

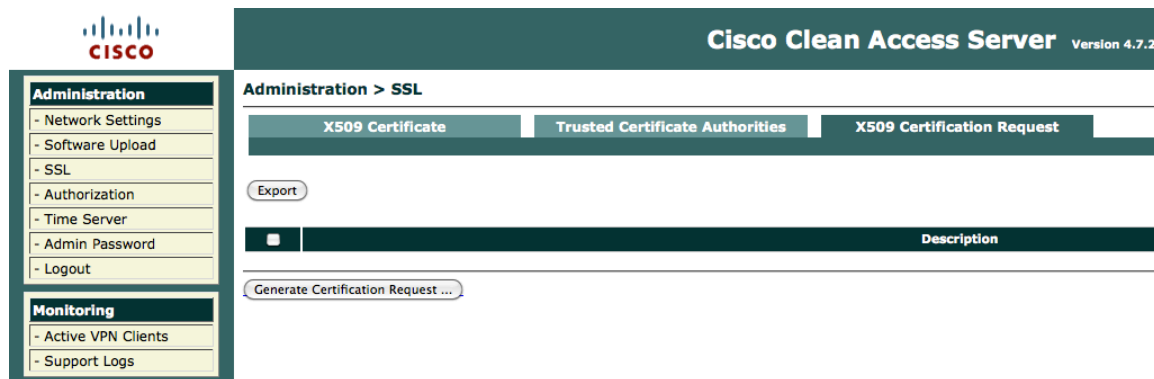
How to install a third party signed certificate on a CAS with self-signed CAM cert

For the sake of this document, I'm making these assumptions:

- 1 Standalone CAM with an IP address of 14.36.147.50
- 1 Standalone CAS with an IP address of 172.18.62.203
- Certificate of CAM is a true self-signed certificate (not signed by any third party)
- Certificate of CAS is going to be signed by a third party CA (We'll use Digicert for this example) which already has its root certificates in most of the common OS certificate stores


First step for this would be to generate a CSR (Certificate Signing Request), which we will send to Digicert, and they will return a certificate in return.

To get the CSR, go to the CAS admin page and Click on SSL -> X509 Certification Request:



The screenshot shows the Cisco Clean Access Server Administration interface. The top navigation bar includes the Cisco logo and the text "Cisco Clean Access Server Version 4.7.2". The main content area is titled "Administration > SSL" and contains three tabs: "X509 Certificate", "Trusted Certificate Authorities", and "X509 Certification Request". The "X509 Certification Request" tab is active. Below the tabs, there is an "Export" button and a table with a "Description" header. A "Generate Certification Request ..." button is located at the bottom of the page.

Click on Generate Certification Request and fill out the info:



Administration

- Network Settings
- Software Upload
- SSL
- Authorization
- Time Server
- Admin Password
- Logout

Monitoring

- Active VPN Clients
- Support Logs

Administration > SSL

X509 Certificate | Trust

Export

Hide

Full Domain Name or IP * 172.18.62.203

Organization Unit Name IT

Organization Name JLBSF Inc.

City Name RTP


State Name NC

2-letter Country Code US

RSA Key Size 1024

Generate

Click on Generate:



Cisco Clear

Administration

- Network Settings
- Software Upload
- SSL
- Authorization
- Time Server
- Admin Password
- Logout

Monitoring

- Active VPN Clients
- Support Logs

Administration > SSL

X509 Certificate

Trusted Certificate Authorities

[Export](#)

Certification Request: CN=172.18.62.203,OU=IT,O=JLBSF Inc.,L=RTP,ST=NC,C=US
 Private Key: RSA,1024 bits

[Hide](#)

Full Domain Name or IP *

Organization Unit Name

Organization Name

City Name

State Name

2-letter Country Code

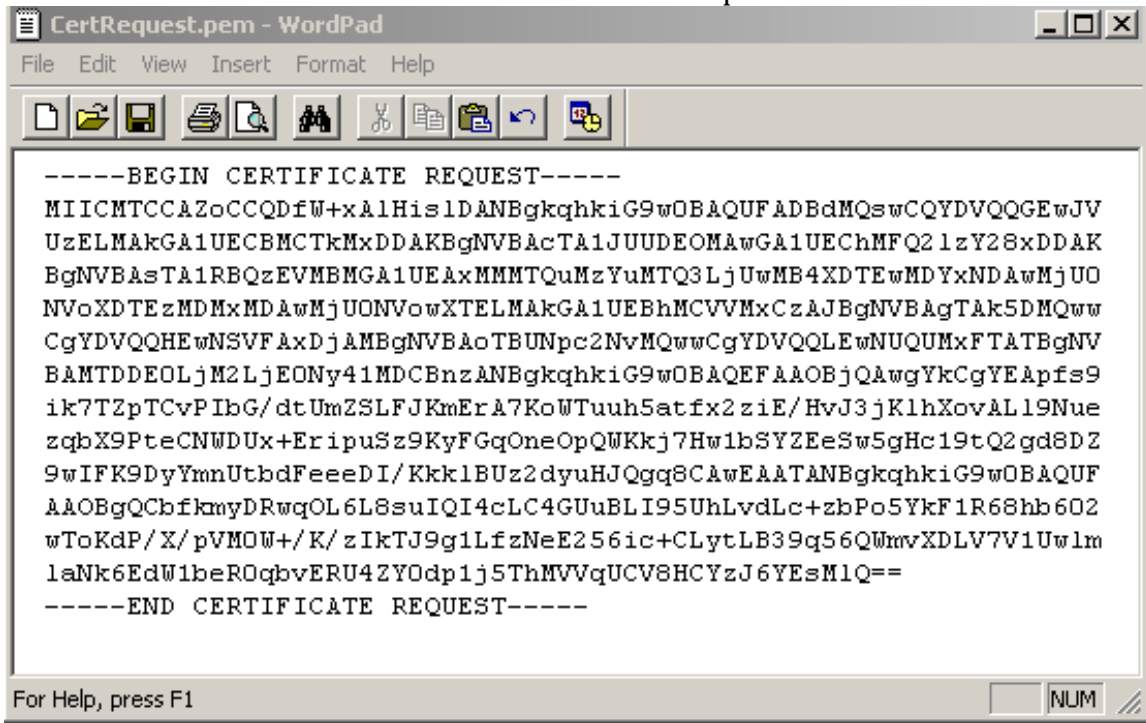
RSA Key Size

[Generate](#)

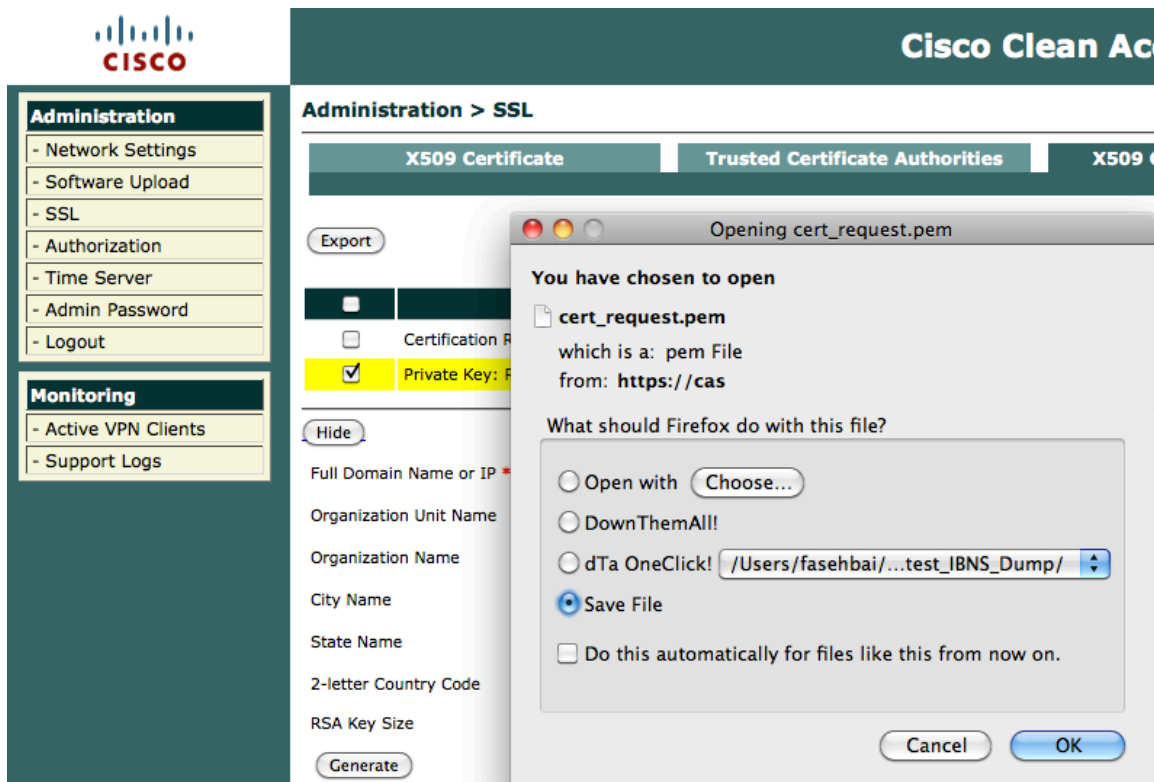
Checkmark the Certification Request and hit export. Save this file and you will send this CSR out to DigiCert:

The screenshot shows the Cisco ClearPass Administration console. The left sidebar contains navigation menus for Administration and Monitoring. The main content area is titled "Administration > SSL" and has two tabs: "X509 Certificate" and "Trusted Certificate Authorities". The "X509 Certificate" tab is active, showing a table of certificates. One certificate is selected, and the "Export" button is visible. A Firefox dialog box titled "Opening cert_request.pem" is overlaid on the console. The dialog box contains the following text: "You have chosen to open cert_request.pem which is a: pem File from: https://cas". Below this, it asks "What should Firefox do with this file?" and provides four options: "Open with Choose...", "DownThemAll!", "dTa OneClick! /Users/fasehbai/...test_IBNS_Dump/", and "Save File" (which is selected). There is also a checkbox for "Do this automatically for files like this from now on." and "Cancel" and "OK" buttons at the bottom.

Saved CSR would look like this when viewed in Wordpad:



Now checkmark the Private key and export it. **Save the private key in a safe place.** This private key is linked to the CSR and **you will need it when you get the certificate back from DigiCert:**



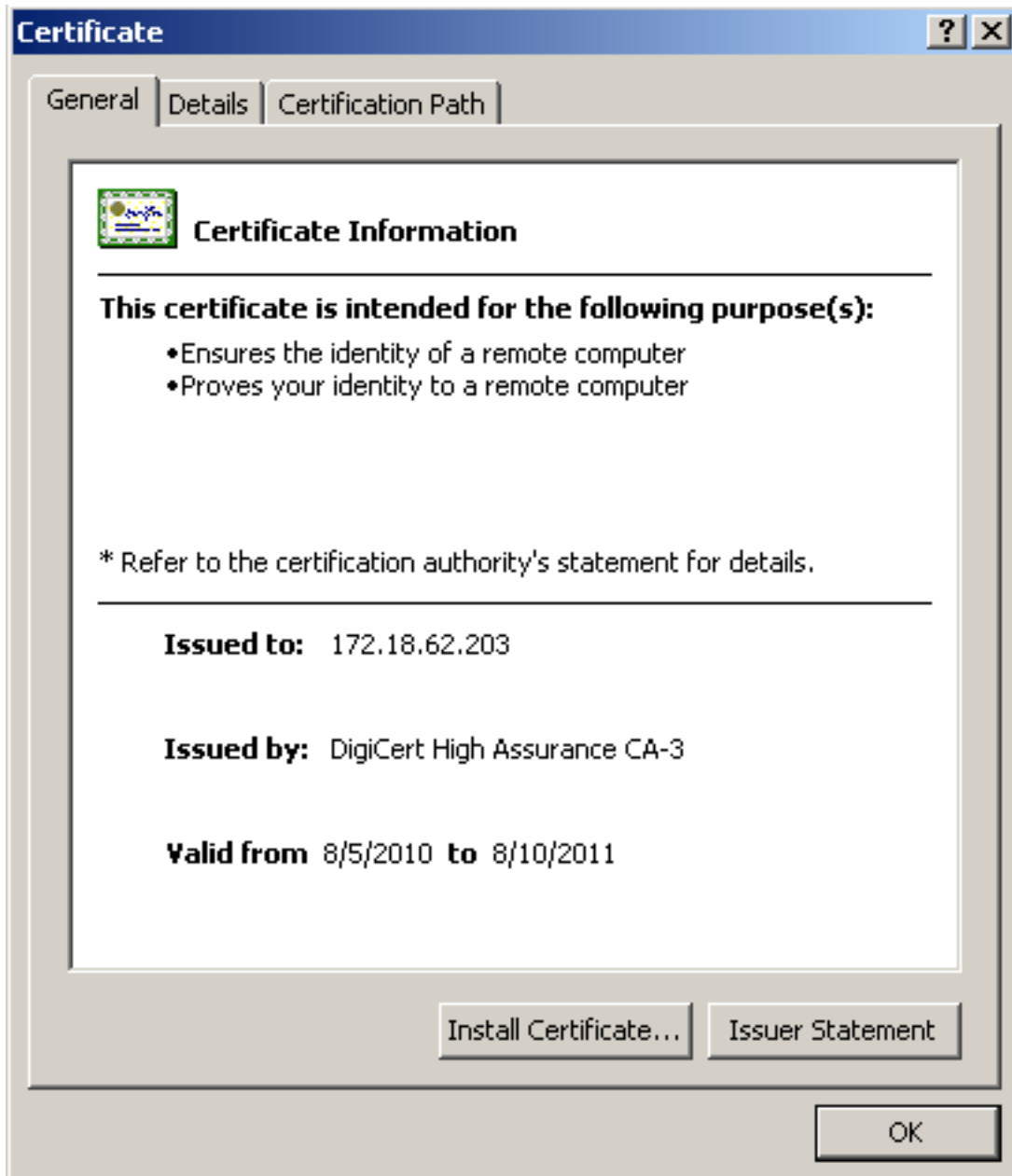
When you get the certificate from DigiCert, it will be in text format looking something like this:

-----BEGIN CERTIFICATE-----

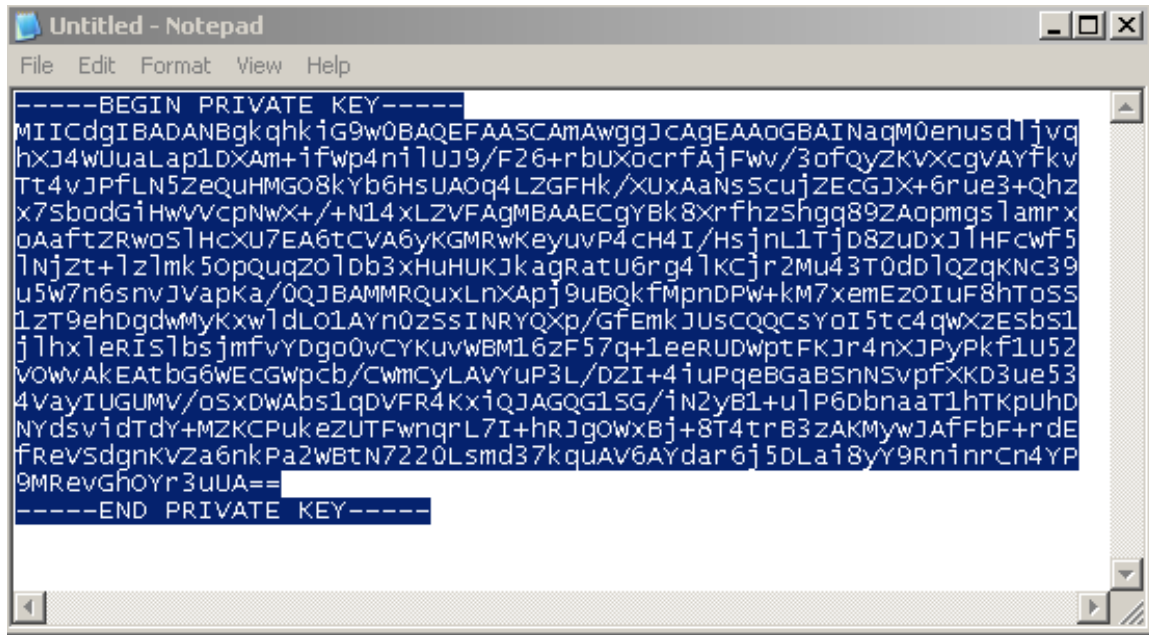
```
MIIHNjCCBR6gAwIBAgIQAVyv57SaTECqWRaAaRb/LITANBgkqhkiG9w0BAQUFADBm
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSUwIwYDVQQDExxEaWdpQ2VydCBlaWdoIEFzc3VyYW5j
ZSBDQS0zMB4XDTEwMDAwMfoXDTEwMDAwMDIxNTk1OVowdTElMAkGA1UEBhMkGA1UE
BhMCMVVMxETAPBgNVBAGTCCE5ldyBZb3JrMRAwDgYDVQQHEwdCdWZmYWxvMRkwFwYD
VQKExBNZWRhaWxsZSBDdb2xsZWdlMQ4wDAYDVQQLEwVjaXNjbCEWMBQGA1UEAxMN
MTcyLjE4LjYyLjIwMzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCYEAjbgZVBWz
jOVcea378eYzr6W18qlKHKPl2MoRjFvklN/uRLxdTuLXk8gMwDdxEQJ6j45bo1K
2kBuQda0nvIj/PubAlu2qGBLmuszryero8fkwdw0zzrMt9nxqXOEdeh5kTl62Rsc+
QDIW7AIVPledRYrmoL8XS2nb6CPUPAy4kj8CAwEAQA1MwggNPMB8GA1UdIwQY
MBaAFFDqc4nbKfsQj57IASDU3nmZSIP3MB0GA1UdDgQWBbT5X00WNMvZyWxp4YAL
HNd1kPjRWzAeBgNVHREEFzAVgg0xNzluMTguNjluMjAzhwSsEj7LMH8GCCsGAQUF
BwRBBHMwctAKBggrBgEFBQcwAYYYaHR0cDovL29jc3AuZGlnaWNlcnQuY29tMEK
CCsGAQUFBzAChj1odHRwOi8vd3d3LmRlZ2ljZXJ0LmNvbS9DQUUNlcnRzL0RpZ2ID
ZXJ0SGlnaEFzc3VyYW5jZUNBLTMuY3J0MA4GA1UdDwEB/wQEAwIFoDAMBGNVHRMB
Af3EAjAAMGUGA1UdHwReMFwwLKAqoCiGJmh0dHA6Ly9jcmwzLmRlZ2ljZXJ0LmNv
bS9jYTMtMjA3Y3J0MA4GA1UdIASCAB0wggG5MIIBTQYLIZIAYb9bAEDAAEw
ggGkMD0GCCsGAQUFBwIBFi5odHRwOi8vd3d3LmRlZ2ljZXJ0LmNvbS9zc2wtY3Bz
LXJlcG9zaXRvcnuaHRtMIIIBZAYIKwYBBQUHAgIwggFWhoIBUgBBAG4AeQAgAHUA
cwBlACAAbwBmACAAdABoAGkAcwAgAEMAZQByAHQAaQBmAGkAYwBhAHQAZQAgAGMA
bwBuAHMAdABpAHQAdQB0AGUAcwAgAGEAYwBjAGUAcAB0AGEAbgBjAGUAIAbvAGYA
IAB0AGgAZQAgAEQAaQBnAGkAQwBlAHIAAdAAgAEMAUAaAvAEMAUAATACAAYQBuAGQA
IAB0AGgAZQAgAFIAZQBsaHkAaQBuAGcAIAABQAGEAcgB0AHkAIAABBAGcAcgBlAGUA
bQBlAG4AdAAgAHcAaABpAGMAaAAAgAGwAaQBtAGkAdAAgAGwAaQBhAGIAaQBsAGkA
dAB5ACAAYQBuAGQAIABhAHIAZQAgAGkAbgBjAG8AcgBwAG8AcgBhAHQAZQBkACAA
aABIAHIAZQBpAG4AIABiAHkAIAByAGUAZgBlAHIAZQBuAGMAZQAuMB0GA1UdJQW
MBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQUFAAOCAQEAm4Dxdvzp
Ze+Ogn+RtPEUEhWxj7NdRr9esmOBbUYjd67BRcfvaSIWPbzB5LOzXvbnwVJO06Hk
aetxy5zE/S0A3Rm58Fq+a9qhZcwOGF+IpXRwe4EftSryX4l5XN7csIcBBvlRPVya
J7E689i3oVy+qgdr5S8grZe41F1bkawtulSL0Z6e/6zAYr8S7zLQRtk1Unjl1ntV
Ld+bpEkf/EZg2V0u48drqGS5GhPpVie+ReaPhlNjt7jlHHeAC78QTrFy63bi6ld6
kYhy1dFj6h1ADP7nt8kWjl7yUDdm3vyPk53WIKlGrCi5jqGhplqPw4+8144rfde
PRe7zUo0zxlaTw==
```

-----END CERTIFICATE-----

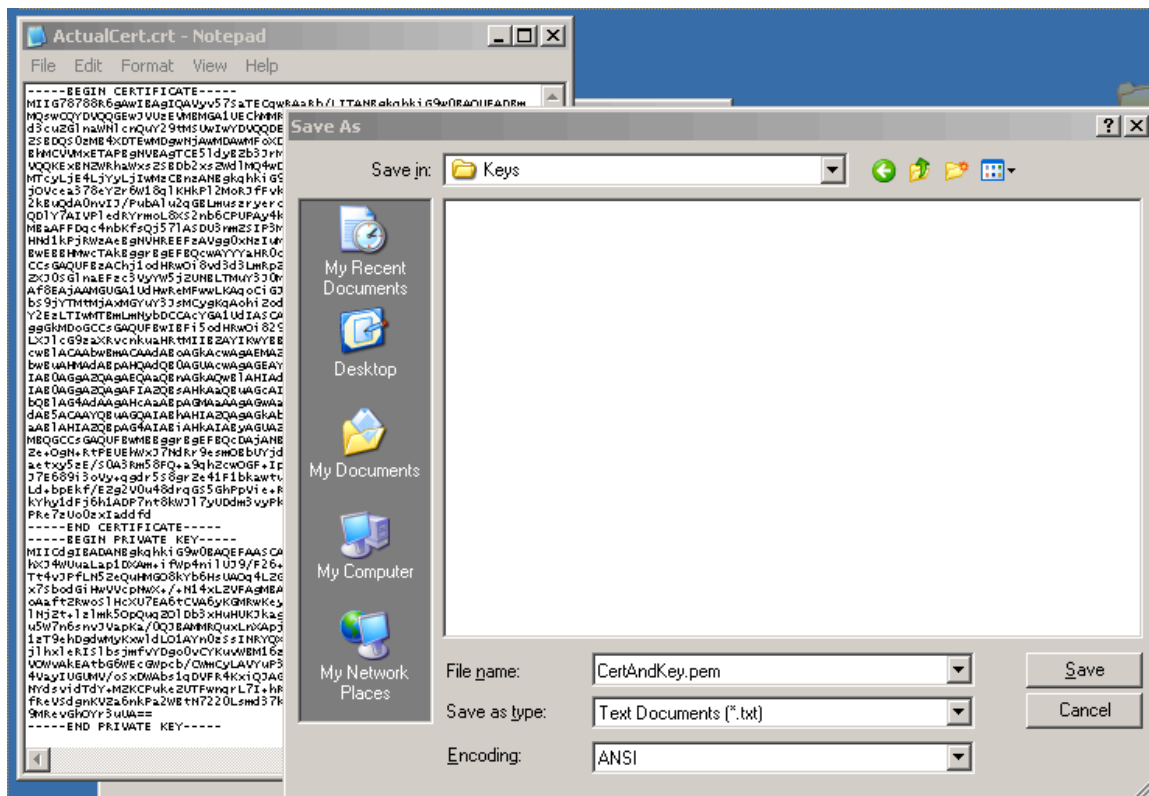
Opening the certificate in Windows, it would look something like this. You can see it's signed by DigiCert:



Now open the private key that you had saved in another notepad and copy the contents of the private key from that:



Paste the private key in the certificate Notepad instance and save it:

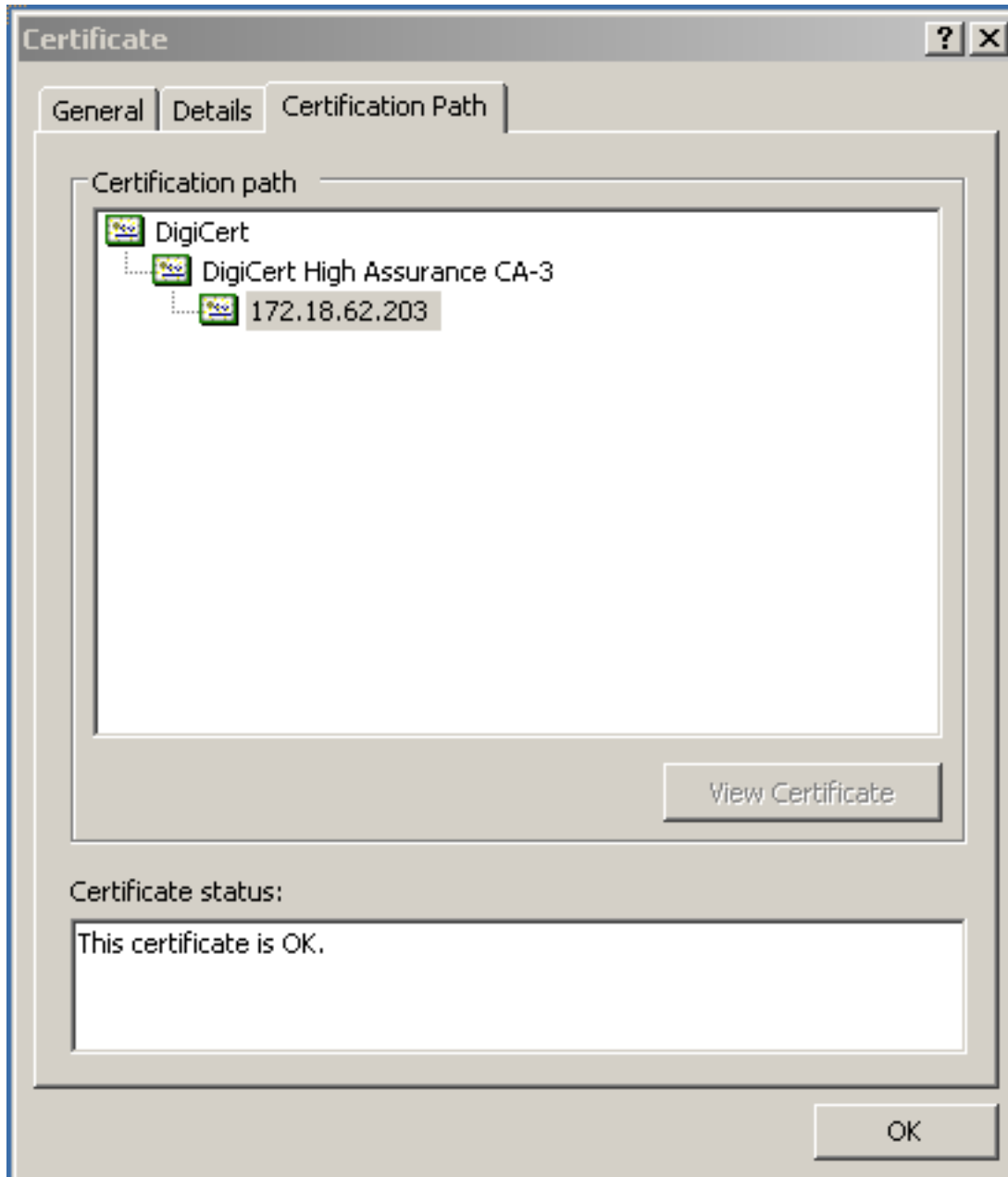


Now at this point in time we have the signed certificate from DigiCert and we're ready to import it in to the CAS.

This will work, or not work, based on whether we have the Root and Intermediate certificates in our CAS's trusted root store. If you built the CAS on 4.7 or above, chances are that it does not have the Root/Intermediate certificates that we need to install the DigiCert certificate successfully. If you upgraded from a previous version to 4.7 and above, chances are that your certificate store already contains the DigiCert Root and intermediate certificates.

Assuming that you don't have the certificates in your root store, here's how you get them and install.

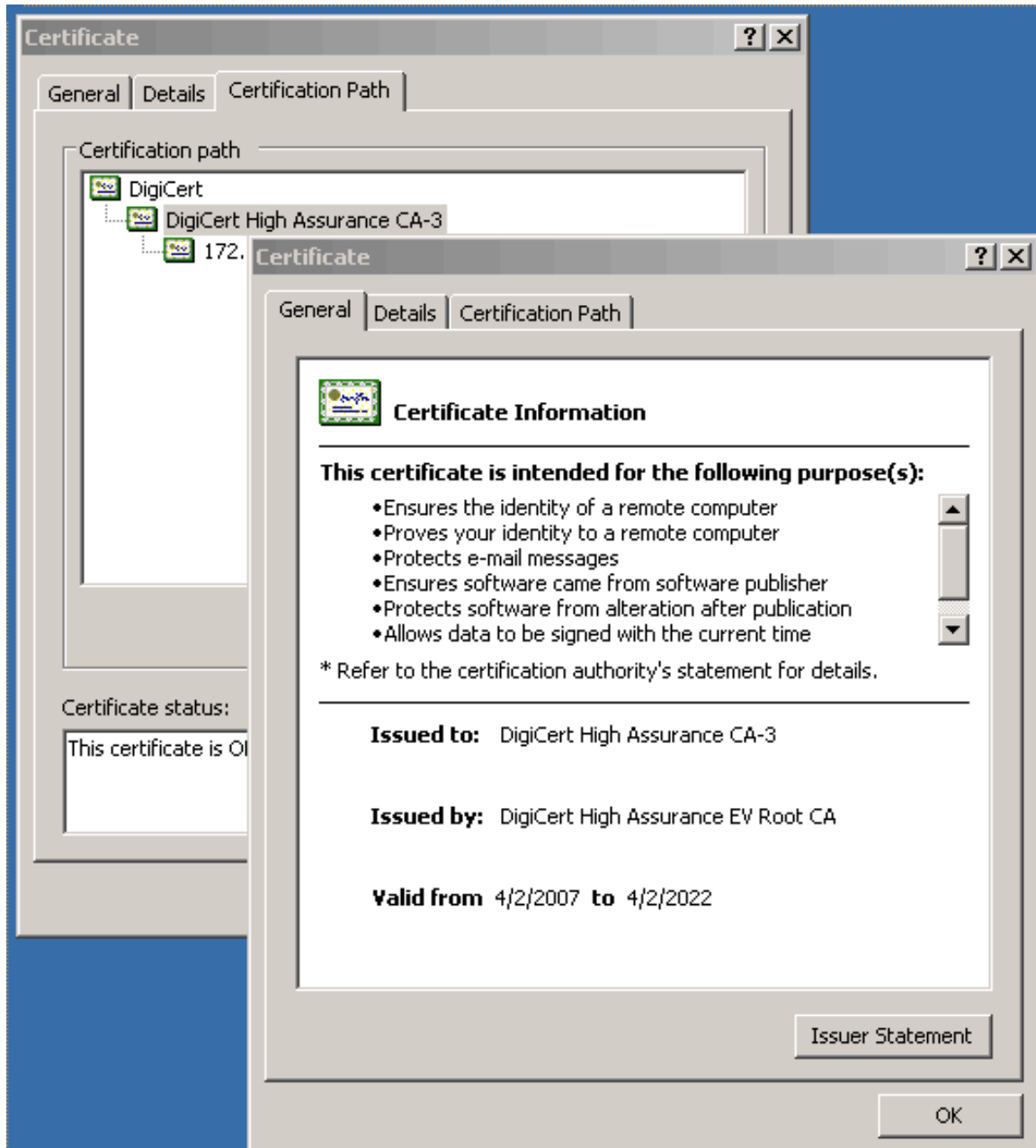
First thing is to see what Root and Intermediate certificates we require, in order to install the CAS certificate. Open the certificate that DigiCert sent you, and click on the Certification Path



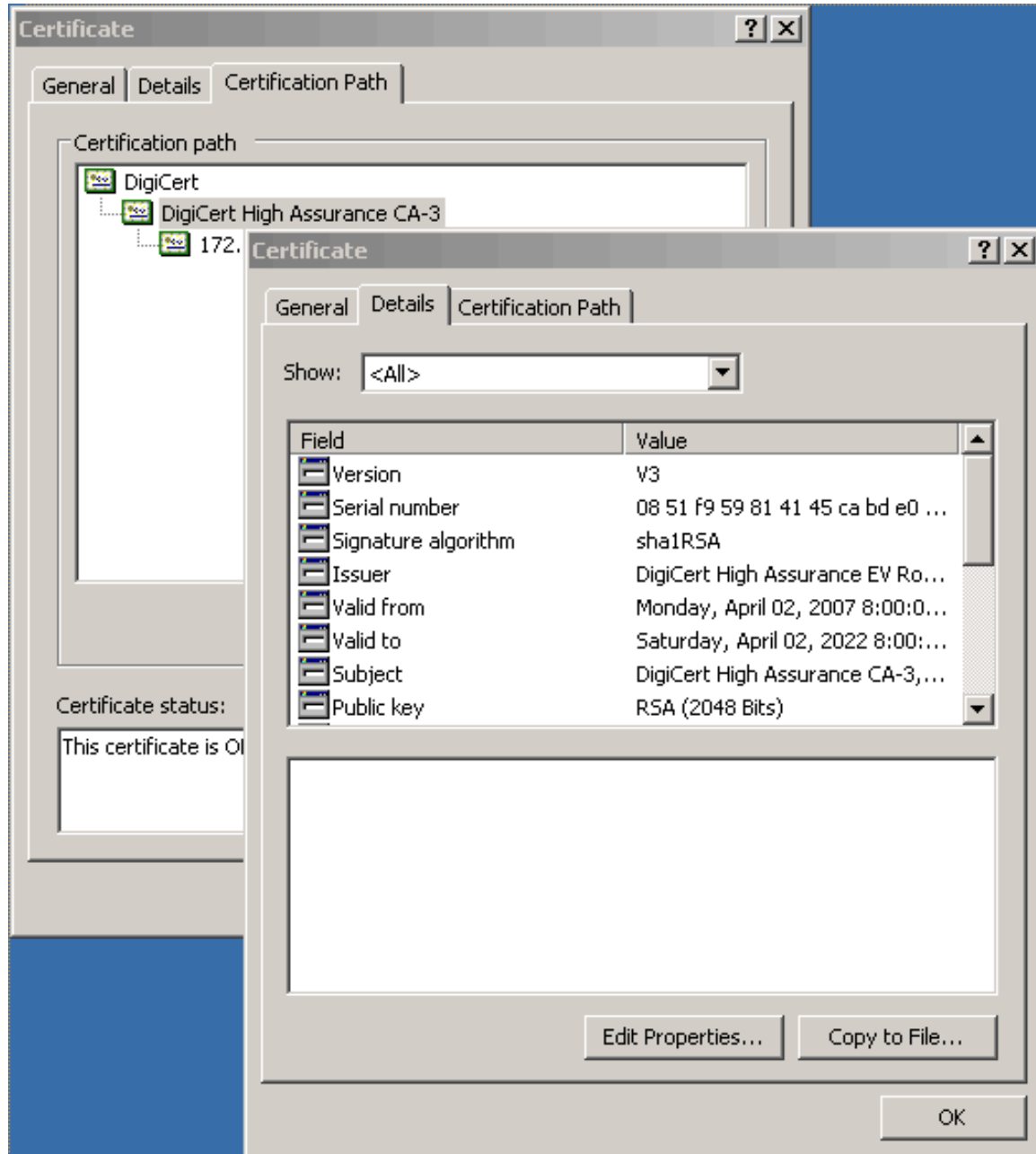
This means we need these two certificates, the intermediate "DigiCert High Assurance CA-3" and the root "DigiCert" installed in the CAS Trusted Root store before we can import the identity certificate in the CAS itself.

There are two ways we can get these root/intermediate certificates. We can either visit the DigiCert website and download them from there, or if we have the certificates showing up (as shown above), we can just export them from there. Here's how:

Double Click on the certificate shown as "DigiCert High Assurance CA-3"



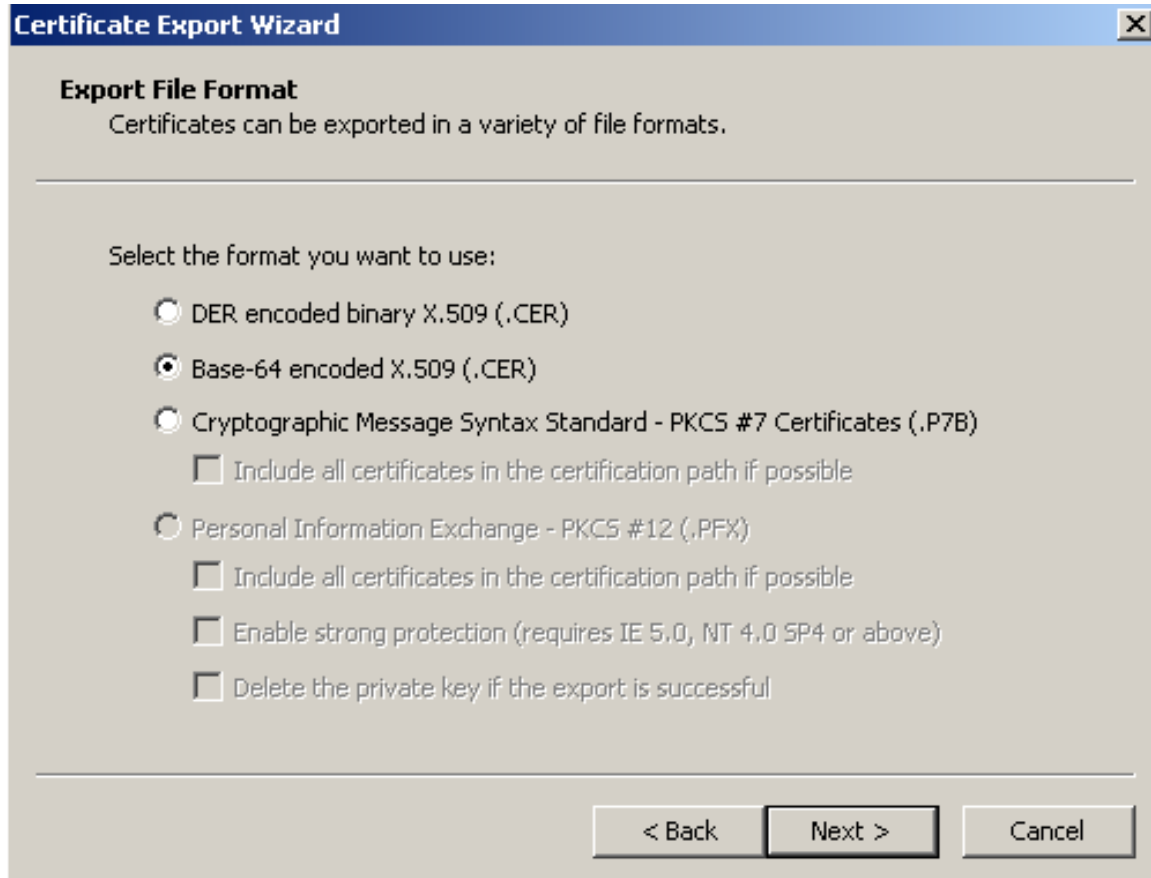
Click on Details and then Copy to File:



This launches the Wizard:



Click Next and choose Base 64:



Certificate Export Wizard [X]

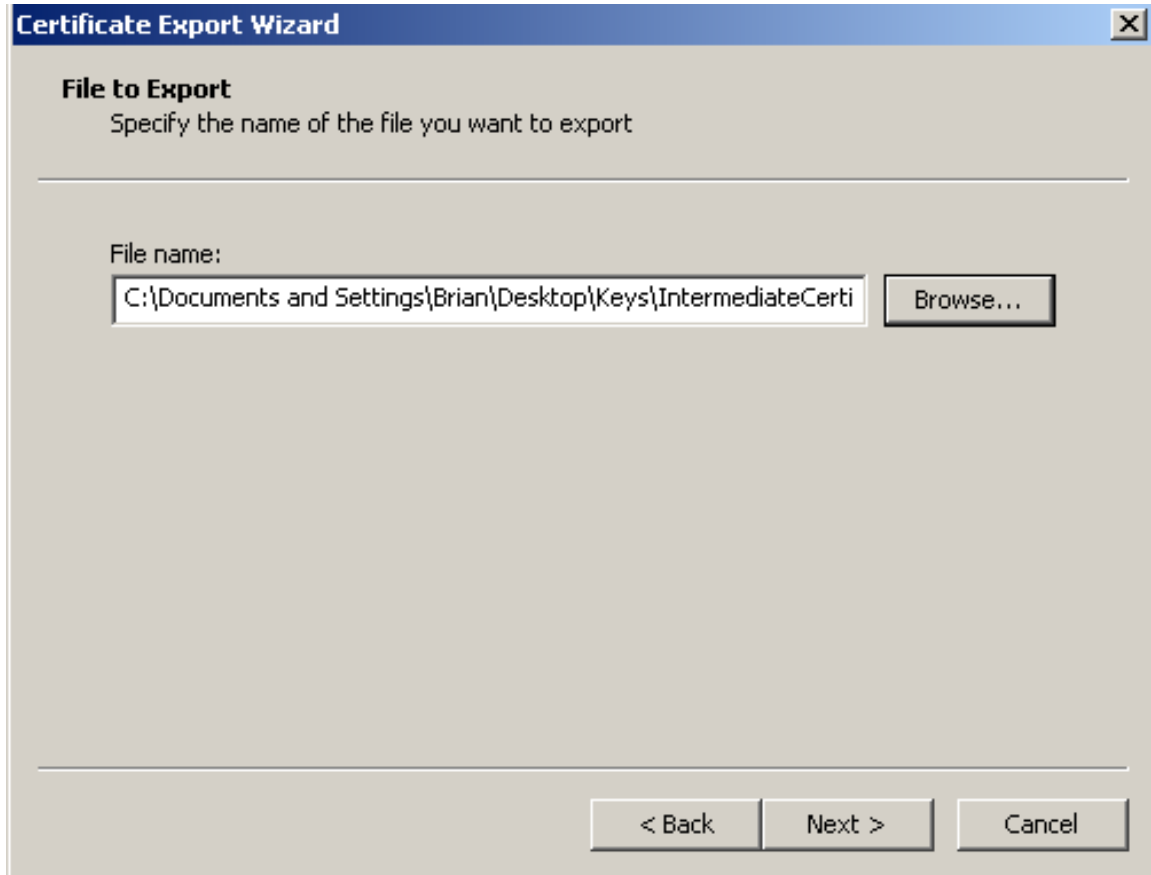
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 - Include all certificates in the certification path if possible
- Personal Information Exchange - PKCS #12 (.PFX)
 - Include all certificates in the certification path if possible
 - Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
 - Delete the private key if the export is successful

< Back Next > Cancel

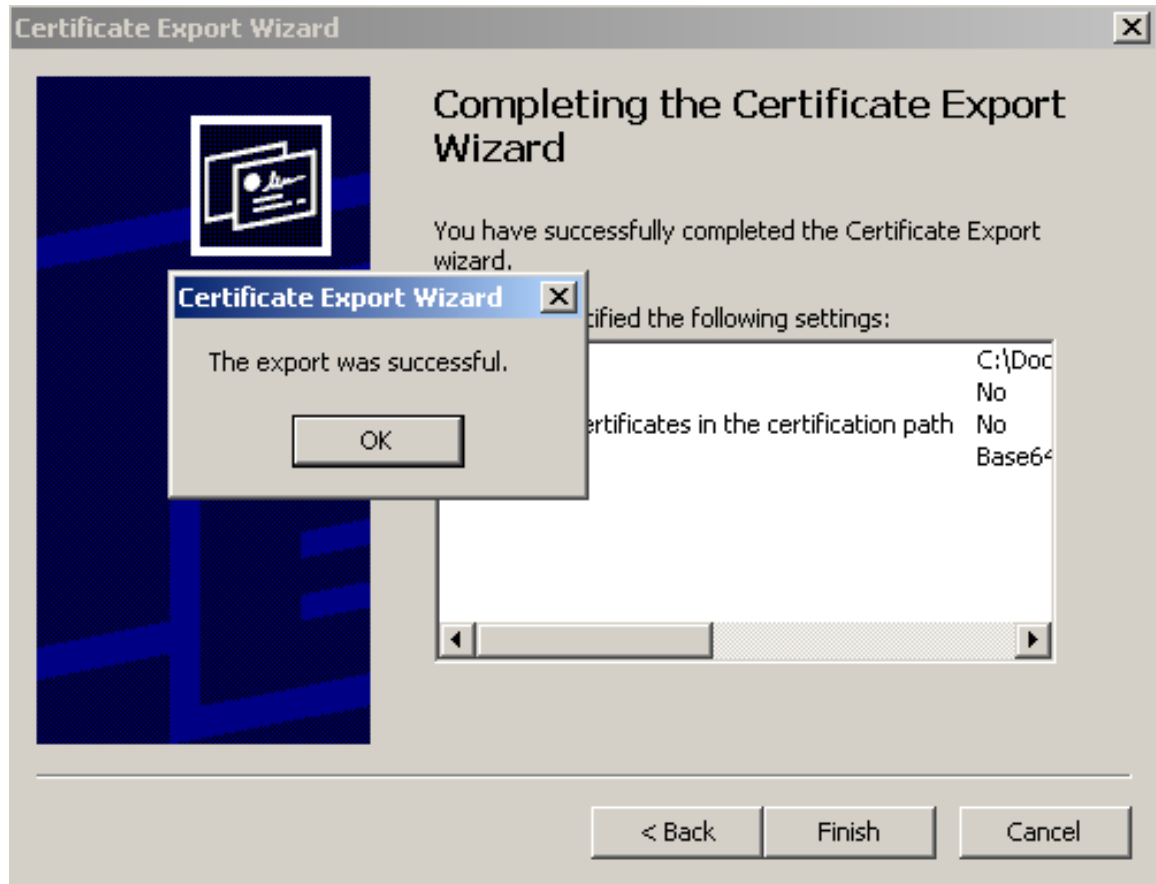
Specify the path and Next:



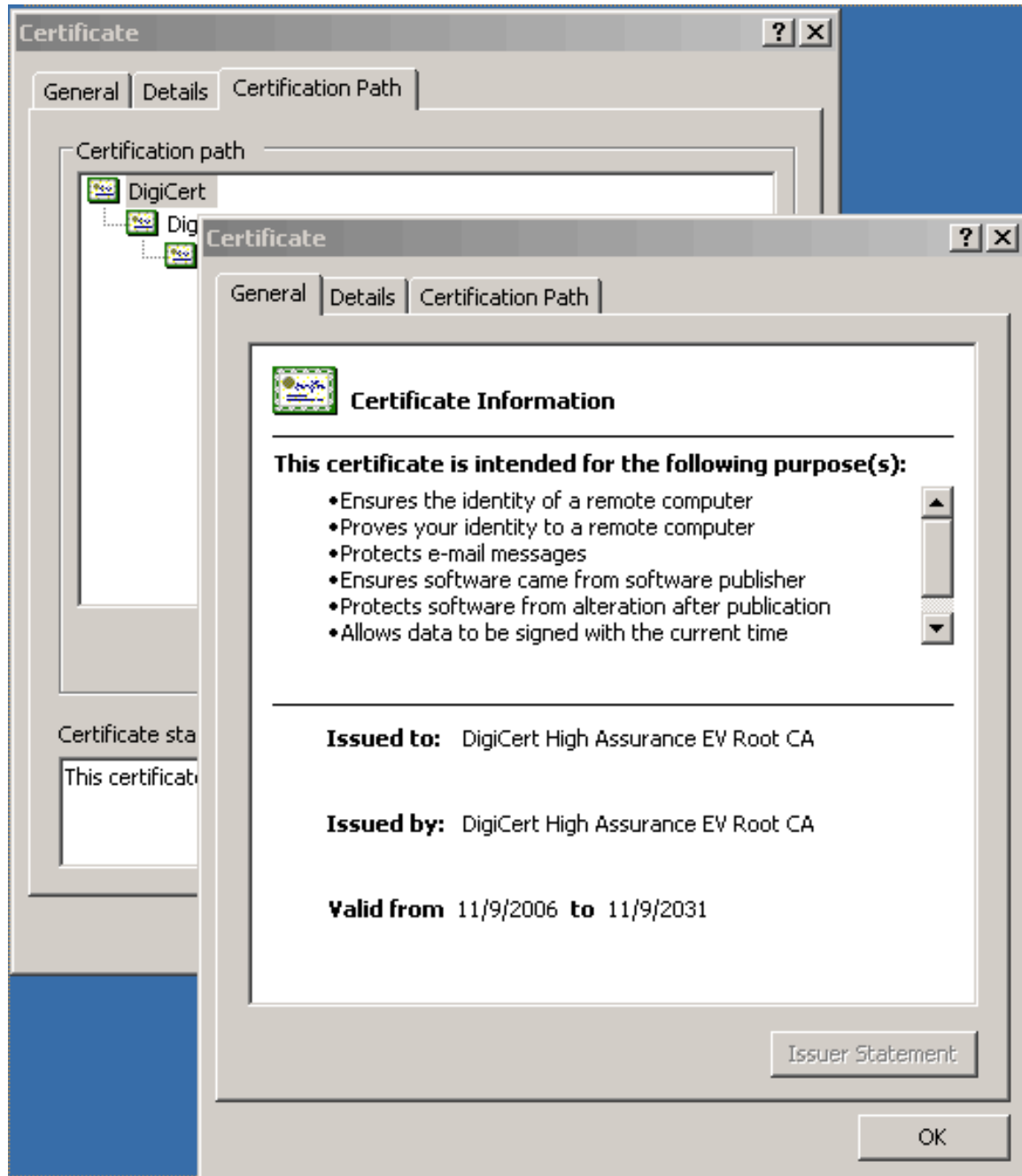
The image shows a Windows-style dialog box titled "Certificate Export Wizard". The window has a blue title bar with a close button (X) in the top right corner. The main area is light gray and contains the following elements:

- File to Export**: A section header in bold black text.
- Specify the name of the file you want to export: A line of instructional text below the header.
- File name: A label positioned above a text input field.
- Text input field: Contains the path "C:\Documents and Settings\Brian\Desktop\Keys\IntermediateCerti".
- Browse... button: A button located to the right of the text input field.
- Navigation buttons: At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

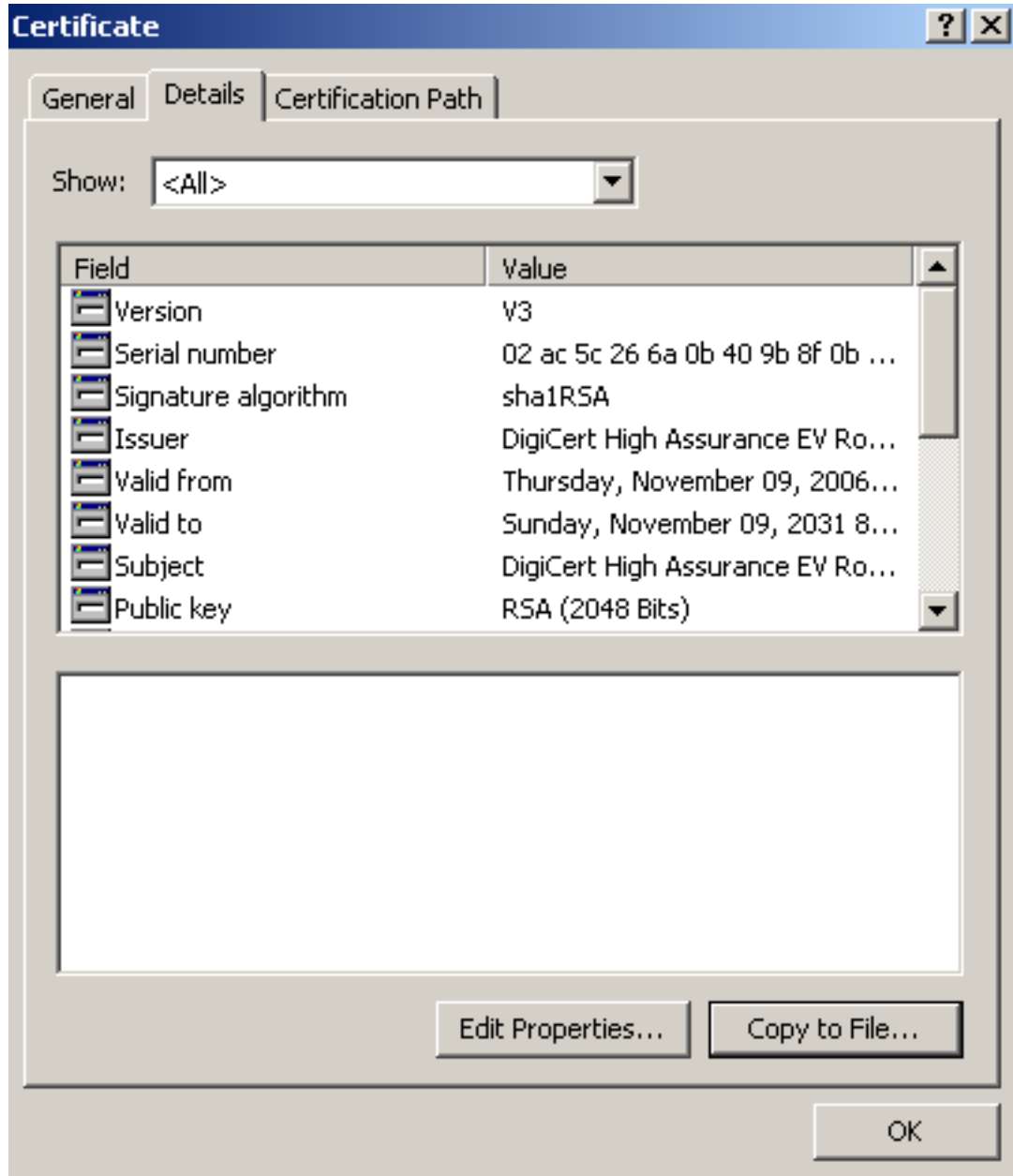
Click on Next and then Finish. The export is successful message shows up and you will have the IntermediateCertificate.crt file in the directory were you saved it:

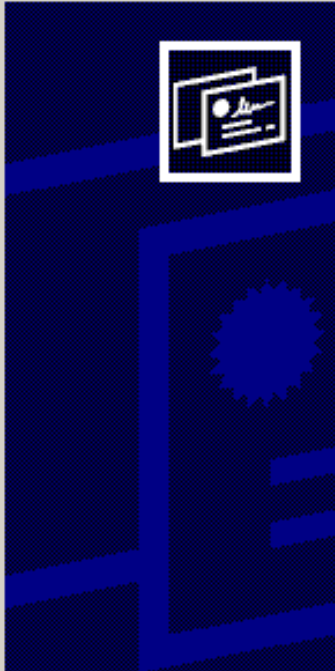


Now we do the same thing for the root certificate. Double Click on the DigiCert certificate as shown below.



Click on Details, and Copy to File:





Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

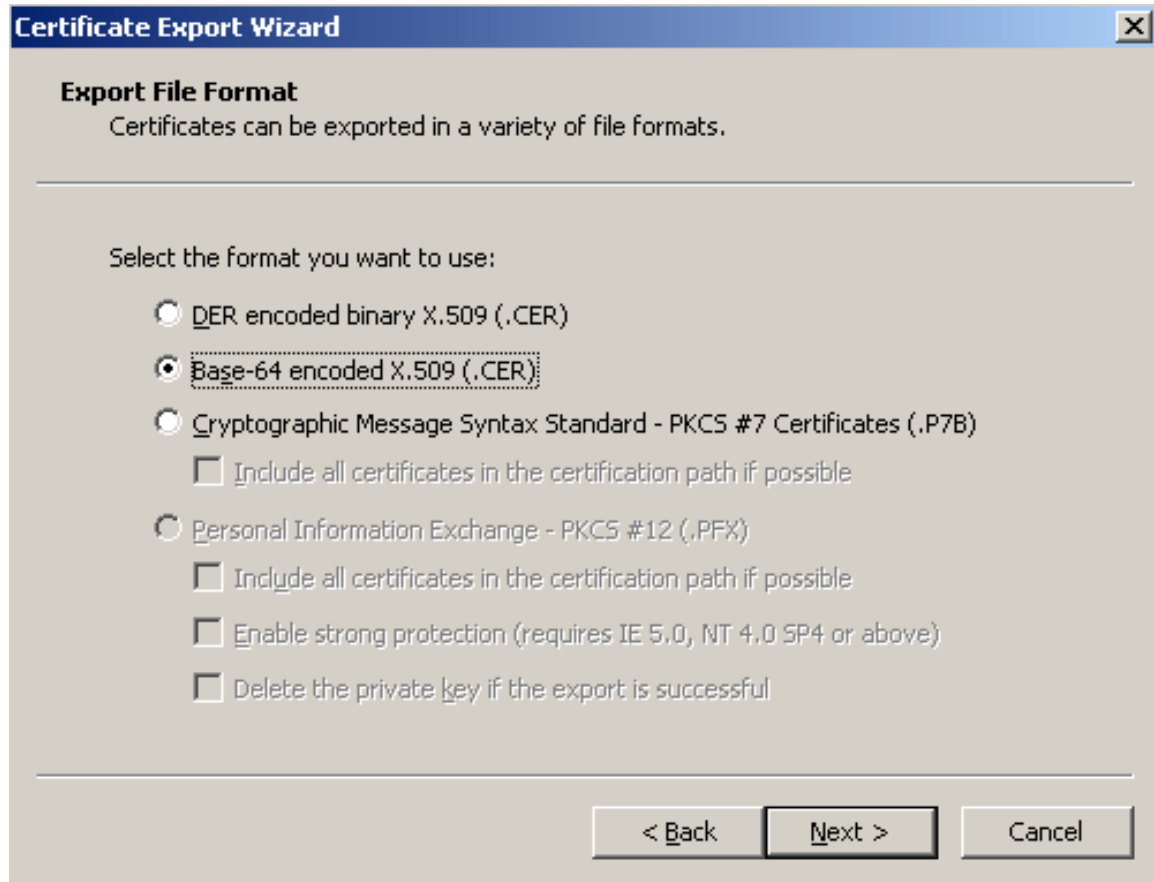
To continue, click Next.

< Back

Next >

Cancel

Choose Base-64 Encoded:



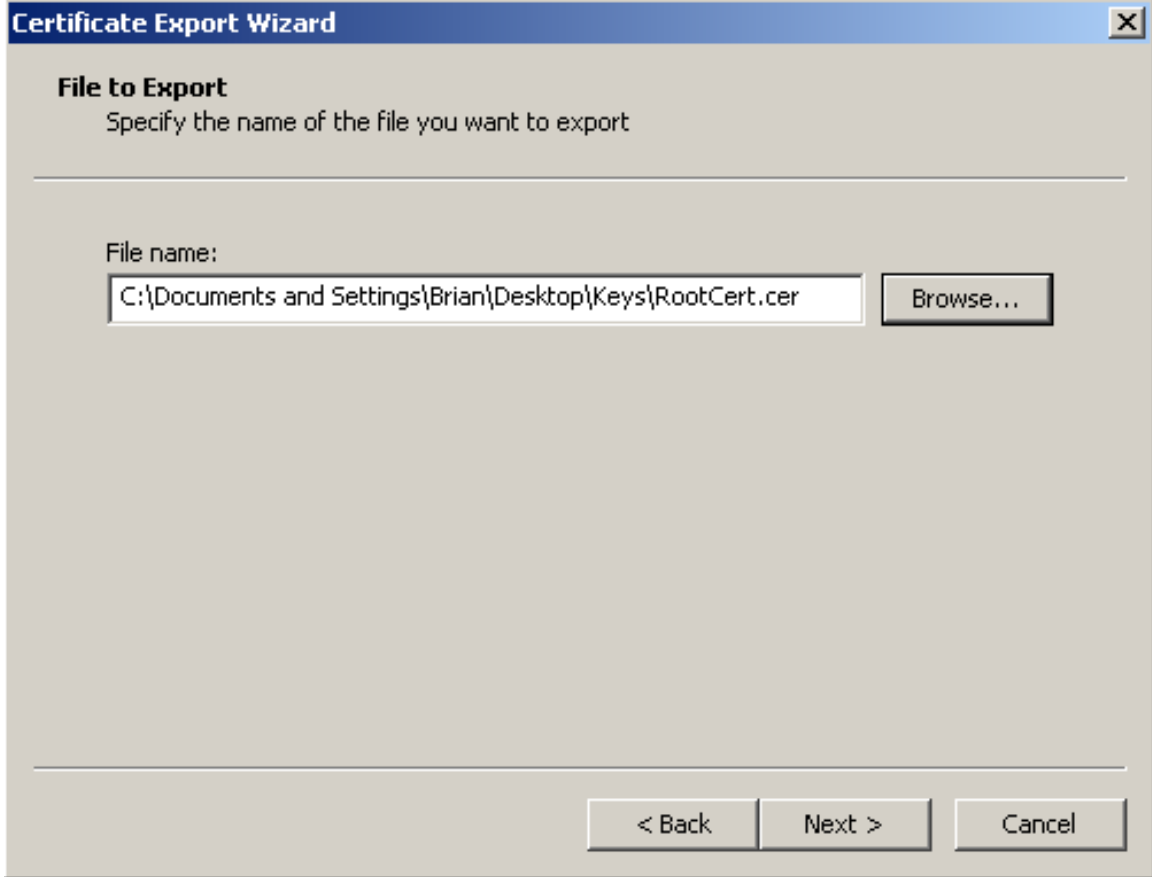
Certificate Export Wizard [X]

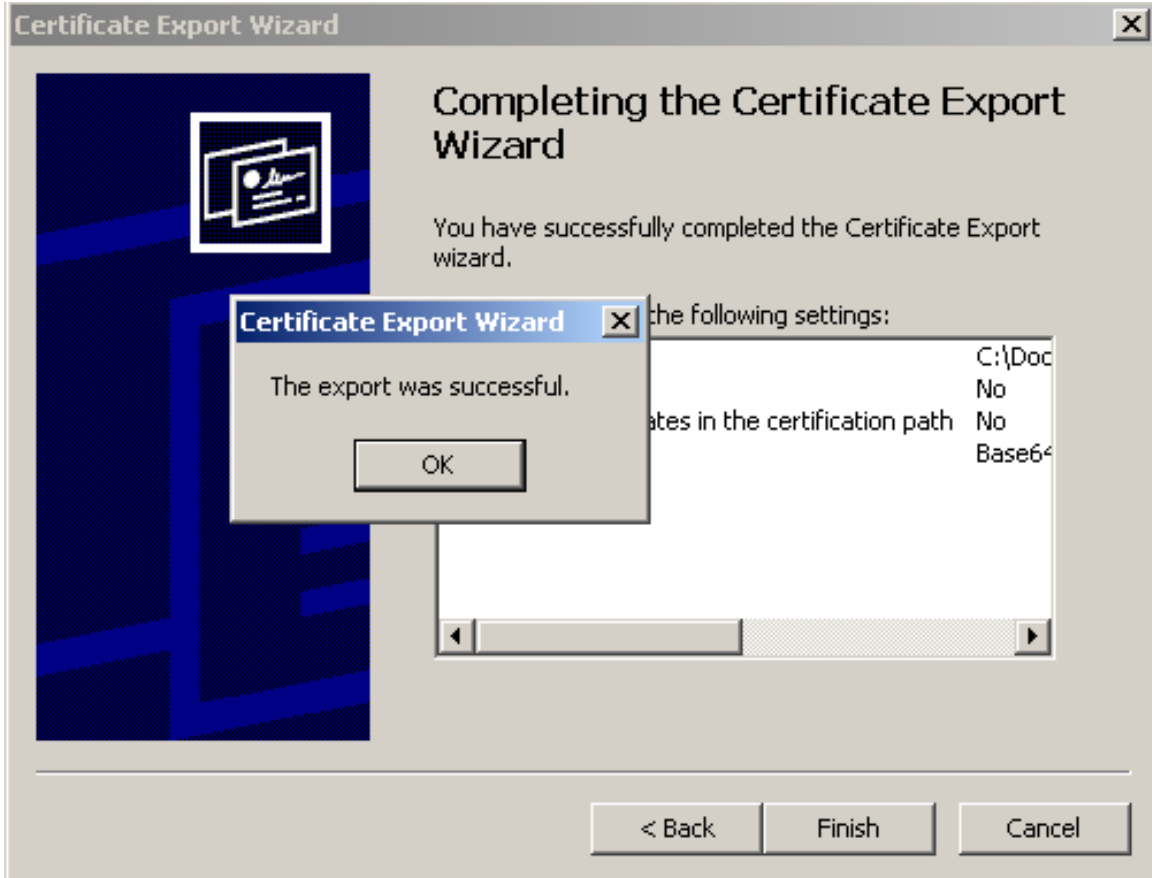
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

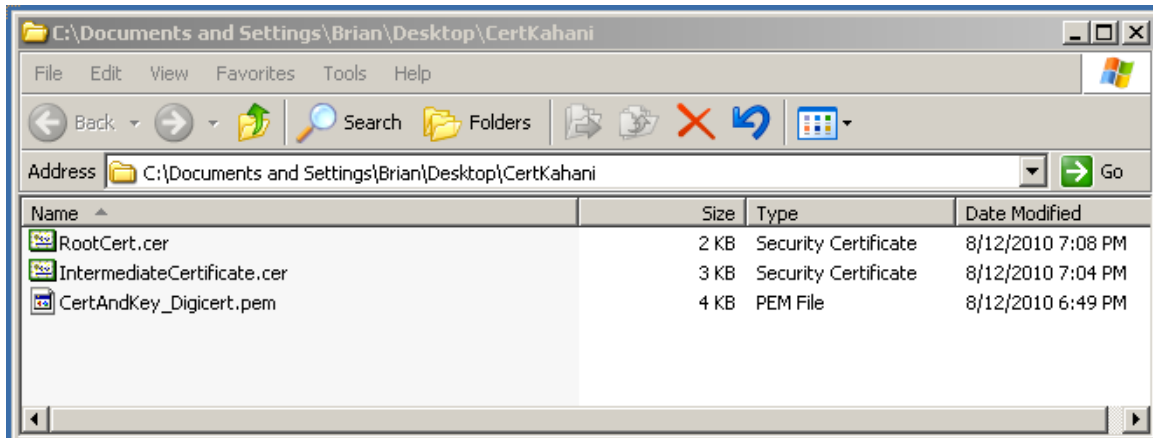
- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 - Include all certificates in the certification path if possible
- Personal Information Exchange - PKCS #12 (.PFX)
 - Include all certificates in the certification path if possible
 - Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
 - Delete the private key if the export is successful

< Back Next > Cancel



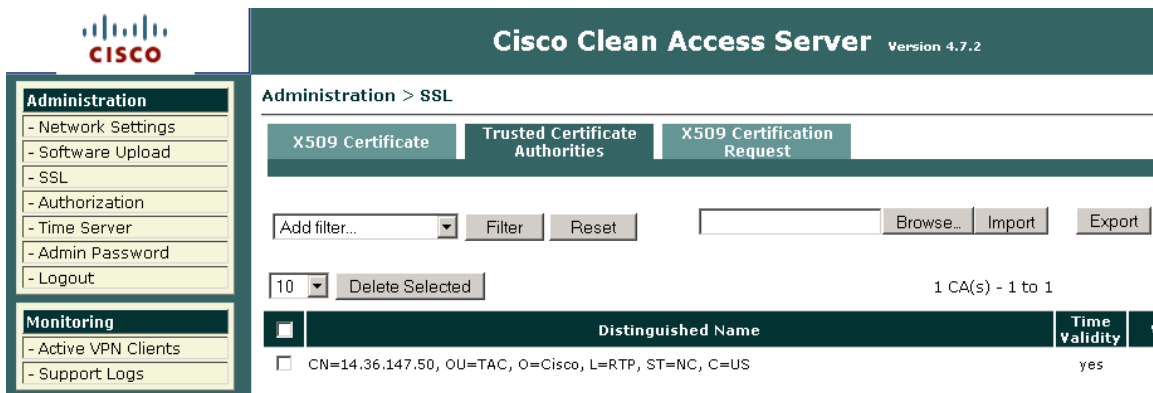


Now we have the RootCert.crt, IntermediateCert.crt and the Certificate and Private key in the same file on our file system:



To install the cert now, we first need to import the Root and Intermediate certificate in the Trusted Certificate Authorities tab on the CAS.

Open CAS Admin page, and browse to SSL -> Trusted Certificate Authorities tab:



Click on Browse and choose the RootCert.crt file first:



Click on Import and the root cert should be added to the store:

Administration > SSL

X509 Certificate Trusted Certificate Authorities X509 Certification Request

Add filter... Filter Reset Browse... Import Export

10 Delete Selected 2 CA(s) - 1 to 2

<input type="checkbox"/>	Distinguished Name	Time Validity	View
<input type="checkbox"/>	CN=14.36.147.50, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US	yes	
<input type="checkbox"/>	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	yes	

Do the same with the intermediate cert:

Administration > SSL

X509 Certificate Trusted Certificate Authorities X509 Certification Request

Add filter... Filter Reset Browse... Import Export

intermediateCertificate.cer Browse... Import Export

Click on Import and the Intermediate should show up in the store too:

Administration > SSL

X509 Certificate Trusted Certificate Authorities X509 Certification Request

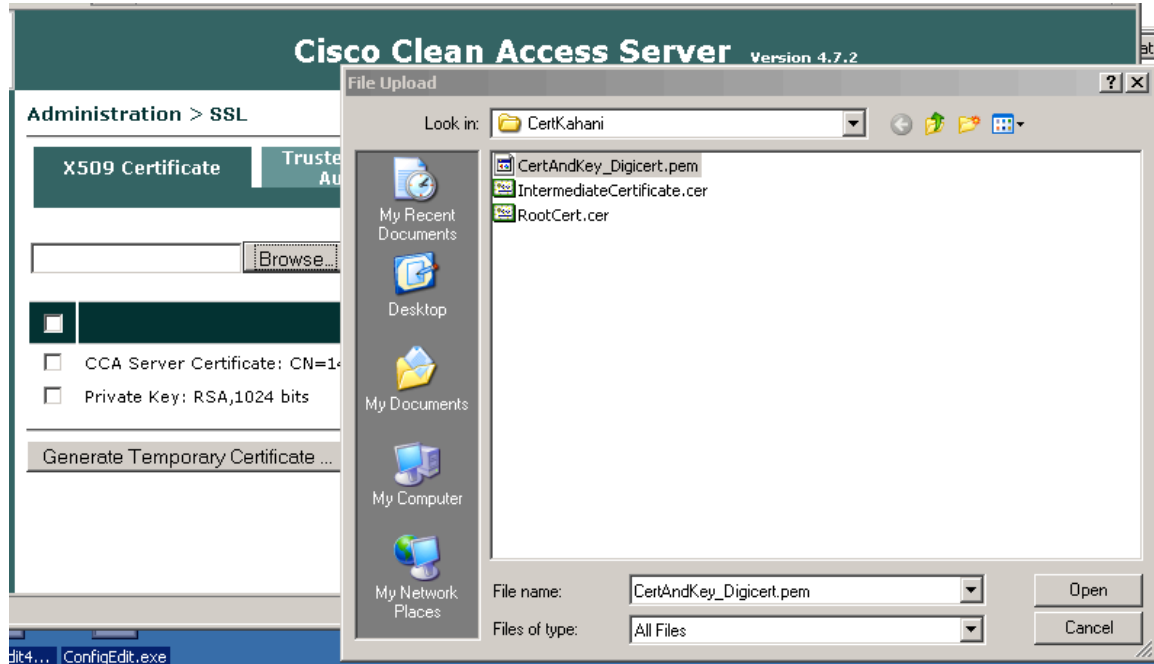
Add filter... Filter Reset Browse... Import Export

10 Delete Selected 3 CA(s) - 1 to 3

<input type="checkbox"/>	Distinguished Name	Time Validity	View
<input type="checkbox"/>	CN=14.36.147.50, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US	yes	
<input type="checkbox"/>	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	yes	
<input type="checkbox"/>	CN=DigiCert High Assurance CA-3, OU=www.digicert.com, O=DigiCert Inc, C=US	yes	

Now with the root and intermediate certificates in the store, we should be able to import the certificate in our CAS successfully. Let's try:

Open the admin page for CAS and click on SSL. Click on Browse and select the CertAndKey_DigiCert.pem file (If you named it something else, click on that filename)



Click on import and the certificate is installed. You should reboot your CAS for the cert to be used with all the services on the CAS.

The last step to make sure that the CAM/CAS communication is intact after the installation of the new cert is to make sure that the root and intermediate certificates are also in place in the CAM Trusted Certificate Authorities store.

To check on that, open the CAM admin page, click on CCA Manager -> SSL -> Trusted Certificate Authorities. If the DigiCert root and intermediate certs are not there, import them here:

Administration > Clean Access Manager

Network | Failover | System Time | SSL | Software Upload | Licensing | Policy S

X509 Certificate · Trusted Certificate Authorities · X509 Certification Request

Add filter... Filter Reset CertKahani\RootCert.cer Browse... Import Export

10 Delete Selected 2 CA(s) - 1 to 2

<input type="checkbox"/>	Distinguished Name
<input type="checkbox"/>	CN=14.36.147.45, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US
<input type="checkbox"/>	CN=14.36.147.65, OU=TAC, O=TAC, L=RTP, ST=NC, C=US

Click on import and root shows up in the store:

Administration > Clean Access Manager

Network | Failover | System Time | SSL | Software Upload

X509 Certificate · Trusted Certificate Authorities · X509 Certification Request

Add filter... Filter Reset

10 Delete Selected

<input type="checkbox"/>	Distinguished Name
<input type="checkbox"/>	CN=14.36.147.45, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US
<input type="checkbox"/>	CN=14.36.147.65, OU=TAC, O=TAC, L=RTP, ST=NC, C=US
<input type="checkbox"/>	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US

Do the same for the intermediate cert:

The screenshot shows the 'Trusted Certificate Authorities' page. The breadcrumb trail is 'X509 Certificate > Trusted Certificate Authorities > X509 Certification Request'. The 'SSL' tab is active. A search filter 'intermediateCertificate.cer' is entered in the search box. Below the search box, there are buttons for 'Filter', 'Reset', 'Browse...', 'Import', and 'Export'. A dropdown menu shows '10' and a 'Delete Selected' button. The table below shows 3 CA(s) - 1 to 3.

<input type="checkbox"/>	Distinguished Name	Time Validity	View
<input type="checkbox"/>	CN=14.36.147.45, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US	yes	
<input type="checkbox"/>	CN=14.36.147.65, OU=TAC, O=TAC, L=RTP, ST=NC, C=US	yes	
<input type="checkbox"/>	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	yes	

Click on import and the Intermediate cert should show up in the store also:

The screenshot shows the 'Trusted Certificate Authorities' page after importing a new certificate. The breadcrumb trail is 'Administration > Clean Access Manager > Trusted Certificate Authorities > X509 Certification Request'. The 'SSL' tab is active. The search box is empty. Below the search box, there are buttons for 'Filter', 'Reset', 'Browse...', 'Import', and 'Export'. A dropdown menu shows '10' and a 'Delete Selected' button. The table below shows 4 CA(s) - 1 to 4.

<input type="checkbox"/>	Distinguished Name	Time Validity	View
<input type="checkbox"/>	CN=14.36.147.45, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US	yes	
<input type="checkbox"/>	CN=14.36.147.65, OU=TAC, O=TAC, L=RTP, ST=NC, C=US	yes	
<input type="checkbox"/>	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	yes	
<input type="checkbox"/>	CN=DigiCert High Assurance CA-3, OU=www.digicert.com, O=DigiCert Inc, C=US	yes	

Now the CAS should have the DigiCert certificate installed, and the CAM will be able to talk to the CAS also