How do I get a PEM certificate from Windows Server 2008 for IEEE 802.1x Network Authentication?

Answer:

If the certificate generated is in .DER format, you will need to convert it to .pfx before you can convert it to .PEM format for uploading to a PCoIP zero client or PCoIP host card.

Converting the certificate from .DER to .PEM

1. Install .DER certificate into the system local certificate store of a windows system.
2. Export the certificate including the private key which converts to a .PFX format.

Exporting a certificate into PFX format (PKC12) from Windows Server 2008:

Instructions: http://technet.microsoft.com/en-us/library/cc754329.aspx

Using Win32 OpenSSL to convert PFX to PEM:

Download: http://www.slproweb.com/products/Win32OpenSSL.html (light version will suffice)

Instructions:

1. Install Windows OpenSSL.
2. In a command prompt, enter the following:
   ```
   C:\OpenSSL-Win32\bin\openssl.exe pkcs12 –in <client_cert.pfx> –out <client_cert.pem> -nodes
   ```
3. Check if the private key in <client_cert.pem> has a ***RSA Private Key***.
   It should look something like this:

- Bag Attributes
  - localKeyID: 01 00 00 00
  - friendlyName: le-380a3f50-625c-4140-845a-db949bfdbbbb
  - Microsoft CSP Name: Microsoft RSA SChannel Cryptographic Provider
- Key Attributes
- X509v3 Key Usage: 10
- -----BEGIN RSA PRIVATE KEY-----
  ...
  -----END RSA PRIVATE KEY-----

Bag Attributes

- localKeyID: 01 00 00 00
- subject=/CN=pd02-test
- issuer=/DC=local/DC=serco/CN=serco-LAB-DC-01-CA
- -----BEGIN CERTIFICATE-----
  ...
  -----END CERTIFICATE----

If it does, then your certificate is ready to be uploaded to the zero client.

4. If it does not have a RSA private key, it will most likely look like this:

- Bag Attributes
    - localKeyID: 01 00 00 00
    - Microsoft CSP Name: Microsoft Enhanced Cryptographic Provider v1.0
    - friendlyName: 5b2aa662e1c98264443f1fb8439a8d55_70cf94c2-8d74-430a-87f4-f30f6b38972b
- Key Attributes
    - X509v3 Key Usage: 10
    - -----BEGIN PRIVATE KEY-----
...
-----END PRIVATE KEY-----
- Bag Attributes
    - localKeyID: 01 00 00 00
    - friendlyName: pcoip-portal-0012fbebf2b2
    - subject=/CN=pcoip-portal-0012fbebf2b2.area33.afnet3.usaf.mil
    - issuer=/DC=mil/DC=usaf/DC=afnet3/CN=A-SCA-00
    - -----BEGIN CERTIFICATE-----
…
-----END CERTIFICATE-----

5. Use OpenSSL to convert it to a RSA private key. In a command prompt enter the following:

```
C:\OpenSSL-Win32\bin\openssl.exe rsa –in <client_cert.pem> –out < client_cert_rsa_key.pem>
```

In <client_cert_rsa_key.pem>, only the RSA private key will be there. You will need to manually cut and paste the key into your original certificate (<client_cert.pem>) and replace the old key. Make sure the "-----BEGIN PRIVATE KEY-----" and "-----END PRIVATE KEY-----" are replaced with "-----BEGIN RSA PRIVATE KEY-----" and "-----END RSA PRIVATE KEY-----" as well.

6. Your certificate is now ready to be used with the zero client.

Important notes:

When setting up 802.1X on a zero client, you will need to make sure it has both a Server Certificate (the Root CA used to verify that we are authenticating with the correct server) and a Client Certificate (which needs to contain both the Private Key and Certificate all in one PEM file).

The Client PEM Certificate needs to have the Private Key in RSA format. You can check by verifying if the key tags are the following:

- "-----BEGIN RSA PRIVATE KEY-----"
- "-----END RSA PRIVATE KEY-----"

See Also: https://www.sslshopper.com/ssl-converter.html