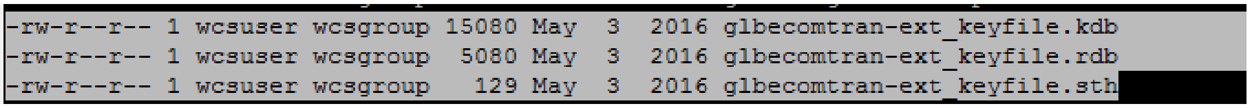
SSL Certificate renewal steps, (for web servers only ssl is there)

- First we have to backup in server in which we are going to do certificate renewal. For that login to that server through particular(wcs,oms,cto,wesb) build server as wcsuser,
- For c0006107,(Build servers ask username & password for wcsuser)

Wcsuser
EtrProd#@741

Sample server,
Ssh g1t2999g.austin.hp.com

cd /opt/apps/IBM/HTTPServer/conf



```
-rw-r--r-- 1 wcsuser wcsgroup 15080 May  3  2016 glbecomtran-ext_keyfile.kdb
-rw-r--r-- 1 wcsuser wcsgroup  5080 May  3  2016 glbecomtran-ext_keyfile.rdb
-rw-r--r-- 1 wcsuser wcsgroup   129 May  3  2016 glbecomtran-ext_keyfile.sth
```

Take backup of above three latest files. (cp filename bkp_filename)

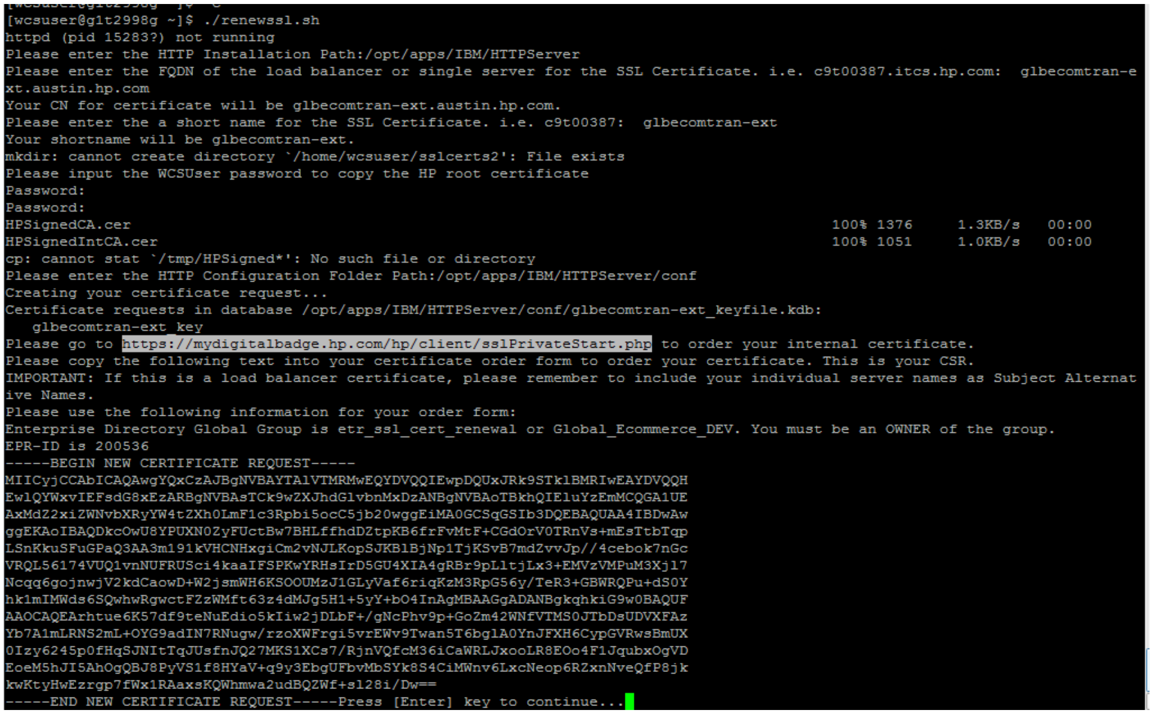
Renew the SSL cert

1. Login to the HIS(web) server as wcsuser. For load balanced certs, log in to one of the IHS servers. Path: /home/wcsuser
   ./renewssl.sh

It will ask password **Ecommerce@2016**

2. At the first prompt asking for the installation path just hit ENTER
3. At the next prompt,
   1. If this SSL cert is for a **single server**, enter the server FQDN (Ex. **c0008101.itcs.hp.com**).
   2. If this server is **load balanced**, enter the full FQDN of the load balancer. (Ex. **glbecomtran-wcsweb-dev7.glb.itcs.hp.com**)
4. At the next prompt, enter the short name of the FQDN above. (**c0008101** or **glbecomtran-wcsweb-dev7**)
   Give password When it prompts.
5. Next, you should see the path to the httpd.conf file which should be /opt/apps/IBM/HTTPServer/conf. Hit ENTER.

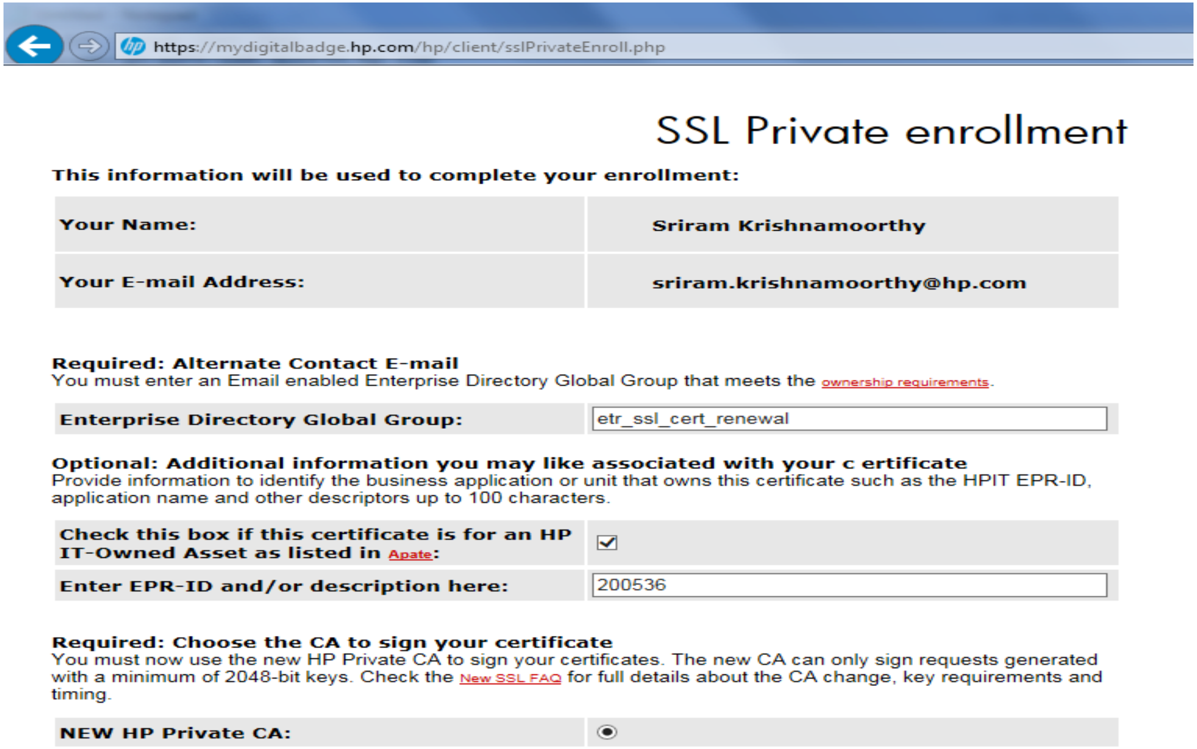
Refer the below screenshots for above mentioned steps,



```
[wcsuser@g1t2998g ~]$ ./renewssl.sh
httpd (pid 15283?) not running
Please enter the HTTP Installation Path:/opt/apps/IBM/HTTPServer
Please enter the FQDN of the load balancer or single server for the SSL Certificate. i.e. c9t00387.itcs.hp.com:  glbecomtran-e
xt.austin.hp.com
Your CN for certificate will be glbecomtran-ext.austin.hp.com.
Please enter the a short name for the SSL Certificate. i.e. c9t00387:  glbecomtran-ext
Your shortname will be glbecomtran-ext.
mkdir: cannot create directory `/home/wcsuser/sslcerts2': File exists
Please input the WCSUser password to copy the HP root certificate
Password:
Password:
HPSignedCA.cer                                                                             100% 1376     1.3KB/s   00:00
HPSignedIntCA.cer                                                                          100% 1051     1.0KB/s   00:00
cp: cannot stat `/tmp/HPSigned*': No such file or directory
Please enter the HTTP Configuration Folder Path:/opt/apps/IBM/HTTPServer/conf
Creating your certificate request...
Certificate requests in database /opt/apps/IBM/HTTPServer/conf/glbecomtran-ext_keyfile.kdb:
   glbecomtran-ext_key
Please go to https://mydigitalbadge.hp.com/hp/client/sslPrivateStart.php to order your internal certificate.
Please copy the following text into your certificate order form to order your certificate. This is your CSR.
IMPORTANT: If this is a load balancer certificate, please remember to include your individual server names as Subject Alternat
ive Names.
Please use the following information for your order form:
Enterprise Directory Global Group is etr_ssl_cert_renewal or Global_Ecommerce_DEV. You must be an OWNER of the group.
EPR-ID is 200536
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICyjCCAbICAQAwgYQxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDQUxJRk9STklBMRIwEAYDVQQH
EwlQYWxvIEFsdG8xEzARBgNVBAsTCk9wZXJhdGlvbnMxDzANBgNVBAoTBkhQIEluYzEmMCQGA1UE
AxMdZ2xiZWNvbXRyYW4tZXh0LmF1c3Rpbi5ocC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDkcOwU8YPUXN0ZyFUctBw7BHLffhdDZtpKB6frFvMtF+CGdOrV0TRnVs+mEsTtbTqp
LSnKkuSFuGPaQ3AA3m191kVHCNHxgiCm2vNJLKopSJKBlBjNp1TjKSvB7mdZvvJp//4cebok7nGc
VRQL56174VUQ1vnNUFRUSci4kaaIFSPKwYRHsIrD5GU4XIA4gRBr9pLltjLx3+EMVzVMPuM3Xjl7
Ncqq6gojnwjV2kdCaowD+W2jsmWH6KSOOUMzJ1GLyVaf6riqKzM3RpG56y/TeR3+GBWRQPu+dS0Y
hk1mIMWds6SQwhwRgwctFZzWMft63z4dMJg5H1+5yY+bO4InAgMBAAGgADANBgkqhkiG9w0BAQUF
AAOCAQEArhtue6K57df9teNuEdio5kIiw2jDLbF+/gNcPhv9p+GoZm42WNfVTMS0JTbDsUDVXFAz
Yb7A1mLRNS2mL+OYG9adIN7RNugw/rzoXWFrgi5vrEWv9Twan5T6bglA0YnJFXH6CypGVRwsBmUX
0Izy6245p0fHqSJNItTqJUsfnJQ27MKS1XCs7/RjnVQfcM36iCaWRLJxooLR8EOo4F1JqubxOgVD
EoeM5hJI5AhOgQBJ8PyVS1f8HYaV+q9y3EbgUFbvMbSYk8S4CiMWnv6LxcNeop6RZxnNveQfP8jk
kwKtyHwEzrgp7fWx1RAaxsKQWhmwa2udBQZWf+sl28i/Dw==
-----END NEW CERTIFICATE REQUEST-----Press [Enter] key to continue...
```

6. Follow the on screen instructions. Go to this link https://mydigitalbadge.hp.com/hp/client/sslPrivateStart.php and fill out all the information.

Please find the screenshot below and fill the details as per mentioned in the screenshot



https://mydigitalbadge.hp.com/hp/client/sslPrivateEnroll.php

SSL Private enrollment

This information will be used to complete your enrollment:

Your Name:	**Sriram Krishnamoorthy**
Your E-mail Address:	**sriram.krishnamoorthy@hp.com**

Required: Alternate Contact E-mail
You must enter an Email enabled Enterprise Directory Global Group that meets the ownership requirements.

Enterprise Directory Global Group:	etr_ssl_cert_renewal

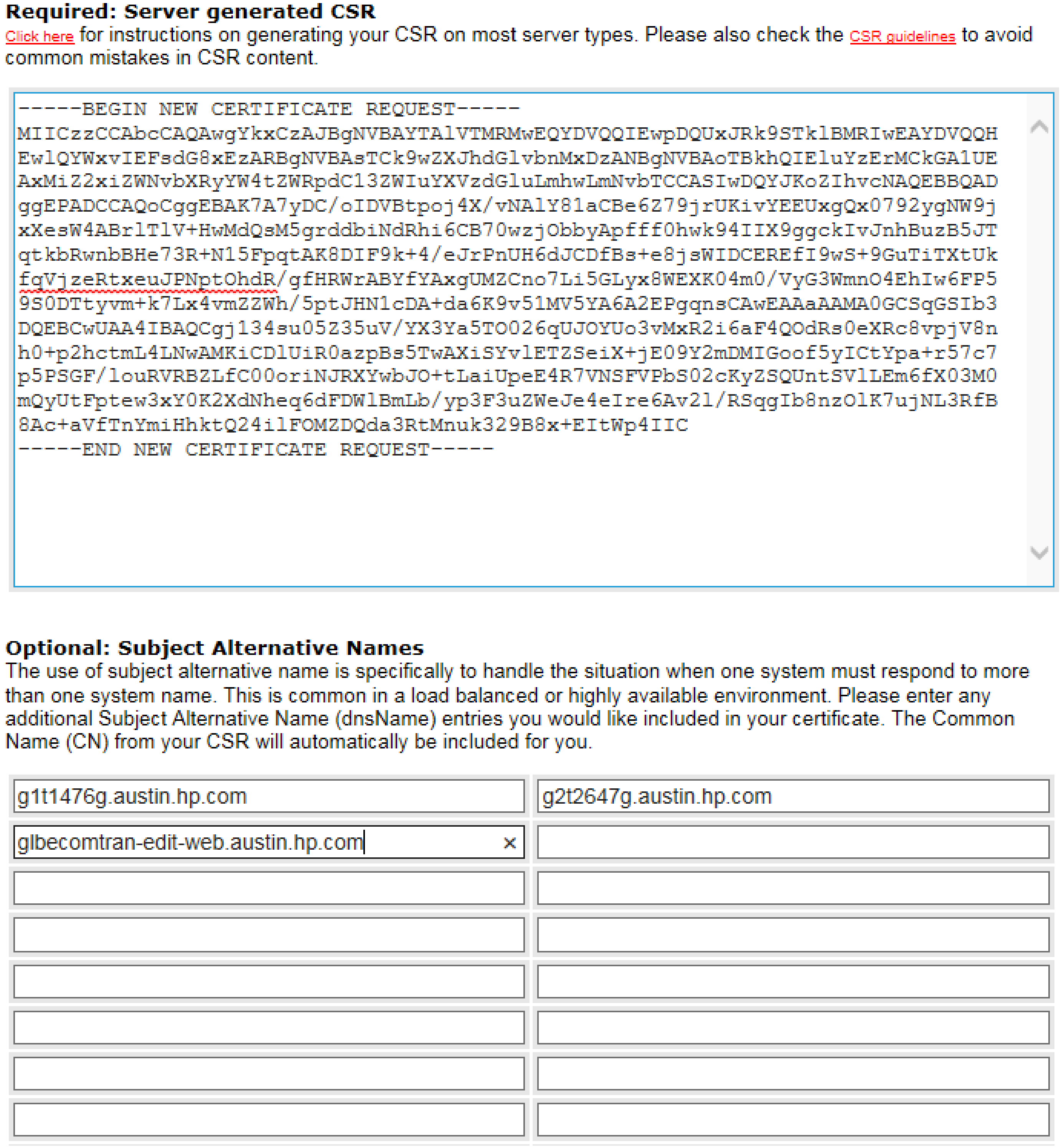
Optional: Additional information you may like associated with your c ertificate
Provide information to identify the business application or unit that owns this certificate such as the HPIT EPR-ID, application name and other descriptors up to 100 characters.

Check this box if this certificate is for an HP IT-Owned Asset as listed in Apate:	☑
Enter EPR-ID and/or description here:	200536

Required: Choose the CA to sign your certificate
You must now use the new HP Private CA to sign your certificates. The new CA can only sign requests generated with a minimum of 2048-bit keys. Check the New SSL FAQ for full details about the CA change, key requirements and timing.

NEW HP Private CA:	●

Below Is example of certificate key generation you give the details according to what you have generated: (in the server we are working copy in putty and paste here and server names you are going to do ssl)



Required: Server generated CSR

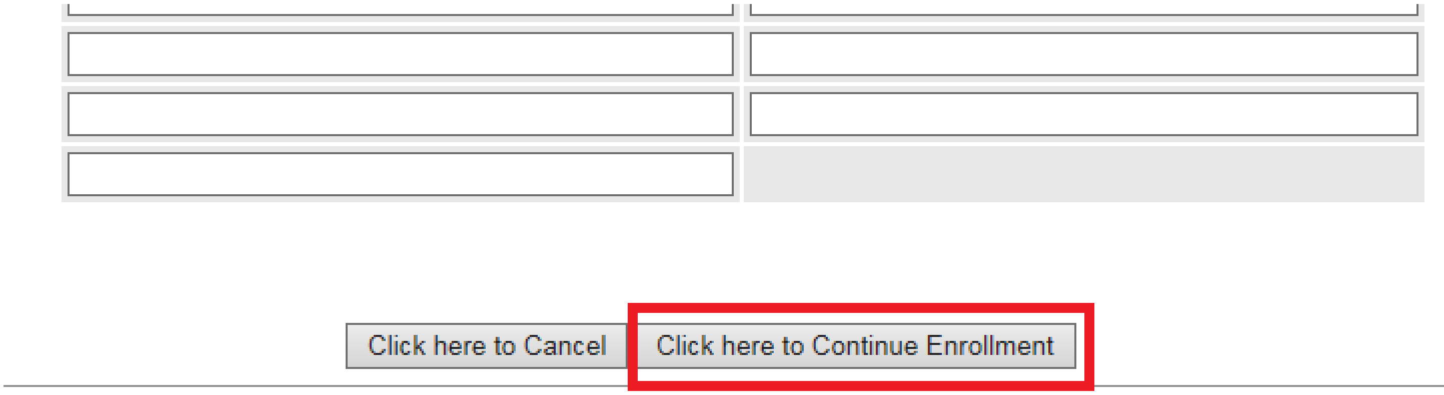
Click here for instructions on generating your CSR on most server types. Please also check the CSR guidelines to avoid common mistakes in CSR content.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICzzCCAbcCAQAwgYkxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDQUxJRk9STklBMRIwEAYDVQQH
EwlQYWxvIEFsdG8xEzARBgNVBAsTCk9wZXJhdGlvbnMxDzANBgNVBAoTBkhQIEluYzErMCkGA1UE
AxMiZ2xiZWNvbXRyYW4tZWRpdC13ZWIuYXVzdGluLmhwLmNvbTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAK7A7yDC/oIDVBtpoj4X/vNAlY81aCBe6Z79jrUKivYEEUxgQx0792ygNW9j
xXesW4ABrlTlV+HwMdQsM5grddbiNdRhi6CB70wzjObbyApfff0hwk94IIX9ggckIvJnhBuzB5JT
qtkbRwnbBHe73R+N15FpqtAK8DIF9k+4/eJrPnUH6dJCDfBs+e8jsWIDCEREfI9wS+9GuTiTXtUk
fqVjzeRtxeuJPNptOhdR/gfHRWrABYfYAxgUMZCno7Li5GLyx8WEXK04m0/VyG3WmnO4EhIw6FP5
9S0DTtyvm+k7Lx4vmZZWh/5ptJHN1cDA+da6K9v51MV5YA6A2EPgqnsCAwEAAaAAMA0GCSqGSIb3
DQEBCwUAA4IBAQCgj134su05Z35uV/YX3Ya5TO026qUJOYUo3vMxR2i6aF4QOdRs0eXRc8vpjV8n
h0+p2hctmL4LNwAMKiCDlUiR0azpBs5TwAXiSYvlETZSeiX+jE09Y2mDMIGoof5yICtYpa+r57c7
p5PSGF/louRVRBZLfC00oriNJRXYwbJO+tLaiUpeE4R7VNSFVPbS02cKyZSQUntSVlLEm6fX03M0
mQyUtFptew3xY0K2XdNheq6dFDWlBmLb/yp3F3uZWeJe4eIre6Av2l/RSqgIb8nzOlK7ujNL3RfB
8Ac+aVfTnYmiHhktQ24ilFOMZDQda3RtMnuk329B8x+EItWp4IIC
-----END NEW CERTIFICATE REQUEST-----
```

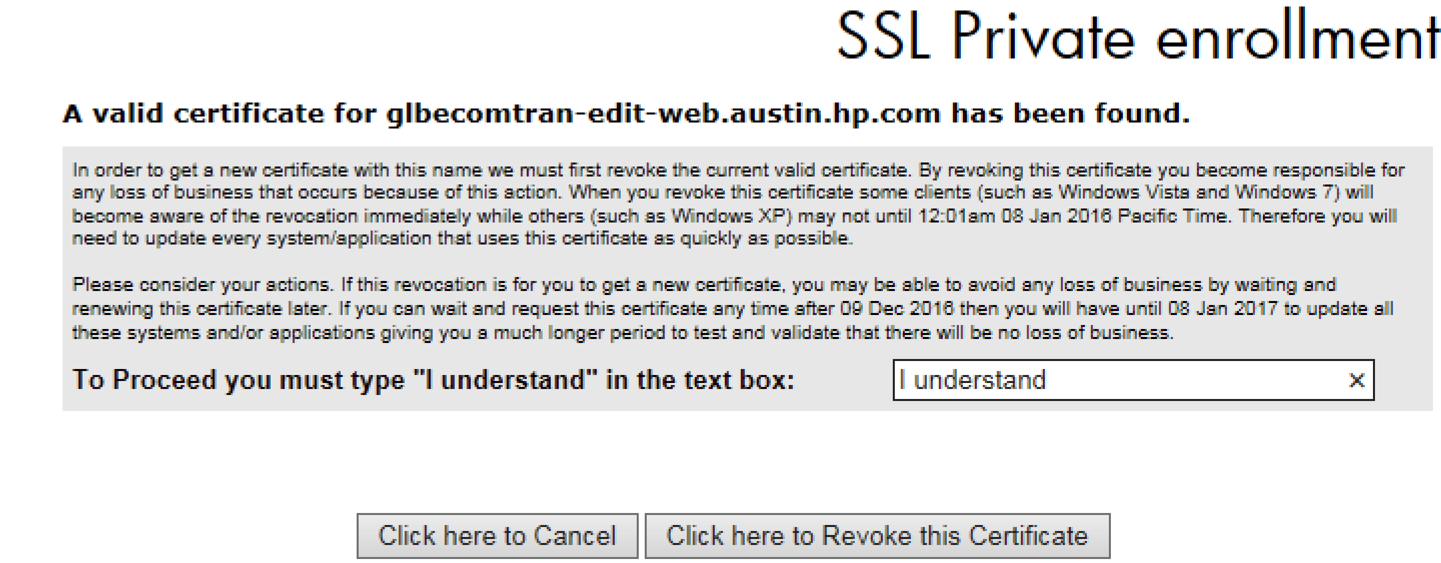
Optional: Subject Alternative Names

The use of subject alternative name is specifically to handle the situation when one system must respond to more than one system name. This is common in a load balanced or highly available environment. Please enter any additional Subject Alternative Name (dnsName) entries you would like included in your certificate. The Common Name (CN) from your CSR will automatically be included for you.

g1t1476g.austin.hp.com	g2t2647g.austin.hp.com
glbecomtran-edit-web.austin.hp.com ×	



In Next page:



SSL Private enrollment

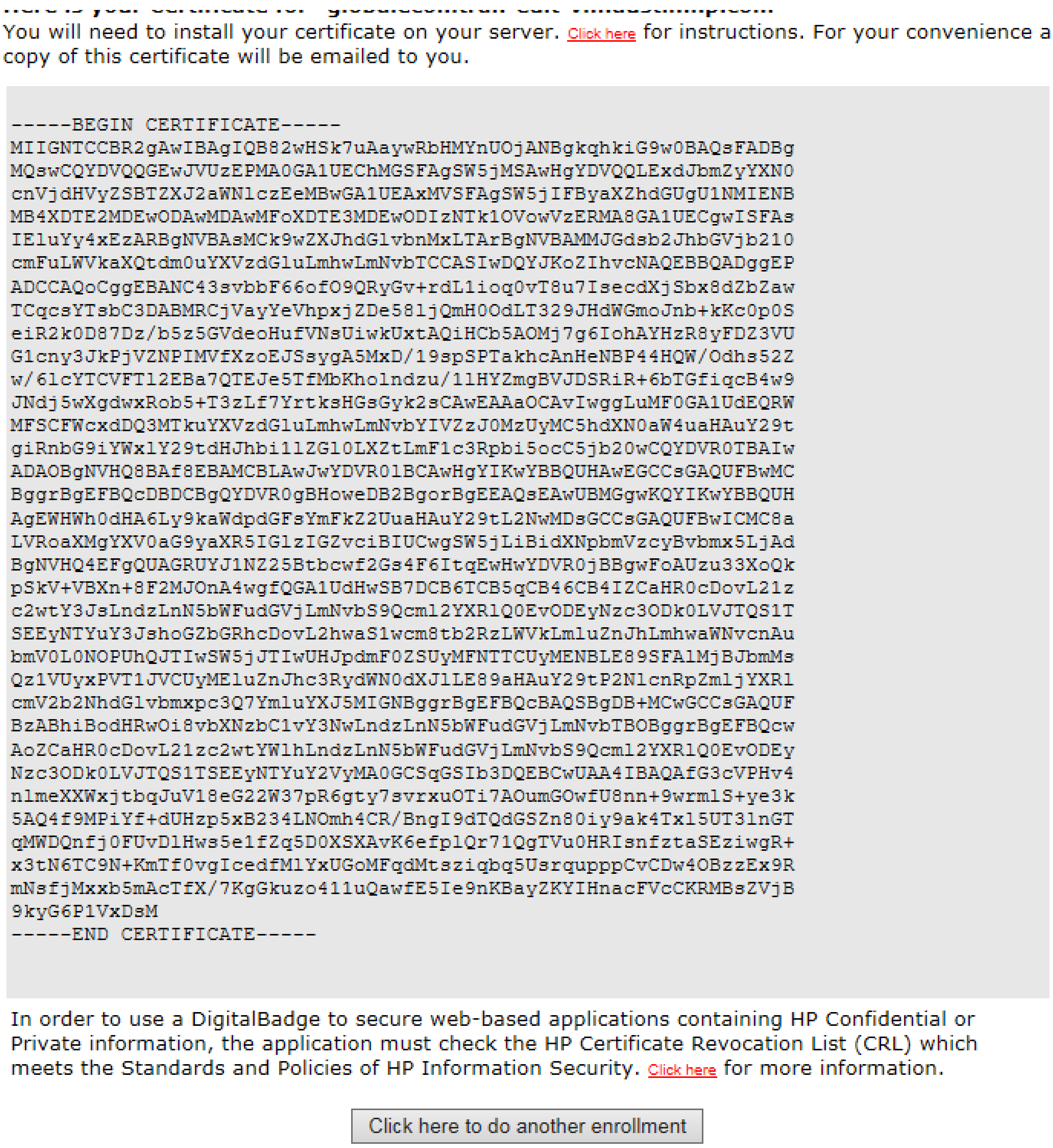
A valid certificate for glbecomtran-edit-web.austin.hp.com has been found.

In order to get a new certificate with this name we must first revoke the current valid certificate. By revoking this certificate you become responsible for any loss of business that occurs because of this action. When you revoke this certificate some clients (such as Windows Vista and Windows 7) will become aware of the revocation immediately while others (such as Windows XP) may not until 12:01am 08 Jan 2016 Pacific Time. Therefore you will need to update every system/application that uses this certificate as quickly as possible.

Please consider your actions. If this revocation is for you to get a new certificate, you may be able to avoid any loss of business by waiting and renewing this certificate later. If you can wait and request this certificate any time after 09 Dec 2016 then you will have until 08 Jan 2017 to update all these systems and/or applications giving you a much longer period to test and validate that there will be no loss of business.

To Proceed you must type "I understand" in the text box: I understand

Copy the certificate from this below page and paste it in Unix box:



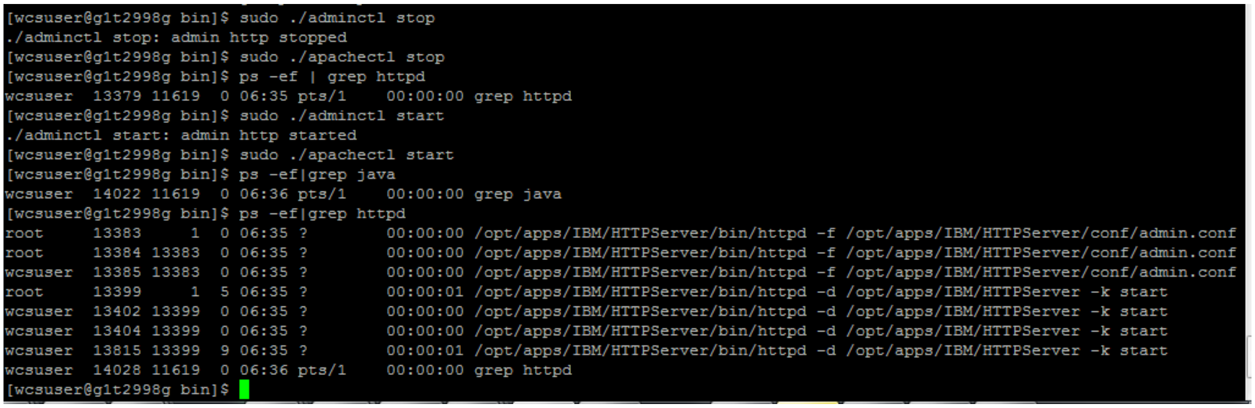
You will need to install your certificate on your server. Click here for instructions. For your convenience a copy of this certificate will be emailed to you.

```
-----BEGIN CERTIFICATE-----
MIIGNTCCBR2gAwIBAgIQB82wHSk7uAaywRbHMYnUOjANBgkqhkiG9w0BAQsFADBg
MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGSFAgSW5jMSAwHgYDVQQLExdJbmZyYXN0
cnVjdHVyZSBTZXJ2aWNlczEeMBwGA1UEAxMVSFAgSW5jIFByaXZhdGUgU1NMIENB
MB4XDTE2MDEwODAwMDAwMFoXDTE3MDEwODIzNTk1OVowVzERMA8GA1UECgwISFAs
IEluYy4xEzARBgNVBAsMCk9wZXJhdGlvbnMxLTArBgNVBAMMJGdsb2JhbGVjb210
cmFuLWVkaXQtdm0uYXVzdGluLmhwLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBANC43svbbF66ofO9QRyGv+rdL1ioq0vT8u7IsecdXjSbx8dZbZaw
TCqcsYTsbC3DABMRCjVayYeVhpxjZDe58ljQmH0OdLT329JHdWGmoJnb+kKc0p0S
eiR2k0D87Dz/b5z5GVdeoHufVNsUiwkUxtAQiHCb5AOMj7g6IohAYHzR8yFDZ3VU
G1cny3JkPjVZNPIMVfXzoEJSsygA5MxD/19spSPTakhcAnHeNBP44HQW/Odhs52Z
w/6lcYTCVFTl2EBa7QTEJe5TfMbKholndzu/1lHYZmgBVJDSRiR+6bTGfiqcB4w9
JNdj5wXgdwxRob5+T3zLf7YrtksHGsGyk2sCAwEAAaOCAvIwggLuMF0GA1UdEQRW
MFSCFWcxdDQ3MTkuYXVzdGluLmhwLmNvbYIVZzJ0MzUyMC5hdXN0aW4uaHAuY29t
giRnbG9iYWxlY29tdHJhbi1lZG10LXZtLmF1c3Rpbi5ocC5jb20wCQYDVR0TBAIw
ADAOBgNVHQ8BAf8EBAMCBLAwJwYDVR0lBCAwHgYIKwYBBQUHAwEGCCsGAQUFBwMC
BggrBgEFBQcDBDCBgQYDVR0gBHoweDB2BgorBgEEAQsEAwUBMGgwKQYIKwYBBQUH
AgEWHWh0dHA6Ly9kaWdpdGFsYmFkZ2UuaHAuY29tL2NwMDsGCCsGAQUFBwICMC8a
LVRoaXMgYXV0aG9yaXR5IGlzIGZvciBIUCwgSW5jLiBidXNpbmVzcyBvbmx5LjAd
BgNVHQ4EFgQUAGRUYJ1NZ25Btbcwf2Gs4F6ItqEwHwYDVR0jBBgwFoAUzu33XoQk
pSkV+VBXn+8F2MJOnA4wgfQGA1UdHwSB7DCB6TCB5qCB46CB4IZCaHR0cDovL21z
c2wtY3JsLndzLnN5bWFudGVjLmNvbS9Qcml2YXRlQ0EvODEyNzc3ODk0LVJTQS1T
SEEyNTYuY3JshoGZbGRhcDovL2hwaS1wcm8tb2RzLWVkLmluZnJhLmhwaWNvcnAu
bmV0L0NOPUhQJTIwSW5jJTIwUHJpdmF0ZSUyMFNTTCUyMENBLE89SFAlMjBJbmMs
Qz1VUyxPVT1JVCUyMEluZnJhc3RydWN0dXJlLE89aHAuY29tP2NlcnRpZmljYXRl
cmV2b2NhdGlvbmxpc3Q7YmluYXJ5MIGNBggrBgEFBQcBAQSBgDB+MCwGCCsGAQUF
BzABhiBodHRwOi8vbXNzbC1vY3NwLndzLnN5bWFudGVjLmNvbTBOBggrBgEFBQcw
AoZCaHR0cDovL21zc2wtYWlhLndzLnN5bWFudGVjLmNvbS9Qcml2YXRlQ0EvODEy
Nzc3ODk0LVJTQS1TSEEyNTYuY2VyMA0GCSqGSIb3DQEBCwUAA4IBAQAfG3cVPHv4
nlmeXXWxjtbqJuV18eG22W37pR6gty7svrxuOTi7AOumGOwfU8nn+9wrmlS+ye3k
5AQ4f9MPiYf+dUHzp5xB234LNOmh4CR/BngI9dTQdGSZn80iy9ak4Txl5UT3lnGT
qMWDQnfj0FUvDlHws5e1fZq5D0XSXAvK6efplQr71QgTVu0HRIsnfztaSEziwgR+
x3tN6TC9N+KmTf0vgIcedfMlYxUGoMFqdMtsziqbq5UsrqupppCvCDw4OBzzEx9R
mNsfjMxxb5mAcTfX/7KgGkuzo4l1uQawfE5Ie9nKBayZKYIHnacFVcCKRMBsZVjB
9kyG6P1VxDsM
-----END CERTIFICATE-----
```

In order to use a DigitalBadge to secure web-based applications containing HP Confidential or Private information, the application must check the HP Certificate Revocation List (CRL) which meets the Standards and Policies of HP Information Security. Click here for more information.

Copy this key to putty server where we are working, After pasting this in Unix server press “ctrl D” twice and it will create certificate key files in /opt/apps/IBM/HTTPServer/conf folder, copy the three key files to other web servers in path: /opt/apps/IBM/HTTPServer/conf.

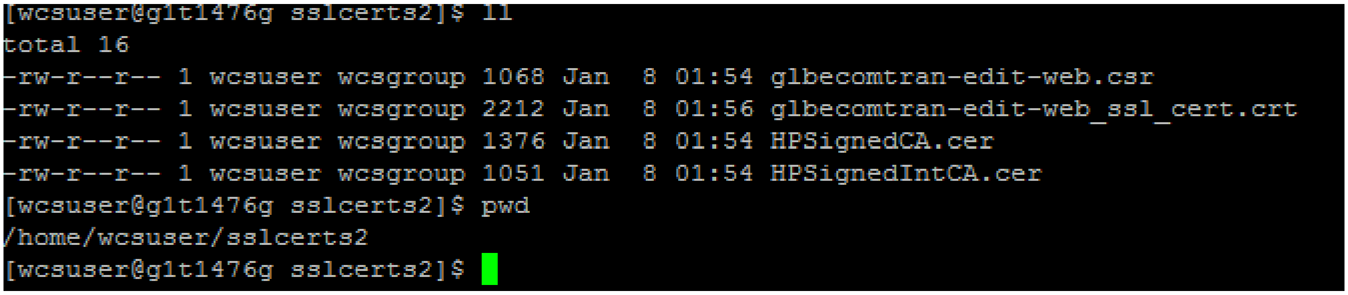
Last step: Restart web servers.
To restart web servers follow screenshot steps,



```
[wcsuser@g1t2998g bin]$ sudo ./adminctl stop
./adminctl stop: admin http stopped
[wcsuser@g1t2998g bin]$ sudo ./apachectl stop
[wcsuser@g1t2998g bin]$ ps -ef | grep httpd
wcsuser  13379 11619  0 06:35 pts/1    00:00:00 grep httpd
[wcsuser@g1t2998g bin]$ sudo ./adminctl start
./adminctl start: admin http started
[wcsuser@g1t2998g bin]$ sudo ./apachectl start
[wcsuser@g1t2998g bin]$ ps -ef|grep java
wcsuser  14022 11619  0 06:36 pts/1    00:00:00 grep java
[wcsuser@g1t2998g bin]$ ps -ef|grep httpd
root     13383     1  0 06:35 ?        00:00:00 /opt/apps/IBM/HTTPServer/bin/httpd -f /opt/apps/IBM/HTTPServer/conf/admin.conf
root     13384 13383  0 06:35 ?        00:00:00 /opt/apps/IBM/HTTPServer/bin/httpd -f /opt/apps/IBM/HTTPServer/conf/admin.conf
wcsuser  13385 13383  0 06:35 ?        00:00:00 /opt/apps/IBM/HTTPServer/bin/httpd -f /opt/apps/IBM/HTTPServer/conf/admin.conf
root     13399     1  5 06:35 ?        00:00:01 /opt/apps/IBM/HTTPServer/bin/httpd -d /opt/apps/IBM/HTTPServer -k start
wcsuser  13402 13399  0 06:35 ?        00:00:00 /opt/apps/IBM/HTTPServer/bin/httpd -d /opt/apps/IBM/HTTPServer -k start
wcsuser  13404 13399  0 06:35 ?        00:00:00 /opt/apps/IBM/HTTPServer/bin/httpd -d /opt/apps/IBM/HTTPServer -k start
wcsuser  13815 13399  9 06:35 ?        00:00:01 /opt/apps/IBM/HTTPServer/bin/httpd -d /opt/apps/IBM/HTTPServer -k start
wcsuser  14028 11619  0 06:36 pts/1    00:00:00 grep httpd
[wcsuser@g1t2998g bin]$
```

And please check the site for latest SSL certificate date and expiry.

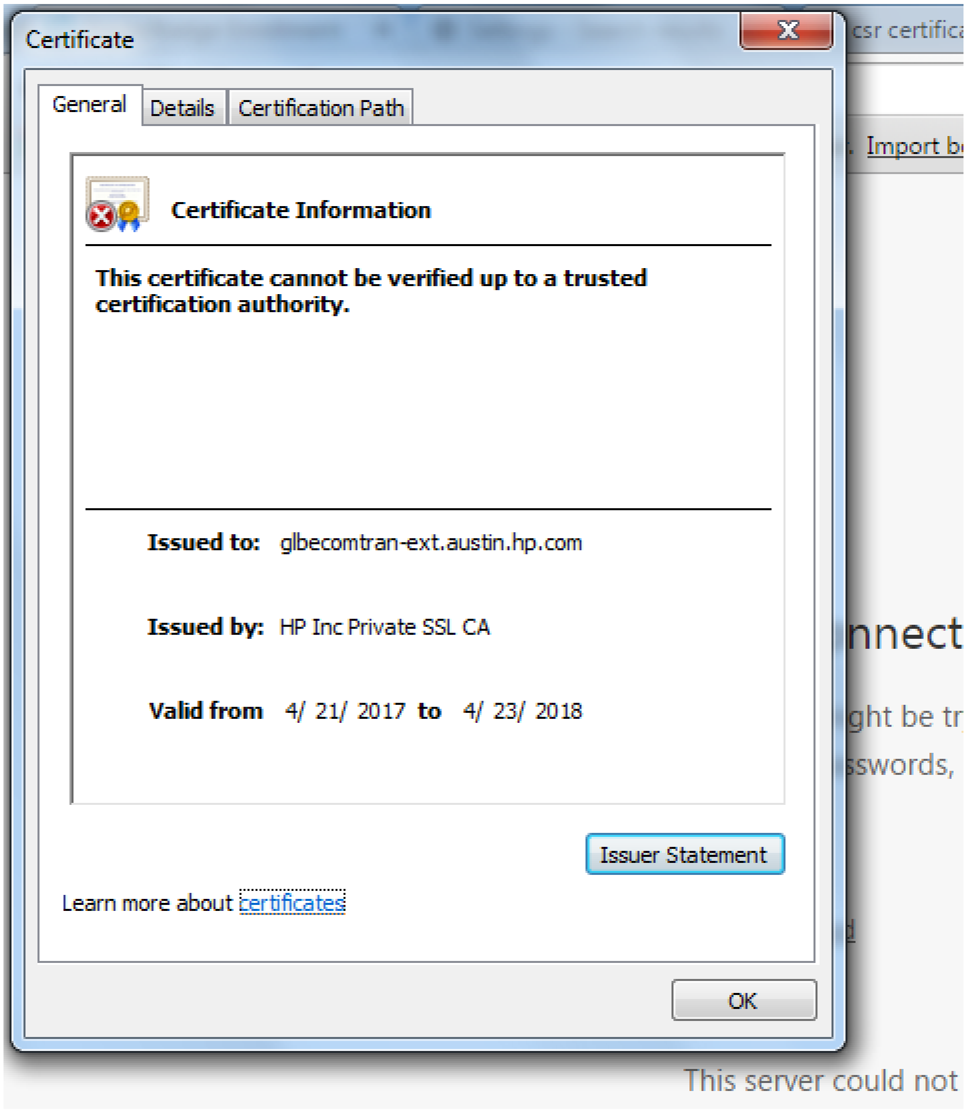
Note: Check in folder for latest file.



```
[wcsuser@g1t1476g sslcerts2]$ ll
total 16
-rw-r--r-- 1 wcsuser wcsgroup 1068 Jan  8 01:54 glbecomtran-edit-web.csr
-rw-r--r-- 1 wcsuser wcsgroup 2212 Jan  8 01:56 glbecomtran-edit-web_ssl_cert.crt
-rw-r--r-- 1 wcsuser wcsgroup 1376 Jan  8 01:54 HPSignedCA.cer
-rw-r--r-- 1 wcsuser wcsgroup 1051 Jan  8 01:54 HPSignedIntCA.cer
[wcsuser@g1t1476g sslcerts2]$ pwd
/home/wcsuser/sslcerts2
[wcsuser@g1t1476g sslcerts2]$
```

Below can be checked by, (For sample server)

https: g1t2999g.austin.hp.com(click on https lock symbol)



Certificate

Certificate Information

This certificate cannot be verified up to a trusted certification authority.

Issued to: glbecomtran-ext.austin.hp.com

Issued by: HP Inc Private SSL CA

Valid from 4/ 21/ 2017 **to** 4/ 23/ 2018

Learn more about certificates