

How to generate certificates using Microsoft CA for CCA

Assuming that you already have a CA in your enterprise, here's how you can generate the certificates for CCA devices from your CA:

First generate a CSR on the device you're trying to get a certificate for. I'm using a CAS for this example, so on the CAS browse to SSL -> X509 Certification Request and click on Generate Certificate Request. Fill out the information and click on Generate:

The screenshot shows the Cisco Clean Access Server Administration interface. The left sidebar contains navigation menus for Administration (Network Settings, Software Upload, SSL, Authorization, Time Server, Admin Password, Logout) and Monitoring (Active VPN Clients, Support Logs). The main content area is titled "Administration > SSL" and has three tabs: "X509 Certificate", "Trusted Certificate Authorities", and "X509 Certification Request". Below the tabs is an "Export" button. A table with a "Description" header lists two items: "Certification Request: CN=172.18.62.203,OU=IT,O=JLBSF Inc.,L=RTP,ST=NC,C=US" and "Private Key: RSA,1024 bits". Below the table is a "Hide" button and a form with the following fields: Full Domain Name or IP (14.36.147.45), Organization Unit Name (TAC), Organization Name (Cisco), City Name (RTP), State Name (NC), 2-letter Country Code (US), and RSA Key Size (1024). A "Generate" button is at the bottom of the form.

CAS will generate the CSR. Check mark the CSR and export it. You'll need this file to enter in your CA:

This screenshot shows the same "Administration > SSL" interface, but the "X509 Certification Request" tab is active. The "Export" button is now highlighted. The table shows the "Certification Request: CN=14.36.147.45,OU=TAC,O=Cisco,L=RTP,ST=NC,C=US" item selected with a checkmark in the first column. The "Private Key: RSA,1024 bits" item remains unselected.

How to generate certificates using Microsoft CA for CCA

Export the private key also and save that in a safe place. You'll need that for importing the certificate that you get back from the CA:

Administration > SSL

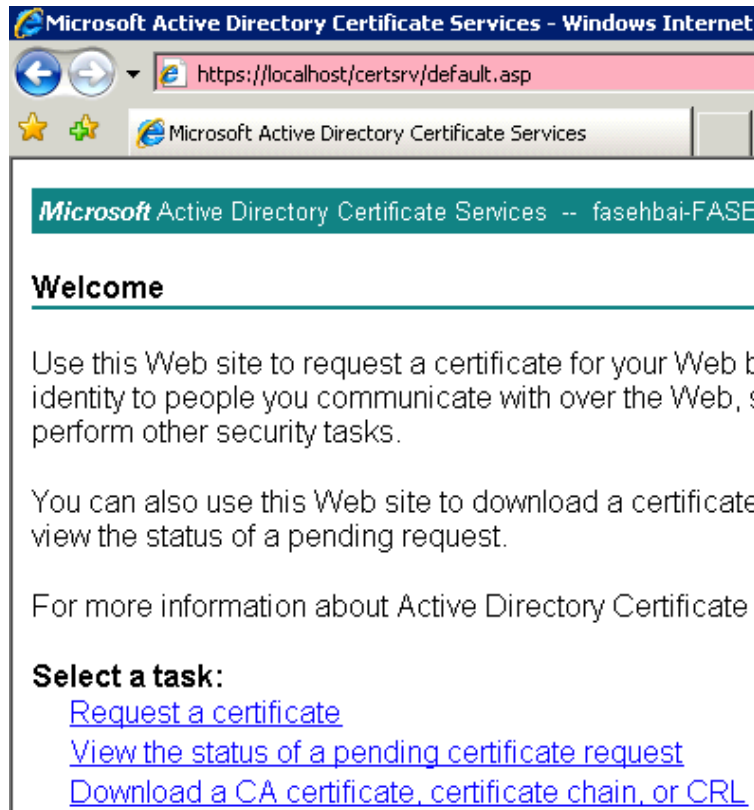
	Description
<input type="checkbox"/>	Certification Request: CN=14.36.147.45,OU=TAC,O=Cisco,L=RTP,ST=NC,C=US
<input checked="" type="checkbox"/>	Private Key: RSA,1024 bits

The CSR file should look like this in a text editor:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBmzCCAQQCAQAwxTELMakGA1UEBhMCVVMxCzAJBgNVBAGTAk5DMQwwCgYDVQ
EwNSVFAXDjAMBgNVBAoTBUNpc2NmMQwwCgYDVQLLEwNUQUxFTATBgNVBAMTD0
LjM2LjE0Ny40NTCBnzANBgkqhkiG9w0BAQEFAA0BjQAwgYkCgYEAp1NyUzmtiN
GFyHoznmflchUzpph2sEyket0FtTyWUerbLa9cYm4Go/2HeElGqZdvz2o7MOR
7H/sL/eUqbImEuw1AqLEX7o5xzILhr6w36phd2g1gwgXRpcSz07/Nhbuy+S4lf
qoyY1rV6lUxW+7Zh2yQshYhmGBVQhyEAWEAATANBgkqhkiG9w0BAQUFAA0BgL
GJNJQjlX2rcnSp8wvdTizchxbc5oCqbqhcmj54wbLL7JRn/FpUhybe3woM6WLh
zJ2Kc1leBW2Vbk+nFmhM1VX1SXLkSqBp2e+IHXSdsYGzIf6ENddLSmaxVCldG
oxJjfSmQIkAd2Z1Jhfpu8080AqoWwvyt49s0vth8Yw==
-----END CERTIFICATE REQUEST-----
```

How to generate certificates using Microsoft CA for CCA

Open the Certificate server's page by browsing to https://<IP_OF_CA>/certsrv/default.asp I'm using a Windows 2008 server as a CA for this document (***Make sure you're using an admin account to do this, or the necessary templates won't be available to you!***):



Click on Request a certificate:

Microsoft Active Directory Certificate Services -- f

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

How to generate certificates using Microsoft CA for CCA

Click on Advanced Certificate Request and click on “Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file”

Microsoft Active Directory Certificate Services -- fasehbai-FASEHBAI-W2K8-CA [Home](#)

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

[Create and submit a request to this CA.](#)

[Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

Paste the text from the Certificate Request file in the box labeled Saved Request, and choose Web Server from the Certificate Template:

Microsoft Active Directory Certificate Services -- fasehbai-FASEHBAI-W2K8

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded C generated by an external source (such as a Web server) in the Saved Request:

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	<pre>-----BEGIN CERTIFICATE REQUEST----- MIIBmzCCAQQCAQAwxTELMakGA1UEBhMCVVMxCzAJ EwNSVFAXDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQL LjM2LjEONy40NTCBnzANBgkqhkiG9wOBAQEFAAOB GFyHoznmflchUzpph2sEyketOftTyWUerbLa9cY: 7H/sL/eUqbImEuw1AqLEX7o5xzILhr6w36phd2g1</pre>
---	---

Certificate Template:

Additional Attributes:	<input type="text" value="Web Server"/>
Attributes:	<ul style="list-style-type: none">UserBasic EFSAdministratorEFS Recovery AgentWeb ServerSubordinate Certification Authority
<input type="button" value="Submit >"/>	

How to generate certificates using Microsoft CA for CCA

Click on Submit, and then choose Base 64 encoded. Click on Download Certificate:

Microsoft Active Directory Certificate Services -- fasehbai-FAST

Certificate Issued

The certificate you requested was issued to you.

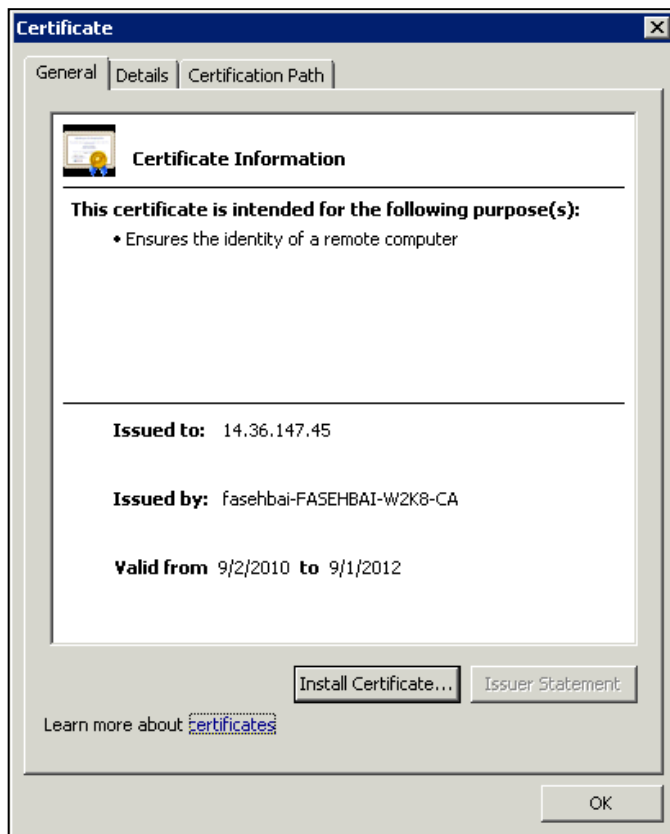
DER encoded or Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

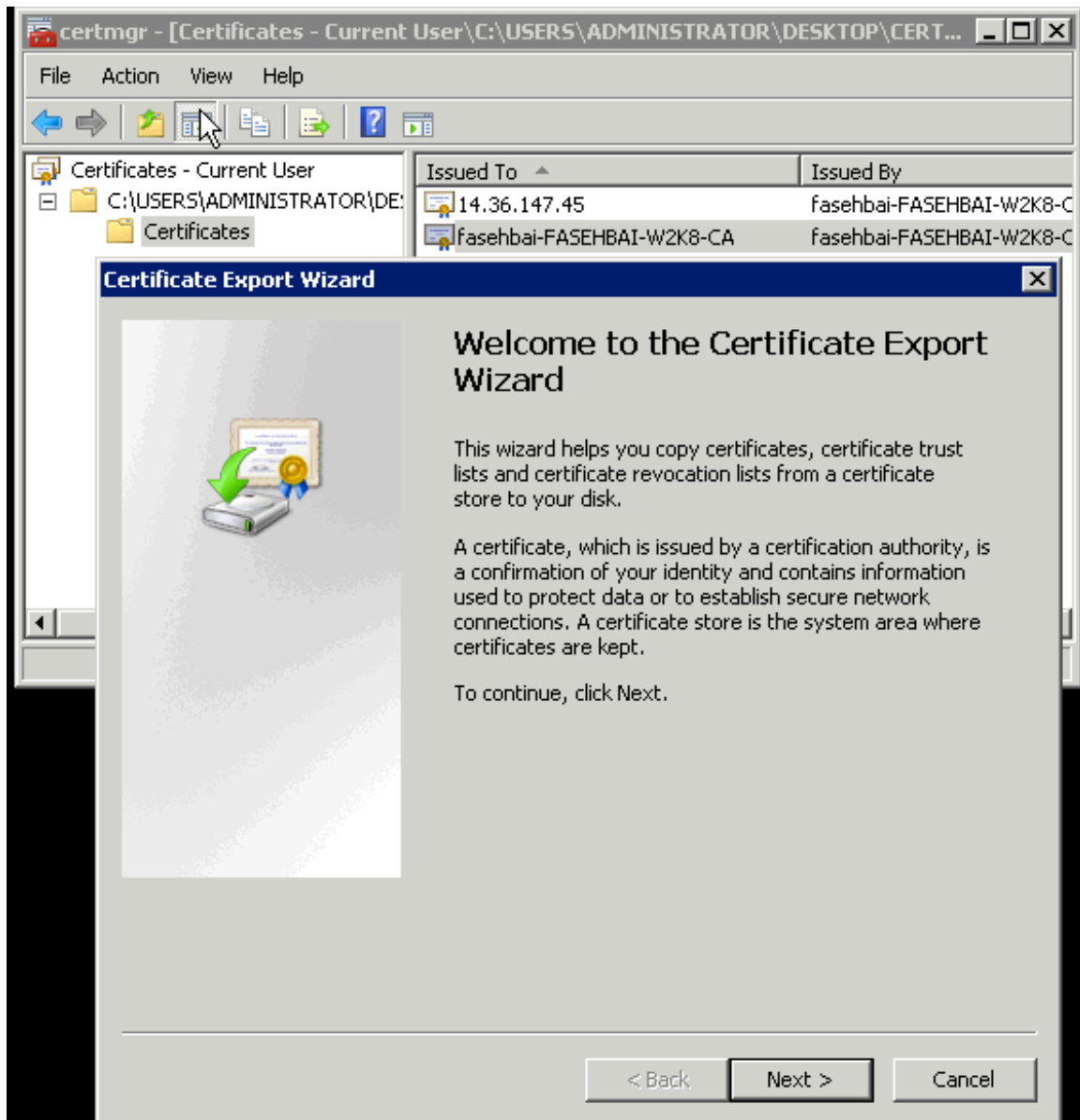
Also click on the Download Certificate Chain and save that in a safe place also. Now if you double click on the certificate it should show that it's issued by the CA:



How to generate certificates using Microsoft CA for CCA

Now at this point you should have four files. The CSR Request, the Private key, the Certificate file, and the Chain file. You will have to install the root certificate of the CA first in your CASs trusted root store, and then the identity certificate itself in the X509 store.

To install the root certificate, double click on the Chain file. On my setup it was named certnew.p7b Double click on the file and it opens in an Explorer like interface. Choose the root certificate file, Right click on it, and choose Export:

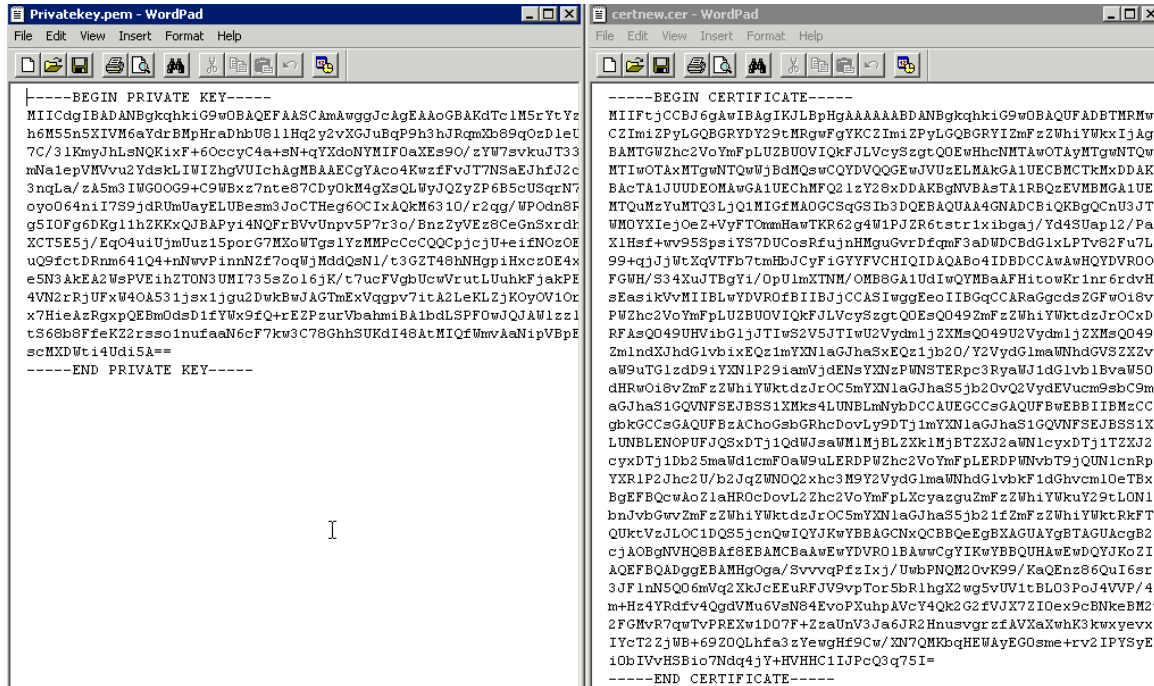


Go through the wizard, choosing Base 64 Encoded X.509 (CER), and saving the file. To import in your CAS, browse to SSL -> Trusted Certificate Authorities, click on Browse, and click on Import

How to generate certificates using Microsoft CA for CCA

Once root is installed, next step is to install the identity certificate itself. To install the certificate, you will need to combine the certificate and the private key into one file.

To do that, open the certificate and the private key both in notepad:



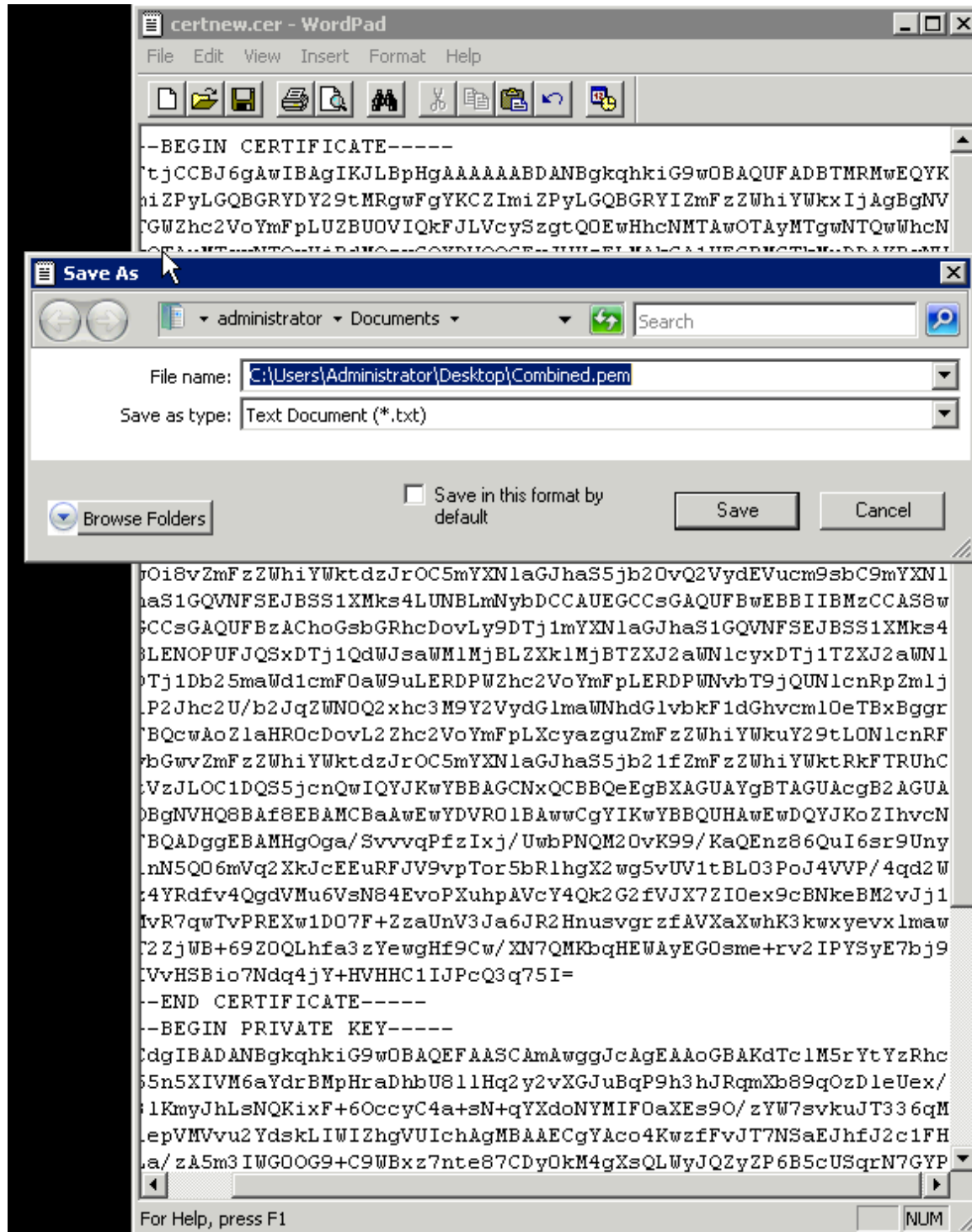
The image shows two Notepad windows side-by-side. The left window, titled 'Privatekey.pem - WordPad', contains a private key in PEM format. The right window, titled 'certnew.cer - WordPad', contains a certificate in PEM format. Both windows have standard Windows menus (File, Edit, View, Insert, Format, Help) and toolbars.

```
-----BEGIN PRIVATE KEY-----
MIICdgIBADANBgkqhkiG9w0BAQEFAAQAAgAgEAAoGBAKdTC1M5rYtYz
h6M5nSXIvM6aYdrBmpHrAdhbU811Hq2y2vXGJuBqP9h3hJRqmXb89QzD1eT
7C/31KmyJhLsNQRkixF60ccyC4a+sN+qYXdoNYMIF0aXEs90/zYU7svkuJT33
mNa1epVMVvu2YdskLIWIZhgVUIchAgMBAAEcGyAco4KwzfFvJT7NSaEJhfJ2c
3nqLa/zA5m3IWGOOG9+C9UBxz7nte87CDyOkM4gXsQLWYJQ2yZP6B5cUSqrN7
oyo064ni17S9jdRumUayELUBesm3JocTHeg6OCIXaQkM6310/r2qg/WPOdn8F
g5IOFg6DKg11hZKKxQJBAPy14NQFrBVvUnpv5P7r3c/BnzZyVEz8CeGnSxrdt
XCT5E5j/Eq04uiUjmUuz15porG7MXoWTgs1YzMMPcCQQCpcejU+eiFNzOE
uQ9fctDRm641Q4+nNvvp1nnNzf7oqUjMddQsNl/t3GZT48hNHgpiHxczOE4x
e5N3AkEA2WspVEihZTON3UMI735s2o16jK/t7ucFVgbUcwVr utLUuhkFjakPF
4VN2rRjUFxW40A531jsx1jgu2DwkBwJAGTmExVgqpv7itA2LeKLZjKoyOV1Or
x7HieAzRgxpQEEmOdsD1fYUx9fQ+REZPzurVbahmiBA1bdLSPFDWJQJAW1zz1
tS68b8FfeKZ2rso1nufaaN6cF7kw3C78GhhSUKdI48tMIQfWmvaAnipVBP
scMXDwt14Udi5A==
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIFtjCCBj6gAwIBAgIKJLBPgAAAAAABDANBgkqhkiG9w0BAQUFADBTMRMwE
CZIm1ZPyLQBGGRYDY29tMRgwFgYKCYZIm1ZPyLQBGGRYI2mFzZWhiYWkxIjAgE
BAhTGTWzHc2VoYmFpLUZBU0VlQkFJLVcySztgtQOEwHhcNMTAwOTAyMTg0NTQw
MTIwOTAxMTg0NTQwWjBdMQswCQYDVQQGEwJVUzELMAkGA1UECmCTkMxMjE1
BkAcTA1JUUDEOMAaGAIUEChMFQ21zY28xMjE1UEChMFQ21zY28xMjE1UECh
MTQwMzYyMTQ3LjQ1MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCnU3JTC
WMOYXiejOeZ+VyFTOmHawTKR62g4W1PJZR6tstr1xibgaJ/Yd45Uap12/Paj
X1Hsf+rv955ps1YS7DUCosRfujnHhguGvrdfgmF3adWDCBdG1xLPTv82Fu7L5
99+qjJjWtXqVTFb7cmHbJCyf1gYFFVCHIQAaBQa4IDBDCCAwAaHQYDVROE
FGWH/S34XwJTBgYi/OpUlmXTNM/OMB8GA1UdIwQYMBaAFHitowKr1nr6rdvHt
sEasikVvMIIBLWYDVROfEIBjCCASlWggEoIIBGQCARaGgcsZGFwOis8Vl
PUzhc2VoYmFpLUZBU0VlQkFJLVcySztgtQOEQ049ZmFzZWhiYWktdzJrOCxDT
RFAsQ049UHvibG1jUTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049C
2mldXJhdG1vbixEQzImYXN1aGJhaSxEXQz1jb20/Y2VydGhmaWVhdGVSZXZvY
aW9uTG1zdD9iYXN1P291amVjdENsYXNzPWNSTERpc3RyaWJldG1vb1EvaW50k
dHRwO18vZmFzZWhiYWktdzJrOC5mYXN1aGJhaS5jb20vQ2VydEVucm9sbC9mY
aGJhaS1GQVNFSEJBS1Xmks4LUNBLmNybDCAUEGCSsGAQUFBwEBB1IBMSCCAJ
gbkGCCsGAQUFBzAChocGsbGRhDovLy9DTj1mYXN1aGJhaS1GQVNFSEJBS1X
LUNBLENOPUFJQSxDTj1QdWJsaW1MjBL2Xk1MjBTZXJ2aWVudm1cyxDTj1LTZXJ2e
cyxDTj1Db25maWd1cmF0aW9uLERDPWZhc2VoYmFpLERDPUNvT9jQU1enRp2
YXR1P2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGhmaWVhdG1vbKf1dGhvcml0eTBxE
BgEFBQcwAoZ1aHR0cDovL2Zhc2VoYmFpLXcySztgtZmFzZWhiYWktdzJrOC5m
bnJvbGwvZmFzZWhiYWktdzJrOC5mYXN1aGJhaS5jb21fZmFzZWhiYWktdzJrOC
qUktVzJlOC1DQ55jcnQwIQYJKwYBAGNxcQBQeEgBxAGUAYgBTAGUAcgB2AJ
cJA0BQNVHQB8BAf8EBAMCBAAwEYDVRO1BAwwCgYIKwYBBQUHAwEwDQYJKoZI
hAEQFBQADggEBAMHgOga/SvvvqPzfIxj/UubPNQM2OvK99/KaQEnz86QuI6sr5
3JFlnN5Q06mVq2XkKjCEEuRFJV9vpTor5bR1hgX2wg5vUV1tBL03PoJ4VVP/4c
m+Hz4YRdfv4QgdVMu6VsN84EvoPXuhpAVcY4Qk2G2fVJX7Z10ex9cBNkE8M2v
2FGmVR7qtVPREXw1D07F+ZzaUnV3Ja6JR2HnsvgrzfAVXaXwhK3kwyeyvx1
IYcT2ZjWB+6920QLhfa3ZyewgHf9Cw/XN7QMKbQHEWYEGOsme+r+2IPYSyE7
10b1VvH3Bic7Ndq4jY+HVHHC1IJPcQ3q75I=
-----END CERTIFICATE-----
```

How to generate certificates using Microsoft CA for CCA

Copy the text from one window and paste into the other. Save the resulting notepad as Combined.pem



How to generate certificates using Microsoft CA for CCA

Now browse to the CAS where you are going to install the cert, SSL -> X509 Certificate tab, click on Browse, choose the Combined.pem file, and click on import.

This will install the certificate on the CAS. Reboot for the cert to take effect.

If this is an HA setup, repeat the above procedure on the other CAS.