# 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".

Name	Date modified	Туре	Size	
🙀 globalscape.crt	6/4/2014 9:10 AM	Security Cer	tificate 2 KB	
Certificate	_	Cert	tificate	
General Details Certification Path		G	General Details Certific	ation Path
			Certification path	
Certificate Information			Go Daddy Class 2	Certification Authority cure Certification Authority
This certificate is intended for the for	ollowing purpose(s):		tech.globa	alscape.com
Proves your identity to a remote co     2.16.840.1.114413.1.7.23.1	omputer			
* Refer to the certification authority's sta	tement for details.			
Issued to: tech.globalscape.com				
Issued by: Go Daddy Secure Cert	ification Authority			
Issued by. Go baddy Secure cert	Addition Additionary			View
Valid from 8/ 19/ 2013 to 8/	19/ 2016		Cortificato status	

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

2

globalscape.crt - Notepad		×
File Edit Format View Help		
Image: Contexperiment of the second secon	IAKGA1UE SGUXGJAY (2VydGln (2VydGln (DC5NjKy (QQLEXhE (MFsc2NK) SUF1jB1 SAZ6FEBA TdX8eno )/MTRLSr TdX8eno )/MTRLSr TdX8eno )/MTRLSr SFE5Q97 )/MTRLSr TdX8eno )/MTRLSr SFE5Q97 )/MTRLSr SFE5Q97 )/MTRLSr SF2SQ7 )/MTRLSr SF2SQ7 )/MTRLSr SF2SQ7 )/MTRLSr	
<u></u>		

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

Vame	Date modified	Type Siz	ze		
🚽 globalscape.crt	6/4/2014 9:10 AM	Security Certificate	2 KB		
rtificate		Certificate			<u> </u>
General Details Certification Path		General Detai	ls Certification Pa	ıth	
Certification path		Show: <all></all>		•	
Go Daddy Class 2 Certification Author	ty hority	Field		Value	
" <mark>H≞a</mark> j tech,giobaiscape.com		E Version Signature Signature Signature Valid from Valid from Valid to	nber : algorithm : hash algorithm n	V3 04 4f 5e 82 4f b9 d1 sha1RSA sha1 07969287, Go Daddy Securd Monday, August 19, 2013 5 Friday, August 19, 2016 5:C tech globalscape.com. Doma	= :0 )6: ▼
*Note*: signed cert is selected, unable to "View Certificate" Certificate status: This certificate is OK.	View Certificate	Click on	details, select	t Copy To File to expo	ort out.
		Learn more ab	out certificate deta	Edit Properties Copy to	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:

	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.
4	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, dick Next.

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

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
Delete the private key if the export is successful
Export all extended properties
<ul> <li>Microsoft Serialized Certificate Store (.SST)</li> </ul>
Learn more about certificate file formats

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.

ertificate E	xport Wizard		<b>—</b> ×
File to Ex	port		
Spec	ify the name of the file	you want to export	
File r	name:		
E:\	cert\signed.cer		Browse

The signed certificate should now be exported:

Certificate Export Wizard		)
	Completing the Certificate Ex Wizard	port
	You have successfully completed the Certificate wizard.	e Export
	You have specified the following settings:	
	File Name	E:\cert'
	Export Keys	No
	Include all certificates in the certification path	No
	File Format	Base64
	Certificate Export Wizard	
	The export was successful.	4
	ОК	
	< Back Finish	Cancel

<b>⊘</b> ,	Computer + BLANK DISK (E:) + cert +			
File Edit View	Tools Help			
Organize 🔻	Open   Burn New folder			
쑦 Favorites	Name	Date modified	Туре	Size
<b>P</b>	igned.cer	6/4/2014 9:36 AM	CER File	2 KB

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

Certificate			×
General	Details	Certification Path	]]
Certif	ication pa	ath	
	Go Daddy Go Da Go Da te	/ Class 2 Certification addy Secure Certifica ech.globalscape.com	n Authority ation Authority n
			View Certificate

5

\_\_\_\_\_

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

Certificate	Certificate	×
General Details Certification Path	General Details Certification Pa	ath
Certification path	Show: <ali></ali>	•
Go Daddy Secure Certification Authority	Field	Value 🔺
*Note* Intermediate cert is selected,	Version Serial number Signature algorithm Signature hash algorithm Issuer Valid from Valid to	V3 03 01 sha 1RSA sha 1 Go Daddy Class 2 Certification Wednesday, November 15, 20 Sunday, November 15, 2026 8 07969287. Go Daddy Secure
"View Certificate" is greyed out         View Certificate         Certificate status:         This certificate is OK.	Click on Details, so export out	elect Copy to File to Edit Properties

You will now be presented with the Certificate Export Wizard:

Certificate Export Wizard	x )
	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

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

ertificate Export Wizard
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
Delete the private key if the export is successful
Export all extended properties
<ul> <li>Microsoft Serialized Certificate Store (.SST)</li> </ul>
Learn more about certificate file formats
< Back Next > Cancel

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**.

Certificate Export Wizard	×
File to Export Specify the name of the file yo	u want to export
File name: E:\cert\inter.cer	Browse
	< Back Next > Cancel

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

Certificate Export Wizard		
	Completing the Certificate Ex Wizard	port
	You have successfully completed the Certificate wizard.	Export
	You have specified the following settings:	
	File Name	E:\cert
	Export Keys	No
	Include all certificates in the certification path	No
	File Format	Base64
	Certificate Export Wizard	
	The export was successful.	•
	ОК	
	< Back Finish	Cancel

<b>30</b> - <b>1</b>	Computer + BLANK DISK (E:) + cert	i 🕨			
File Edit View	Tools Help				
Organize 🔻	Include in library	Burn	New folder		
🔆 Favorites	Name		Date modified	Туре	Size
	igned.cer		6/4/2014 9:36 AM	CER File	2 KB
ز Libraries	inter.cer		6/4/2014 9:58 AM	CER File	2 KB

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

Certificate	J
General Details Certification Path	
Certification path	
View Certificate	

The root certificate should now be selected.

Navigate to the **Details** tab and select **Copy to File**.

ertificate	Certificate
General Details Certification Path	General Details Certification Path
Certification path	Show: <all></all>
	Field Value
*Note* The root cert is select, "View Certificate is greyed out.	E       Version       V3         E       Serial number       00         E       Signature algorithm       sha1RSA         E       Signature hash algorithm       sha1         E       Issuer       Go Daddy Class 2 Certification         E       Valid from       Tuesday, June 29, 2004 12:0         E       Valid to       Thursday, June 29, 2034 12:0         E       Subject       Go Daddy Class 2 Certification
Certificate status: This certificate is OK.	Click on Details, select Copy to File to export out
	Edit Properties 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):

ertificate Export Wizard	<b>X</b>
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 (.P	7B)
Include all certificates in the certification path if possible	
Personal Information Exchange - PKCS #12 (.PFX)	
Include all certificates in the certification path if possible	
Delete the private key if the export is successful	
Export all extended properties	
<ul> <li>Microsoft Serialized Certificate Store (.SST)</li> </ul>	
Learn more about certificate file formats	
< Back Next >	Cancel

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

Certificate Export Wizard	×
File to Export	
Specify the name of the file you want to	export
File name:	
E:\cert\root.cer	Browse
· · · · · · · · · · · · · · · · · · ·	
	< Back Next > Cancel
L	

The root certificate should now be exported:

Certificate Export Wizard		
	Completing the Certificate Expo Wizard	ort
	vou nave successfully completed the Certificate E wizard.	xport
	You have specified the following settings:	
	File Name E	:\cert'
	Export Keys N	lo
	Include all certificates in the certification path	lo
	File Format B	ase64
	Certificate Export Wizard	
	The export was successful.	•
	ОК	
	< Back Finish	Cancel

() ⊂ () •	Computer + BLANK	DISK (E:) 🕨 cert	•			
File Edit View	Tools Help					
Organize 🔻	Include in library 🔻	Share with 🔻	Burn	New folder		
🔆 Favorites	Name	T		Date modified	Туре	Size
	igned.cer			6/4/2014 9:36 AM	CER File	2 KB
🥽 Libraries	root.cer			6/4/2014 10:06 AM	CER File	2 KB
	inter.cer			6/4/2014 9:58 AM	CER File	2 KB

## 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.

Untitled - Notepad	
File Edit Format View Help	
	~
	-

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.

Save As	1 day		-	-		X
<b>⊘</b> ⊽∎«	BLANK DISK (E:)	cert 🕨	• 4 <sub>7</sub>	Search cert		٩
Organize 🔻	New folder				•	0
🔆 Favorites	Name	Date modified	Туре	Size		
	鷆 cert	6/4/2014 9:37 AM	File folder			
📄 Libraries	inter.cer	6/4/2014 9:58 AM	CER File	2 KB		
	root.cer	6/4/2014 10:06 AM	CER File	2 KB		
🖳 Computer	signed.cer	6/4/2014 9:36 AM	CER File	2 KB	1	
🗣 Network	Can name c extension at Save as type as a .txt whi	ertificate as wh t end e "All Files (*.* ich you will hav	atever yo )'', other 'e to rena	ou want wi wise, it wil me later	ith .crt Il save it	
File nan Save as typ	ne: chainedExample pe: All Files (*.*)	e.crt				•
Alide Folders	Encod	ding: ANSI	•	Save	Cance	<b></b>

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

<b>€ • • •</b>	Computer   BLANK DISK (E:)   cert			
File Edit View	Tools Help			
Organize 🔻	🖬 Open 🔻 Burn New folder			
🔆 Favorites	Name	Date modified	Туре	Size
	🔄 chainedExample.crt	6/4/2014 10:23 AM	Security Certificate	6 KB
🥃 Libraries	root.cer	6/4/2014 10:06 AM	CER File	2 KB
	inter.cer	6/4/2014 9:58 AM	CER File	2 KB
🖳 Computer	signed.cer	6/4/2014 9:36 AM	CER File	2 KB

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

Certificate	Certificate
General Details Certification Path	General Details Certification Path
Certificate Information This certificate is intended for the following purpose(s): • Ensures the identity of a remote computer • Proves your identity to a remote computer • 2.16.840.1.114413.1.7.23.1	Certification path Go Daddy Class 2 Certification Authority Go Daddy Secure Certification Authority tech.globalscape.com
* Refer to the certification authority's statement for details.  Issued to: tech.globalscape.com	Certificate path of the "chained cert" looks the same as the non-chained "signed cert"
Issued by: Go Daddy Secure Certification Authority	View Certificate
Valid from 8/ 19/ 2013 to 8/ 19/ 2016	Certificate status:

\_\_\_\_\_\_

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.