRlIFVu
aXZlcnNpdHkxDTALBgNVBAcTBEtlbnQxDTALBgNVBAgTBE9oaW8xCzAJBgNVBAYT
AlVTMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDTN4XVDq92LjjbPc5RfRWB
MTk1LjIwewYKKwYBBAGCNwIBDjFtMGswDgYDVR0PAQH/BAQDAgTwMEQGCSqGSIb3
DQEJDwQ3MDUwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQMEAgIAgDAHBgUrDgMC
BzAKBggqhkiG9w0DBzATBgNVHSUEDDAKBggrBgEFBQcDATCB/QYKKwYBBAGCNw0C
vK4YLiXw0nFIsvYdUjpBzvAp4wkBaGD4W/4kYWgm27tVLDX6CRtYpgj9Oy6/JPID
lu+s7r5/s31OQG0kIyX/0m18i2TvUw23uGNmpJUaNmnmQVZthl893s42AAAAAAAA
AAAwDQYJKoZIhvcNAQEFBQADgYEAV4YTT9a95fNXIgkVkLJiuC4+4bcjw/fbWAV2
ZXQzLDcigPB4KPrmKSsi2LZUsAmSnVrGeRLDExhpkA0T4GkEnrU2ZMDThdSaQONk
ECU6enRgzmZ0q2uKosayEzQLYFWeXroAaooExDlJmaSQNdQrtSaN7IDrXC3d6zZn
KzznvL0=
-----END NEW CERTIFICATE REQUEST-----
```

3. After your CSR has been generated, send it in e-mail to pki-admin@kent.edu with the subject "CSR: your.server.kent.edu". You may include the CSR either as a file attachment, or by cutting and pasting the certificate request text into your message.

4. Wait for the order to be processed. Once you have submitted your request, it will be verified by the site administrator. If any changes are required, the administrator will return your message with comments. Otherwise, the administrator will approve your order and an e-mail will be sent to your address containing the actual certificate.

5. When you receive your certificate, copy it from your email and place it in a file on your server; then import it according to the instructions provided with your web server.

6. Verify that your certificate is valid by visiting your secure web page and checking the certificate details.