**QUESTION**

How can I chain a certificate in CRT format?

**ANSWER**

To chain a cert, first verify that the certificate is trusted and signed by a Certificate Authority (CA). If this has not been done, you must generate a self-signed cert within EFT and then send the .csr [certificate signing request] to a CA such as Verisign or Go Daddy.

**MORE INFORMATION**

The certificate chain is essentially a certificate path from signed certificate to intermediate to CA root certificate to indicate that the certificate is trusted.

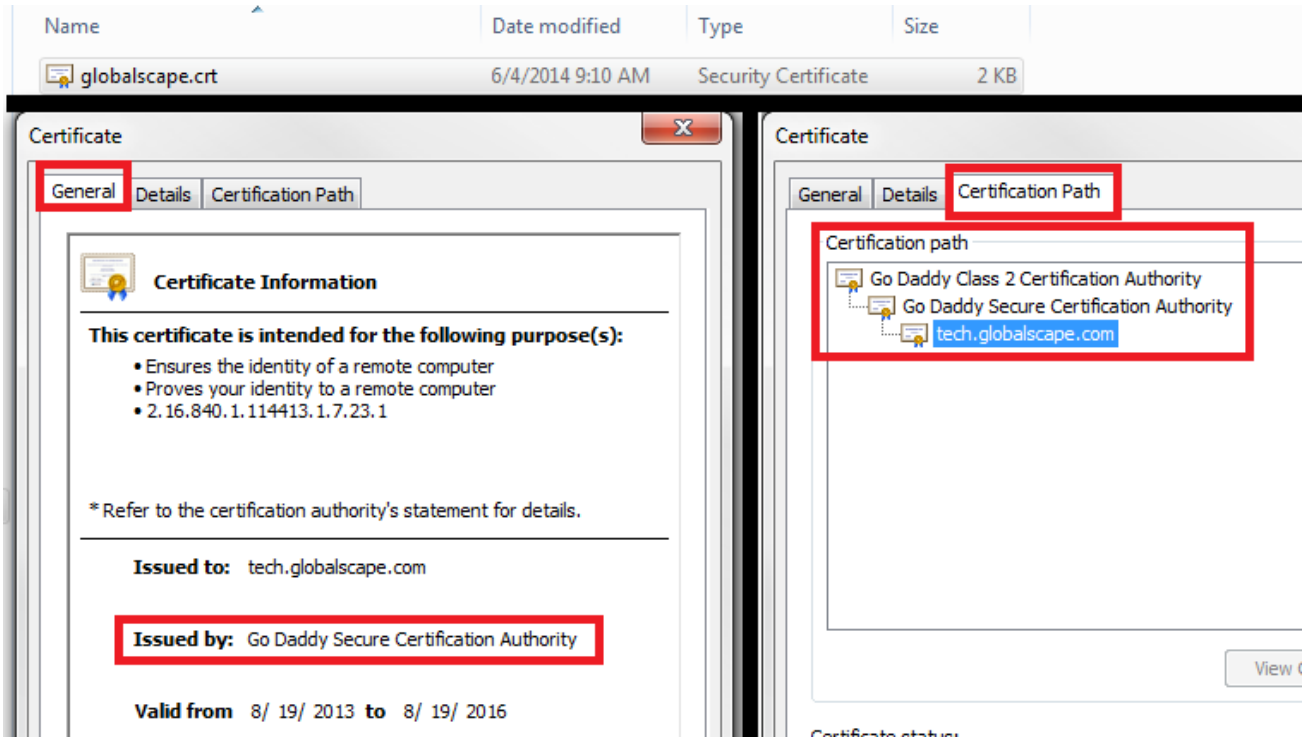
http://msdn.microsoft.com/en-us/library/windows/desktop/aa376515(v=vs.85).aspx
http://en.wikipedia.org/wiki/Certification_path_validation_algorithm

In some environments, Java and other applications may have difficulty in validating the certificate chaining path if only the signed certificate is provided

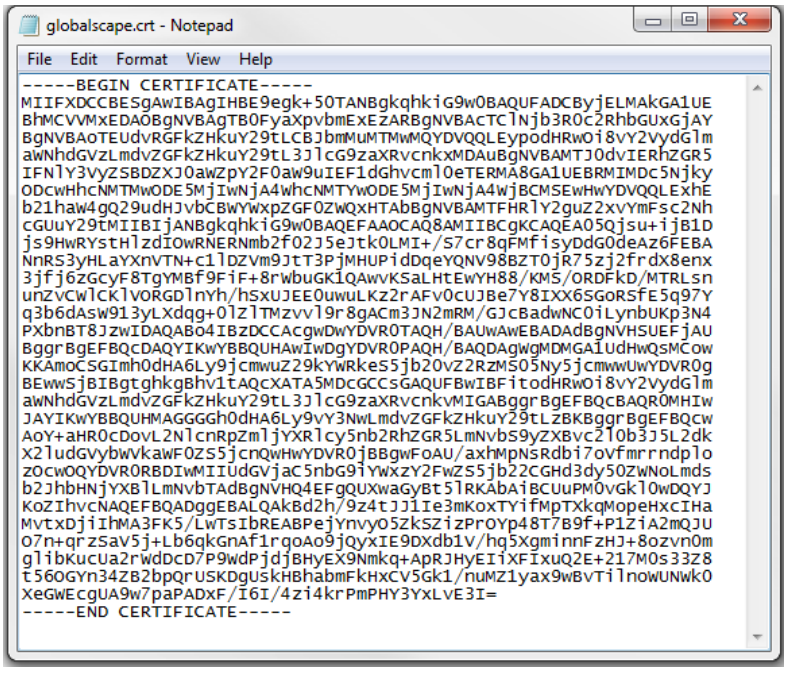
Chaining a certificate makes it easier for Java and other application in some environments to validate the certificate validity path. A chained certificate basically has all of the certs in the certificate path chain in one file.

**To chain a cert,** first verify that the certificate is trusted and signed by a Certificate Authority (CA).
(If this has not been done, you must generate a self-signed certificate within EFT Server and then send the .csr [certificate signing request] to a CA such as Verisign or Go Daddy.)

We can see that the below certificate has been signed by a CA.
This is called the “signed certificate”.

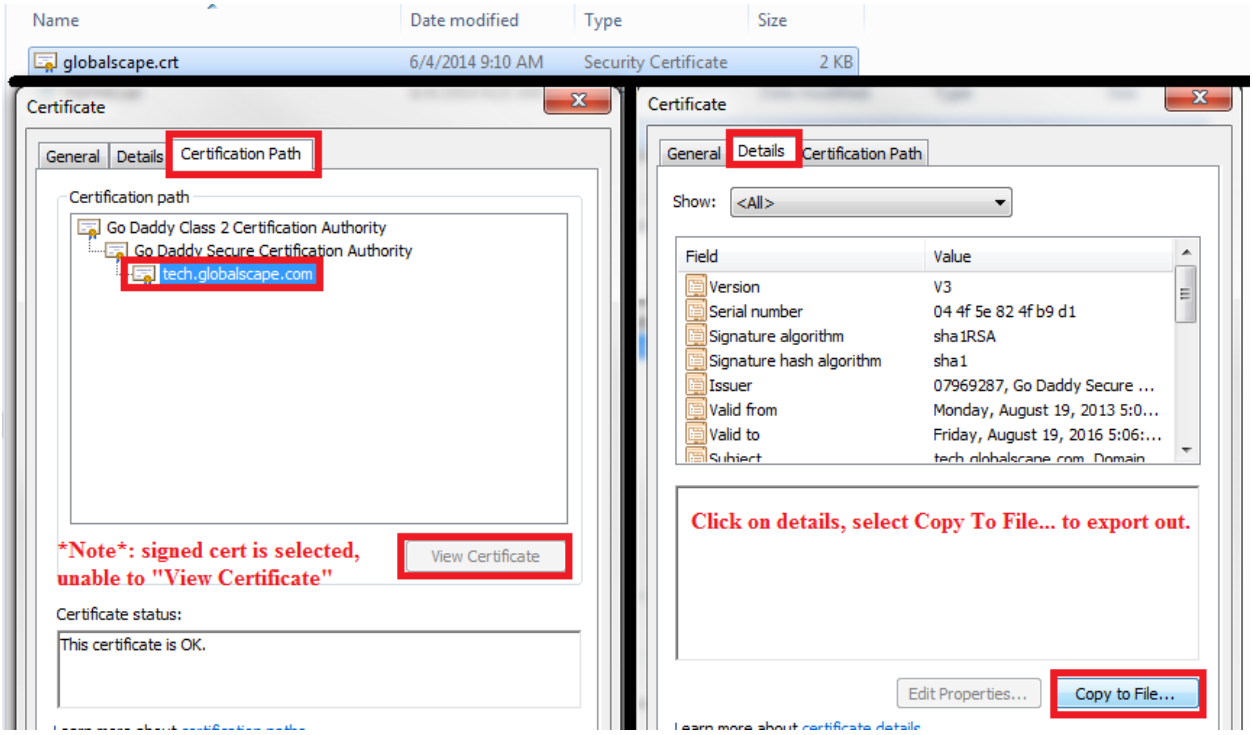



When we open the certificate in notepad, we see that it only has one certificate block.

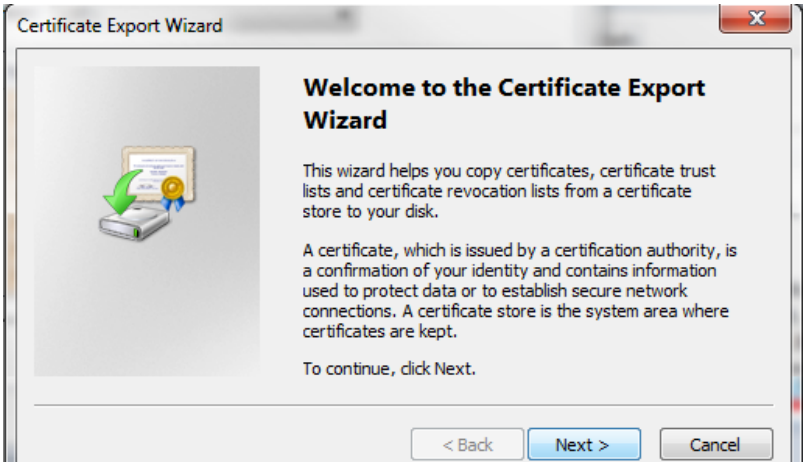


We will have to export out the individual certificates of the chain so that we can merge them into one file.

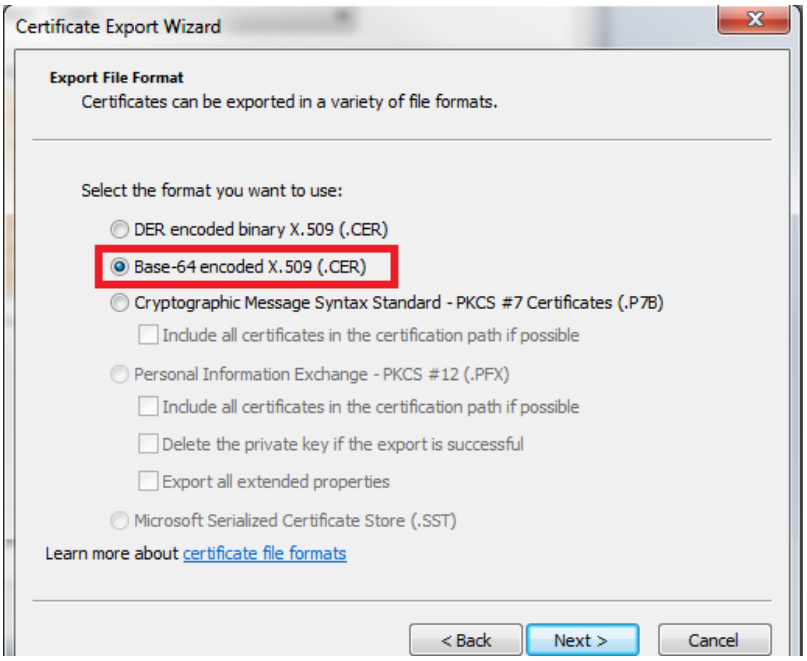
To do this, double click on the **signed cert**. Navigate to the **Details** tab and select **Copy To File…**



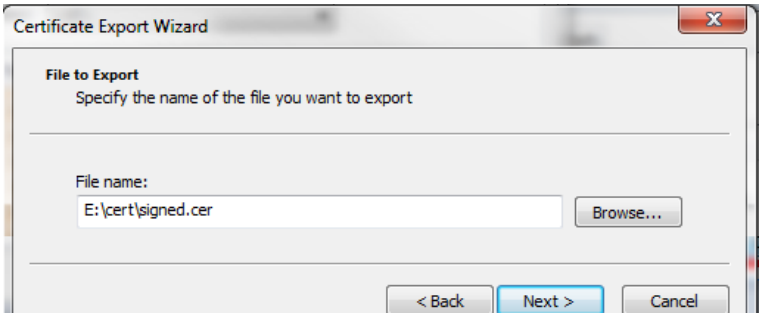

You will now be presented with the Certificate Export Wizard:



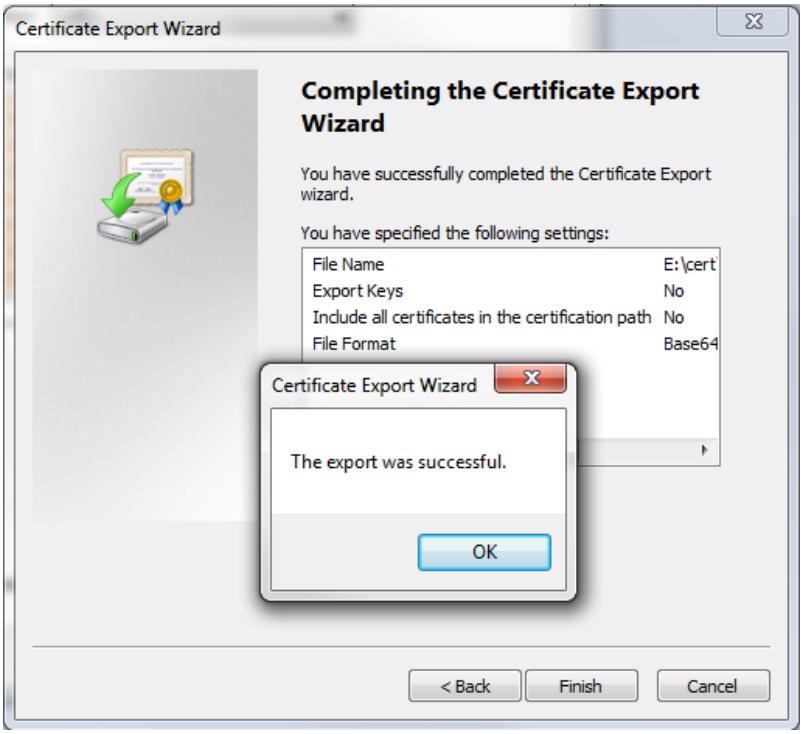
Select the option to export as **Base-64 encoded X.509 (.CER)**:

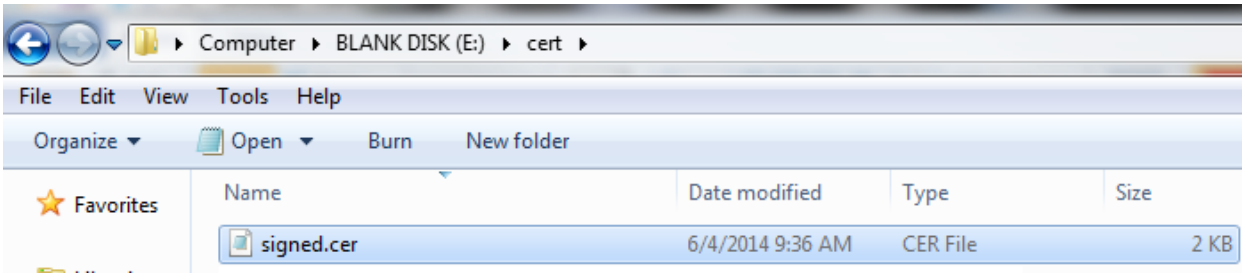



Specify a name for the certificate. It is a good idea to label them based on their certificate level so that it will be easier to pick them out when merging them. In this example, I'll name the certificate **signed.cer**, because it is the signed certificate.

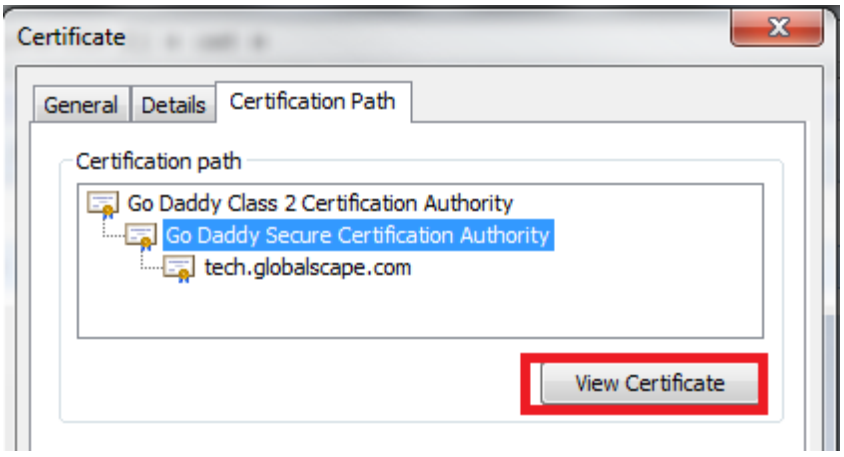



The signed certificate should now be exported:

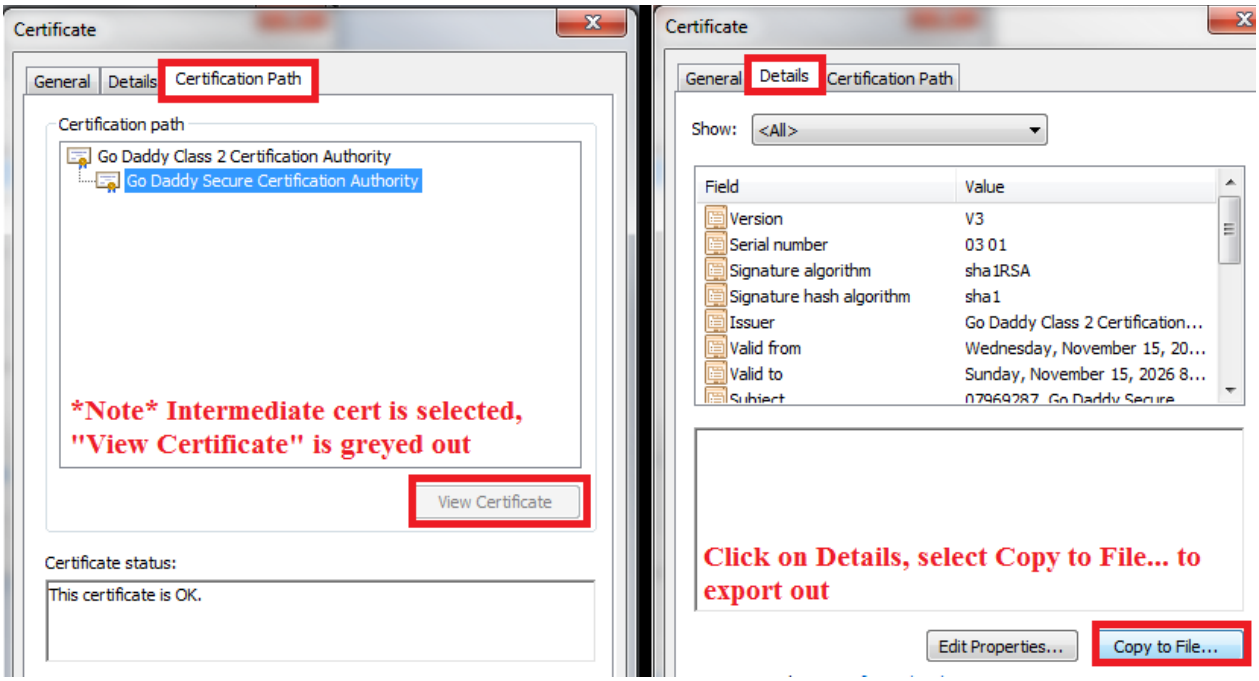


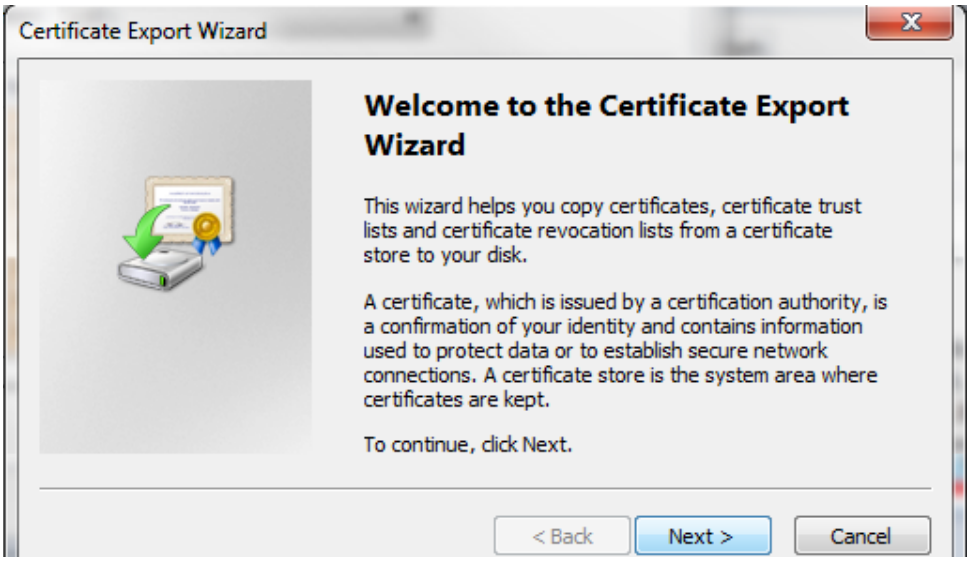

Next, click on the **Intermediate certificate** (there is generally 1-3 of them), and select **View Certificate:**



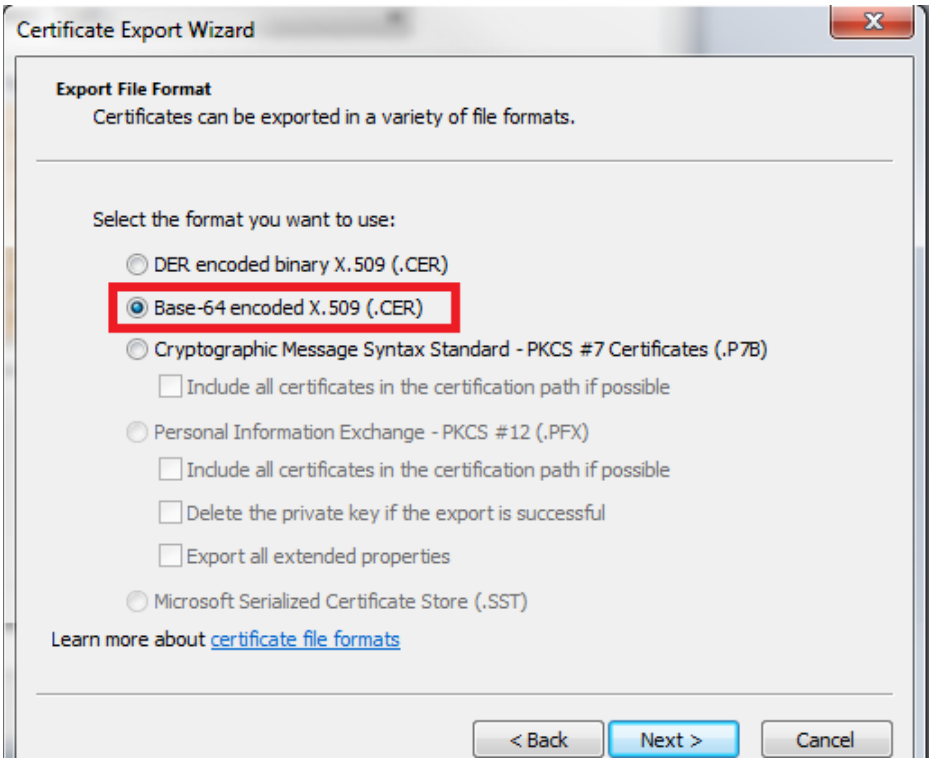
The intermediate certificate should now be selected.
Navigate to the **Details** tab and select **Copy To File…**




You will now be presented with the Certificate Export Wizard:

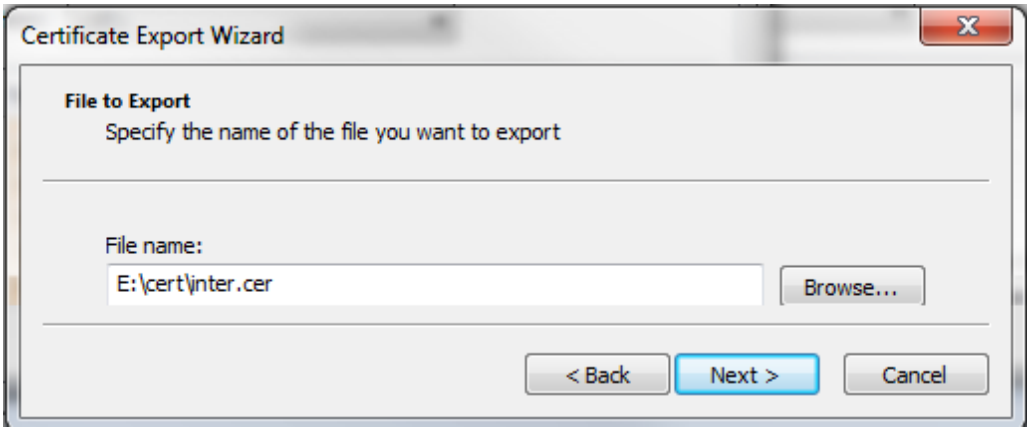


Select the option to export as **Base-64 encoded X.509 (.CER)**:

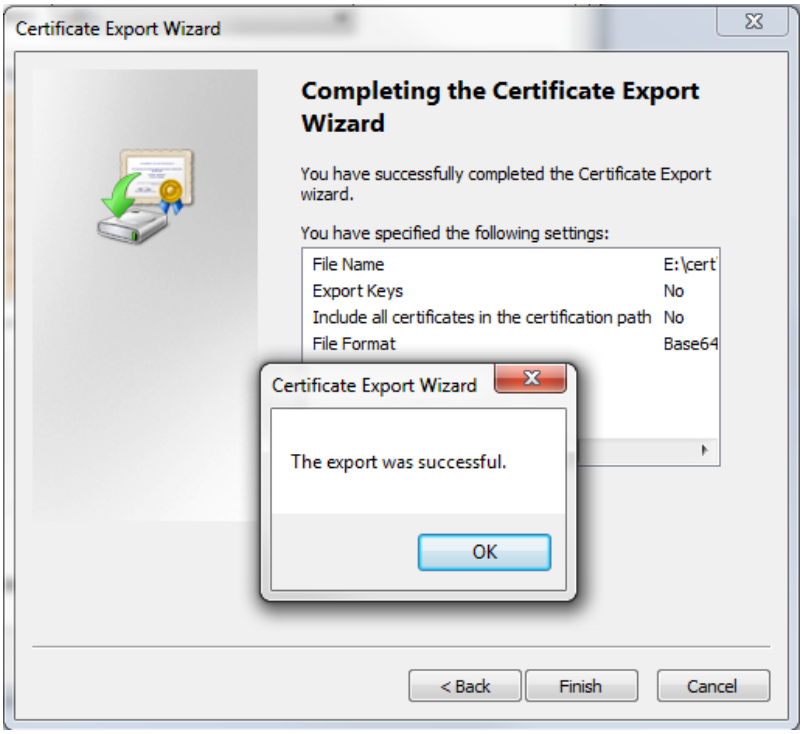


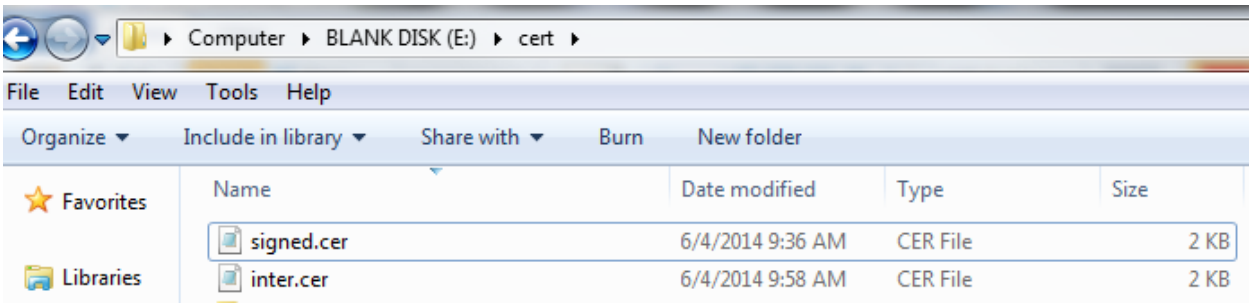

Just as before, it's a good idea to name the certs based on the certificate level so that it will be easier to pick them out when merging them. In this example, I'll name the certificate **inter.cer**, because it is the intermediate certificate.

If this certificate had multiple intermediate certs, I would call this **inter1.cer**.

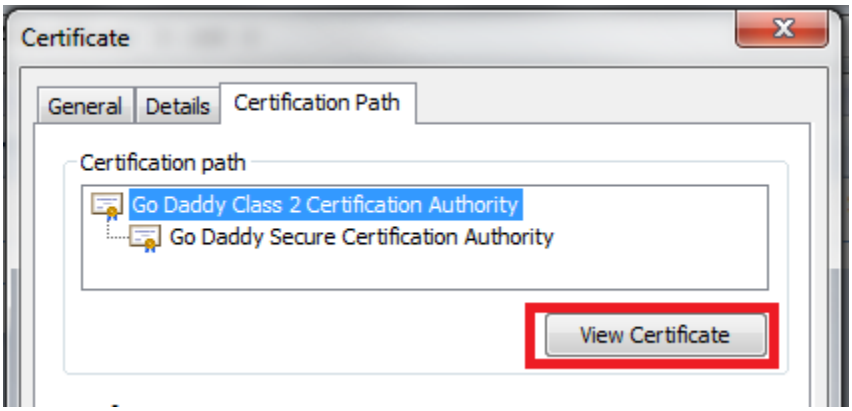


The intermediate certificate should now be exported (if there are multiple intermediate certs in the chain, this will be done for each certificate):

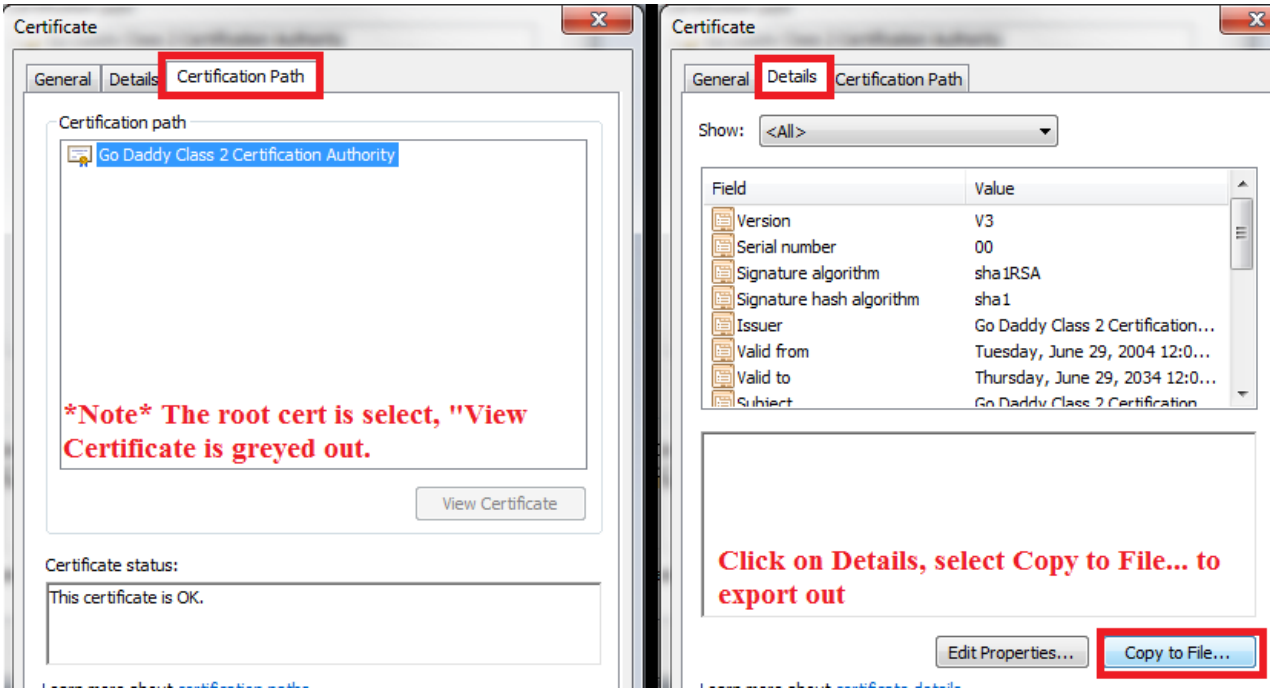


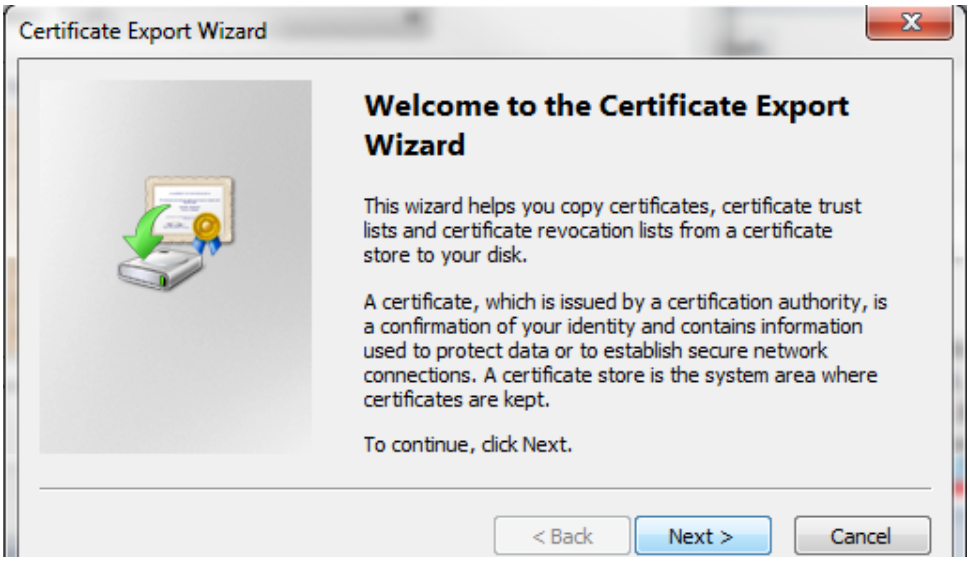
Finally, select the root certificate and click **View Certificate**.



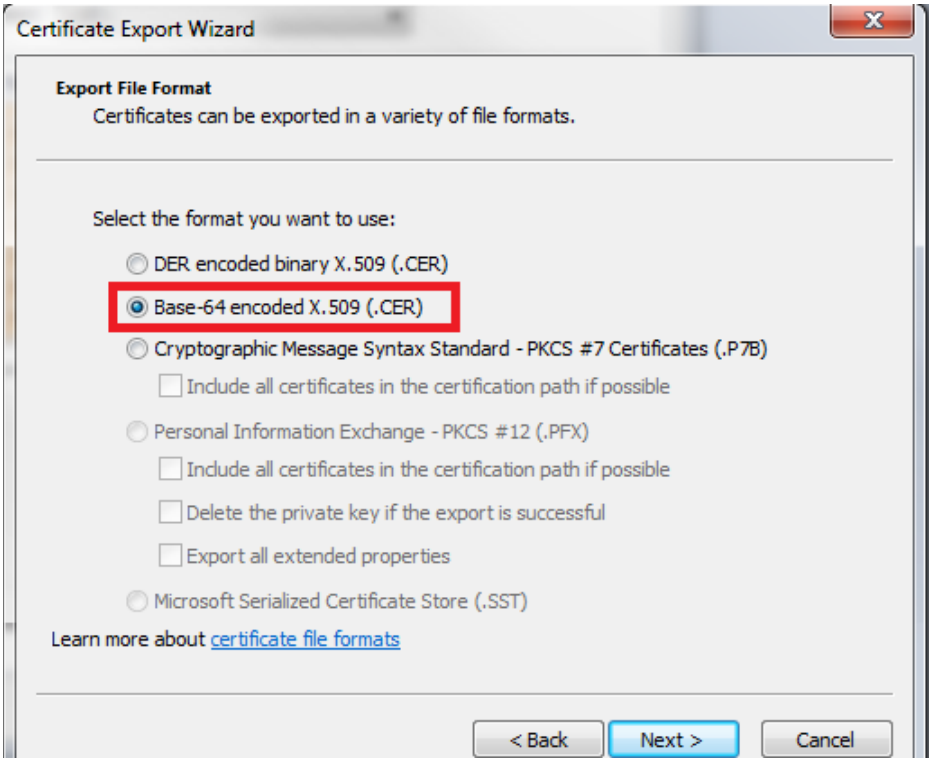

The root certificate should now be selected.
Navigate to the **Details** tab and select **Copy to File**.



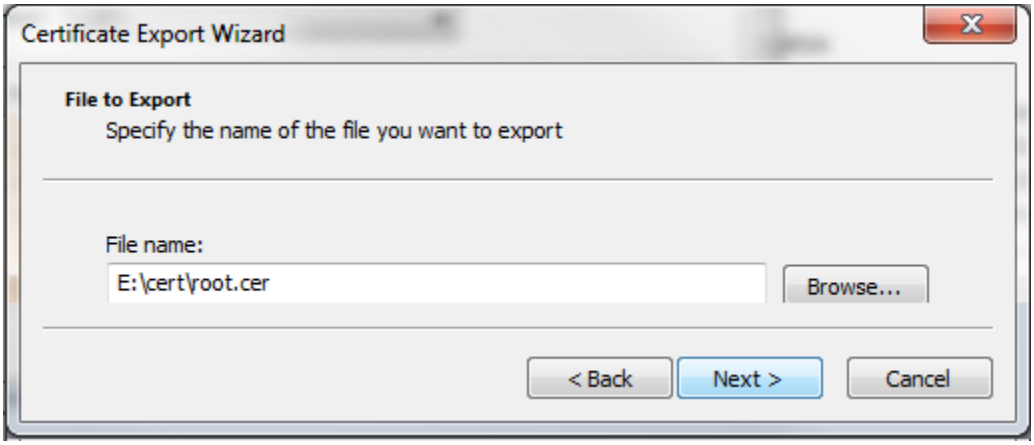
You will now be presented with the Certificate Export Wizard:



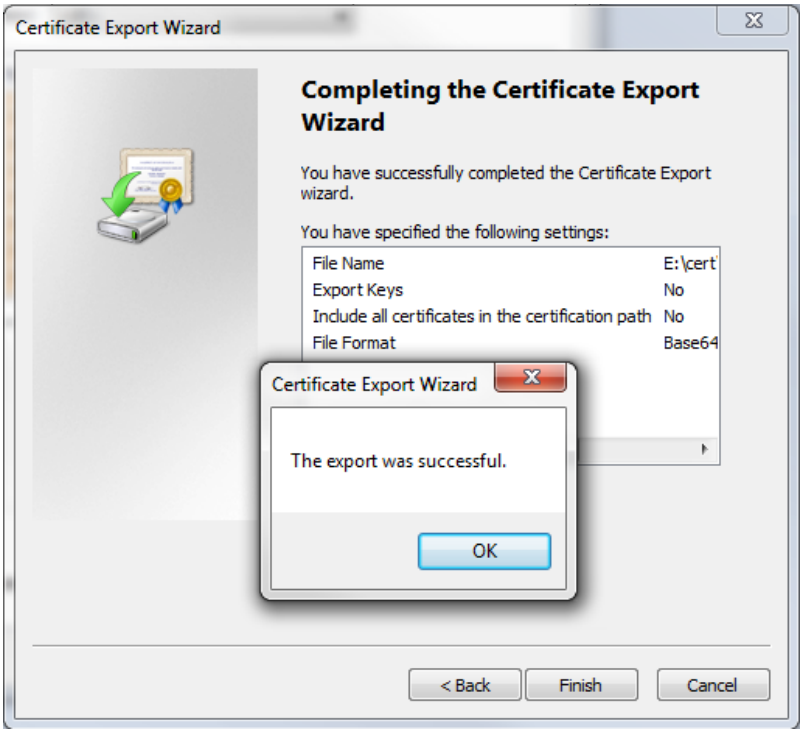

Select the option to export as **Base-64 encoded X.509 (.CER)**:

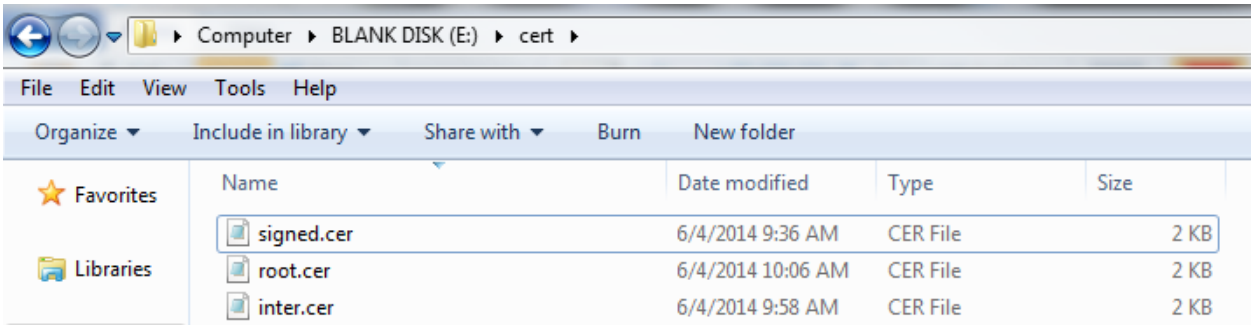


The certificate is being named **root.cer**, because it is the root certificate.



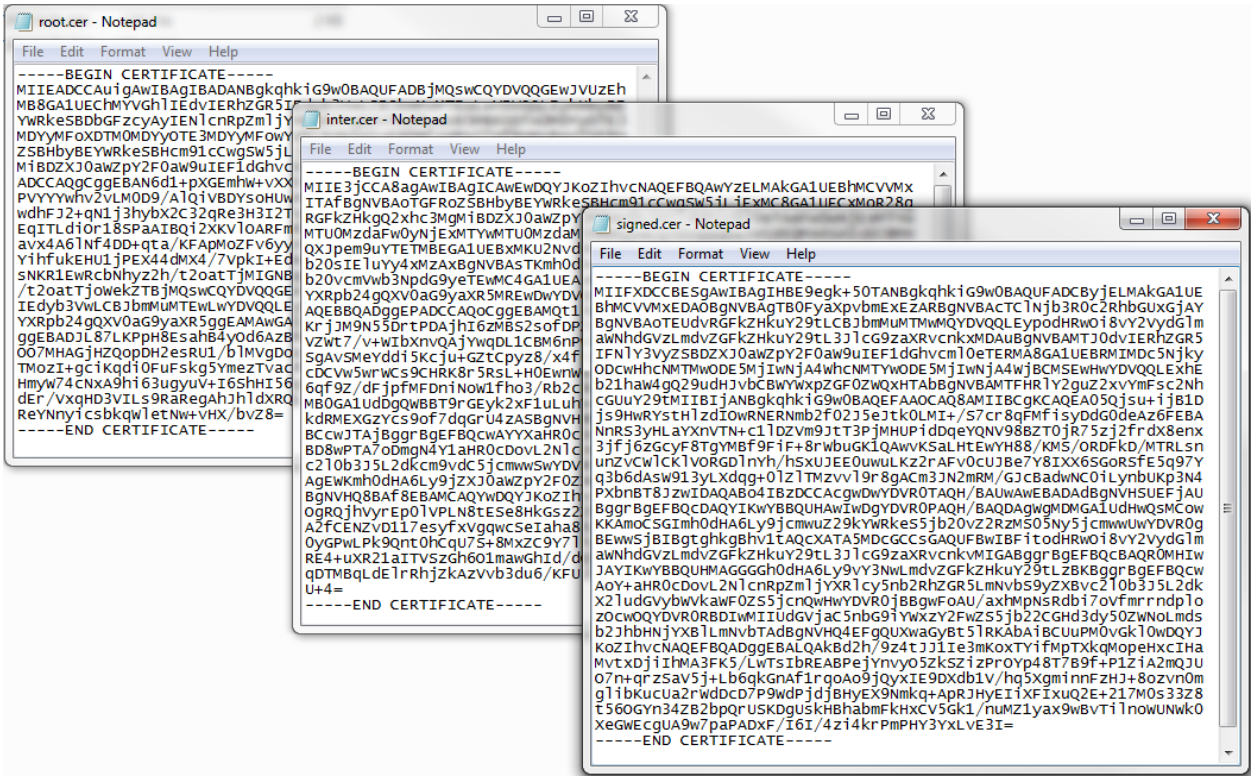

The root certificate should now be exported:



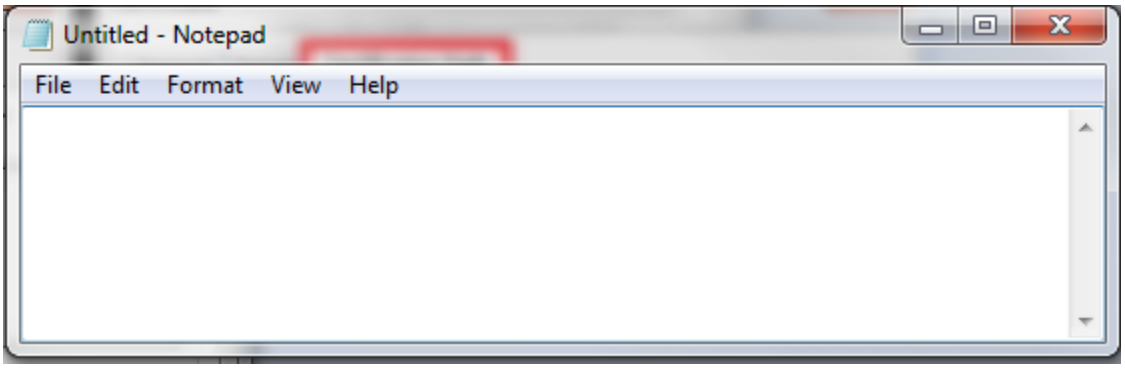



Now that we have all of the certificates in the certificate path, we can chain them together into one file.

First, open each file in notepad



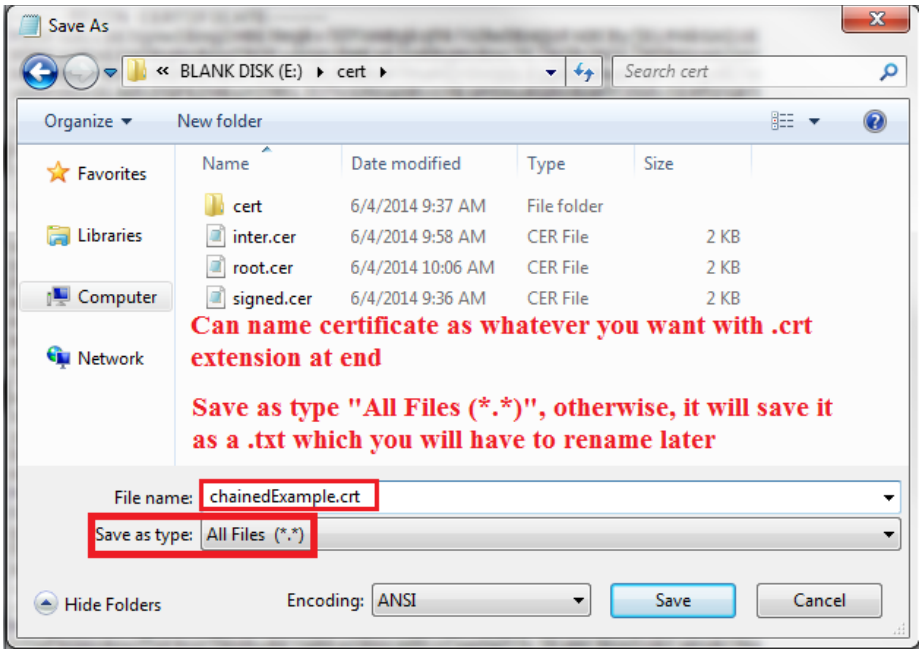

Then, open a blank notepad.



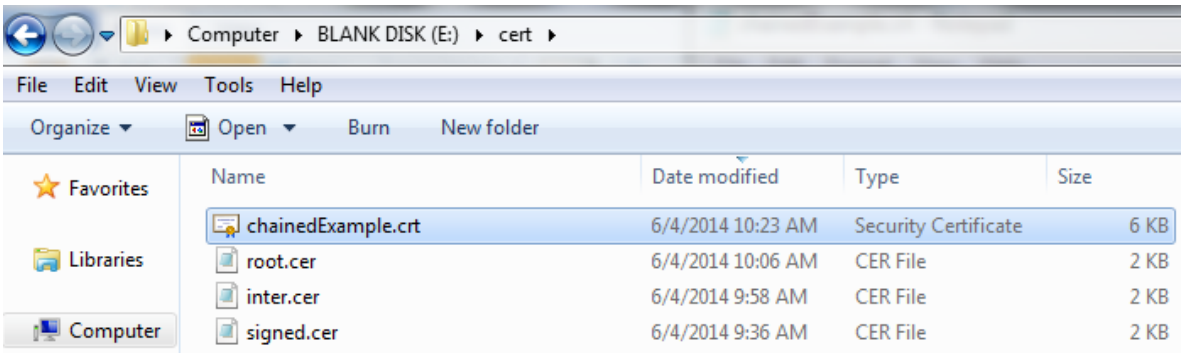

Copy/paste the exported certs in order (from top to bottom)

1) Signed (at the top)
2) Intermediate(s) [if you have multiple, paste them in order]
3) Root (at the bottom)

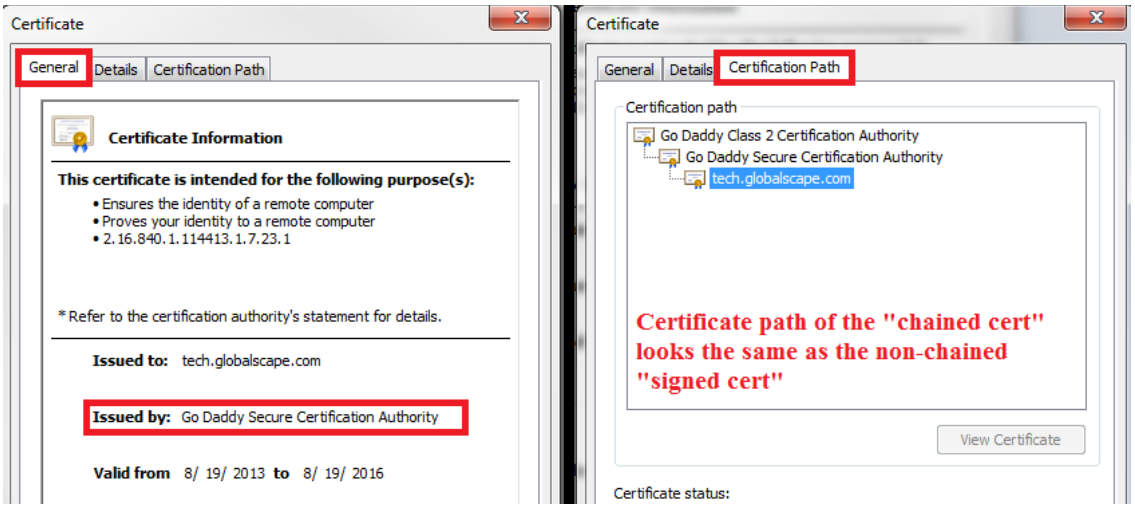

Save the file with a **.crt** extension.




To verify the certificate has been chained properly, double-click to open it.




The chained certificate should appear the same as the signed cert.



The major difference is that this “chained certificate” physically contains each certificate file in the certification path.

When implementing in EFT, you should use this as the certificate. Use the private key+passphrase that was generated during the certificate creation.