Fiscal Service

Public Key Infrastructure

Building a PFX (or P12) File

October 16, 2015

Revision History

Document Version	Document Date	Revision Details	Initials
1.0	October 16, 2015	Initial release	blr

Building a PFX File from a TOCA Certificate

This method to build a PFX file requires an installed, working copy of openSSL, a valid Reference Number, a valid Authorization Code, and access to the web site http://wc.treasury.gov.

Reference number: 50329217
Authorization code: HTBA-BXBK-GX3S

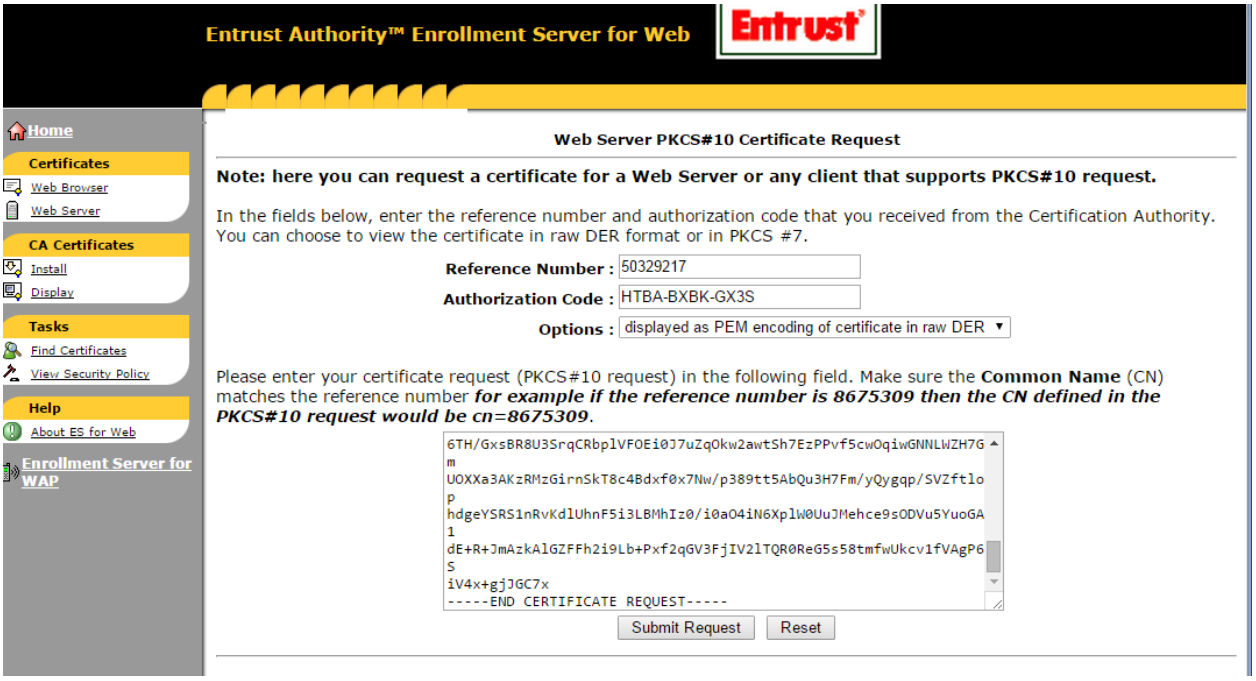
1. Create a certificate signed request (CSR). The value of the Common Name must be set to the Reference Number. Values of the other fields such as the Organizational Name are not used, but cannot be blank.

```
C:\temp>  openssl req -new -newkey rsa:2048 -keyout key.pem -out request.pem

Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....................+++
............+++
writing new private key to 'key.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name [US]:
Organization Name (eg, company) [U.S. Governement]:
Organizational Unit Name (eg, section) [Department of the Treasury]:
Organizational Unit Name (eg, section) [Bureau of the Fiscal Service]:
Common Name (eg, YOUR name) [test]: 50329217
```

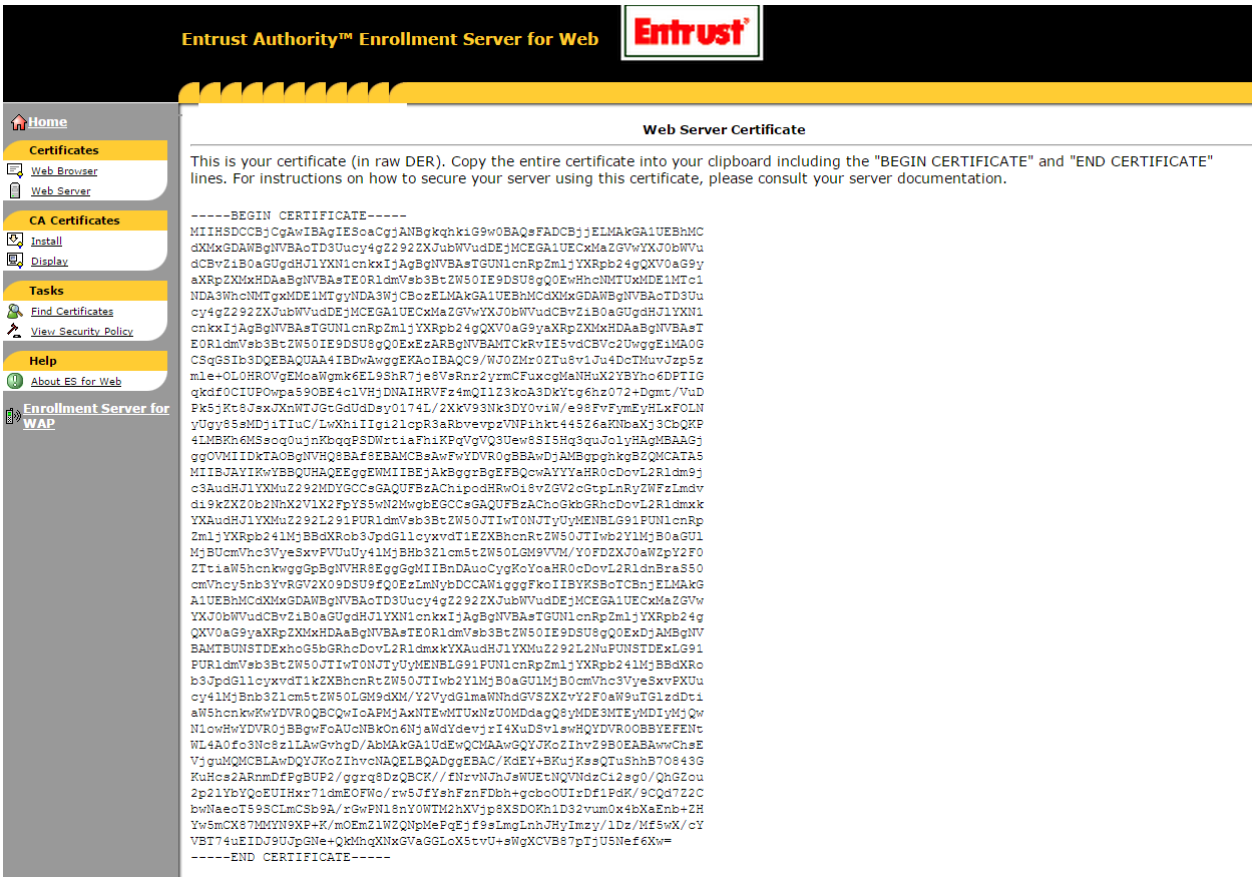
2. The CSR can be inspected using the "type" command and should look similar to the file below.

```
C:\temp> type request.pem

-----BEGIN CERTIFICATE REQUEST-----
MIIDZTCCAk0CAQAwgYcxCzAJBgNVBAYTAlVTMRkwFwYDVQQKExBVLlMuIEdvdmVy
bmVtZW50MSMwIQYDVQQLExpEZXBhcnRtZW50IG9mIHRoZSBUcmVhc3VyeTElMCMG
A1UECxMcQnVyZWF1IG9mIHRoZSBGaXNjYWwgU2VydmljZTERMA8GA1UEAxMINTAz
MjkyMTcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9/WJ0ZMr0ZTu8
v1Ju4DcTMuvJzp5zmle+OL0HROVgEMoaWgmk6EL9ShR7je8VsRnr2yrmCFuxcgMa
NHuX2YBYho6DPTIGqkdf0CIUPOwpa59OBE4clVHjDNAIHRVFz4mQIlZ3koA3DkYt
g6hz072+Dgmt/VuDPk5jKt8JsxJXnWTJGtGdUdDsy0174L/2XkV93Nk3DY0viW/e
98FvFymEyHLxFOLNyUgy85sMDjiTIuC/LwXhiIIgi2lcpR3aRbvevpzVNPihkt44
5Z6aKNbaXj3CbQKP4LMBKh6MSsoq0ujnKbqqPSDWrtiaFhiKPqVgVQ3Uew8SI5Hq
3quJolyHAgMBAAGggZcwgZQGCSqGSIb3DQEJDjGBhjCBgzALBgNVHQ8EBAMCBDAw
CQYDVR0TBAIwADAdBgNVHQ4EFgQUQ21YvgDR+jc1zzOUsDAa+GAP8BswHQYDVR0l
BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMCsGA1UdEQQkMCKCDioucHJzaGFubXUu
Y29tghB3d3cucHJzaGFubXUuY29tMA0GCSqGSIb3DQEBBQUAA4IBAQChyG8eACZv
O48nikFrivTrBUo6jKwRokVGwB/xYlugZ5V7xhAS9bEHG0MhSZMiAoTjT5ITdW0P
6TH/GxsBR8U3SrqCRbplVFOEi0J7uZqOkw2awtSh7EzPPvf5cwOqiwGNNLWZH7Gm
UOXXa3AKzRMzGirnSkT8c4Bdxf0x7Nw/p389tt5AbQu3H7Fm/yQygqp/SVZftlop
hdgeYSRS1nRvKdlUhnF5i3LBMhIz0/i0aO4iN6XplW0UuJMehce9sODVu5YuoGA1
dE+R+JmAzkAlGZFFh2i9Lb+Pxf2qGV3FjIV2lTQR0ReG5s58tmfwUkcv1fVAgP6S
iV4x+gjJGC7x
-----END CERTIFICATE REQUEST-----
```

3. Open a browser and navigate to http://wc.treasury.gov and select **Web Server**. Enter the Reference Number, Authorization Code, and CSR in the fields provided and click **Submit Request**.



4. Copy and paste the resulting certificate into a file named “cert.cer” in the same directory where the “request.pem” and “key.pem” files reside.


Entrust Authority™ Enrollment Server for Web
Entrust
Home
Certificates
Web Browser
Web Server
CA Certificates
Install
Display
Tasks
Find Certificates
View Security Policy
Help
About ES for Web
Enrollment Server for WAP
Web Server Certificate
This is your certificate (in raw DER). Copy the entire certificate into your clipboard including the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. For instructions on how to secure your server using this certificate, please consult your server documentation.
-----BEGIN CERTIFICATE-----
MIIHSDCCBjCgAwIBAgIESoaCgjANBgkqhkiG9w0BAQsFADCBjjELMAkGA1UEBhMC
dXMxGDAWBgNVBAoTD3Uucy4gZ292ZXJubWVudDEjMCEGA1UECxMaZGVwYXJ0bWVu
dCBvZiB0aGUgdHJlYXN1cnkxIjAgBgNVBAsTGUN1cnRpZmljYXRpb24gQXV0aG9y
aXRpZXMxHDAaBgNVBAsTE0RldmVsb3BtZW50IE9DSU8gQ0EwHhcNMTUxMDE1MTc1
NDA3WhcNMTgxMDE1MTgyNDA3WjCBozELMAkGA1UEBhMCdXMxGDAWBgNVBAoTD3Uu
cy4gZ292ZXJubWVudDEjMCEGA1UECxMaZGVwYXJ0bWVudCBvZiB0aGUgdHJlYXN1
cnkxIjAgBgNVBAsTGUN1cnRpZmljYXRpb24gQXV0aG9yaXRpZXMxHDAaBgNVBAsT
E0RldmVsb3BtZW50IE9DSU8gQ0ExEzARBgNVBAMTCkRvIE5vdCBVc2UwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9/WJ0ZMr0ZTu8v1Ju4DcTMuvJzp5z
mle+OL0HROVgEMcaWgmk6EL9ShR7je8VsRnr2yrmCFuxcgMaNHuX2YBYho6DPTIG
qkdf0CIUPOwpa59OBE4clVHjDNAIHRVFz4mQIlZ3koA3DkYtg6hz072+Dgmt/VuD
Pk5jKt8JsxJXnWTJGtGdUdDsy0174L/2XkV93Nk3DY0viW/e98FvFymEyHLxFOLN
yUgy85sMDjiTIuC/LwXhiIIgi2lcpR3aRbvevpzVNPihkt445Z6aKNbaXj3CbQKP
4LMBKh6MSscq0ujnKbqqP5DWrtiaFhiKPqVgVQ3Uew8SI5Hq3quJolyHAgMBAAGj
ggOVMIIDkTAOBgNVHQ8BAf8EBAMCBsAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATA5
MIIBJAYIKwYBBQUHAQEEggEWMIIBEjAkBggrBgEFBQcwAYYYaHR0cDovL2Rldm9j
c3AudHJlYXMuZ292MDYGCCsGAQUFBzAChipodHRwOi8vZGV2cGtpLnRyZWFzLmdv
di9kZXZ0b2NhX2V1X2FpYS5wN2MwgbEGCCsGAQUFBzAChoGkbGRhcDovL2Rldmxk
YXAudHJlYXMuZ292L291PURldmVsb3BtZW50JTIwT0NJTyUyMENBLG91PUNlcnRp
ZmljYXRpb24lMjBBdXRob3JpdGllcyxvdT1EZXBhcnRtZW50JTIwb2YlMjB0aGU1
MjBUcmVhc3VyeSxvPVUuUy4lMjBHb3Zlcm5tZW50LGM9VVM/Y0FDZXJ0aWZpY2F0
ZTtiaW5hcnkwggGpBgNVHR8EggGgMIIBnDAucCygKoYoaHR0cDovL2RldnBraS50
cmVhcy5nb3YvRGV2X09DSU9fQ0EzLmNybDCCAWigggFkoIIBYKSBoTCBnjELMAkG
A1UEBhMCdXMxGDAWBgNVBAoTD3Uucy4gZ292ZXJubWVudDEjMCEGA1UECxMaZGVw
YXJ0bWVudCBvZiB0aGUgdHJlYXN1cnkxIjAgBgNVBAsTGUN1cnRpZmljYXRpb24g
QXV0aG9yaXRpZXMxHDAaBgNVBAsTE0RldmVsb3BtZW50IE9DSU8gQ0ExDjAMBgNV
BAMTBUNSTDExhoG5bGRhcDovL2RldmxkYXAudHJlYXMuZ292L2NuPUNSTDExLG91
PURldmVsb3BtZW50JTIwT0NJTyUyMENBLG91PUNlcnRpZmljYXRpb24lMjBBdXRo
b3JpdGllcyxvdT1kZXBhcnRtZW50JTIwb2YlMjB0aGUlMjB0cmVhc3VyeSxvPXUu
cy4lMjBnb3Zlcm5tZW50LGM9dXM/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdDti
aW5hcnkwKwYDVR0QBCQwIoAPMjAxNTEwMTUxNzU0MDdagQ8yMDE3MTEyMDIyMjQw
NlowHwYDVR0jBBgwFoAUcNBkOn6NjaWdYdevjrI4XuDSvlswHQYDVR0OBBYEFENt
WL4A0fo3Nc8zlLAwGvhgD/AbMAkGA1UdEwQCMAAwGQYJKoZIhvZ9B0EABAwwChsE
VjguMQMCBLAwDQYJKoZIhvcNAQELBQADggEBAC/KdEY+BKujKssQTuShhB7O843G
KuHcs2ARnmDfPgBUP2/ggrq8DzQBCK//fNrvNJhJsWUEtNQVNdzCi2sg0/QhGZou
2p2lYbYQcEUIHxr71dmEOFWo/rw5JfYshFznFDbh+gcboOUIrDf1PdK/9CQd7Z2C
bwNaeoT59SCLmCSb9A/rGwPN18nY0WTM2hXVjp8X5DOKh1D32vum0x4bXaEnb+ZH
Yw5mCX87MMYN9XP+K/mOEmZlWZQNpMePqEjf9sLmgLnhJHyImzy/1Dz/Mf5wX/cY
VBT74uEIDJ9UJpGNe+QkMhqXNxGVaGGLoX5tvU+sWgXCVB87pTjU5Nef6Xw=
-----END CERTIFICATE-----

5. We now have three files: “request.pem”, “cert.cer”, and “key.pem”. Use the command below to generate a file named “file.p12.” A password is applied to the “file.p12” file. The “file.p12” file is a PFX formatted file of the private key and certificate. Once this process is completed destroy the “key.pem” file.

   Once generated the PFX file is ready for import. The friendly name of the installed certificate is “server”. After the certificate is installed and confirmed, the PFX file should be stored securely.

```
C:\temp>  openssl pkcs12 -export -name "server" -inkey key.pem -in cert.cer -out file.p12

Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:
```

6. A complete key store will also need the root certificate and intermediate certificate for the TOCA. These are available as a bundle from http://pki.treas.gov/toca_fullpath.p7b. In the case of some key stores it may be necessary to import the root certificate and intermediate certificate before importing the user certificate.