

Convert a DER Certificate File to PEM Format

A private key, root (CA) certificate and the server / client certificate can be generated using third-party tools (or purchased from a certificate authority), and may be generated as PEM (required format, extension .pem) or DER (extension .cer) format files.

Certificates must be in PEM format for use on the Expressway. Conversion from DER to PEM format is done either using OpenSSL or Windows, as documented in the following sections.

Convert a DER certificate file to a PEM file using OpenSSL

To convert from DER to PEM format, on a system running openssl, execute the command:

openssl x509 -in <filename>.cer -inform DER -out <filename>.pem -outform PEM

Convert a DER certificate file to a PEM file using Microsoft Windows

To convert from DER to PEM format using Microsoft Windows:

1. Double click the DER file to convert (this will likely have a '.cer' extension)

I

19	Certificate Information
Win this	dows does not have enough information to verify certificate.
	Issued to: tsbu-rusc01-alpha-cluster01.cisco.com
	Issued by: rusc-lync-LYNC1-CA Valid from 05/ 07/ 2011 to 04/ 07/ 2013
	Install Certificate Issuer Statement

2. Select the Details tab

iow: <all> Field Value Version V3 Serial number 1e d2 d3 73 00 00 00 00 00 00 08 Signature algorithm sha1RSA Signature hash algorithm sha1 Issuer rusc-lync-LYNC1-CA, rusc-lync Valid from 05 July 2011 17:02:07 Valid to 04 July 2013 17:02:07 Subject tsbu-rusc01-alpha-cluster01.ci</all>		
Field Value Version V3 Serial number 1e d2 d3 73 00 00 00 00 00 00 08 Signature algorithm sha1RSA Signature hash algorithm sha1 Issuer rusc-lync-LYNC1-CA, rusc-lync Valid from 05 July 2011 17:02:07 Valid to 04 July 2013 17:02:07 Subject tshu-rusc01-aloba-cluster01_ci	iow: <ali></ali>	•
Version V3 Serial number 1e d2 d3 73 00 00 00 00 00 00 08 Signature algorithm sha1R5A Signature hash algorithm sha1 Issuer rusc-lync-LYNC1-CA, rusc-lync Valid from 05 July 2011 17:02:07 Valid to 04 July 2013 17:02:07 Subject tsbu-rusc01-alpha-cluster01_ci	Field	Value 🔦
	Version Serial number Signature algorithm Signature hash algorithm Issuer Valid from Valid to Subject	V3 1e d2 d3 73 00 00 00 00 00 00 08 sha1R5A sha1 rusc-lync-LYNC1-CA, rusc-lync 05 July 2011 17:02:07 04 July 2013 17:02:07 http://www.coll-alpha-cluster01_ci

- 3. Click Copy to File...
- 4. On the Welcome page, click Next

5. Select Base-64 encoded X.509 (.CER) and click Next

he format you want to use: DER encoded binary X.509 (.CER) Bage-64 encoded X.509 (.CER)	
DER encoded binary X.509 (.CER) Bage-64 encoded X.509 (.CER)	
Bage-64 encoded X.509 (.CER)	
Cryptographic Message Syntax Standard -	PKCS #7 Certificates (.P78)
Include all certificates in the certification	n path if possible
ersonal Information Exchange - PKCS #12	(.PFX)
Include all certificates in the certification	n path if possible
Delete the private key if the export is s	uccessful
Export all extended properties	
Microsoft Serialized Certificate Store (.SST)	
about <u>certificate file formats</u>	
1	Include all certificates in the certificatio Dersonal Information Exchange - PKCS #12 Include all certificates in the certificatio Delete the private leav if the export is s Export all extended properties Microsoft Serialized Certificate Store (.SST) about certificate file formats

- 6. Click Browse and select required destination for file (e.g. server.pem) and then click Next
- 7. Click Finish
- 8. Change the filename from server.pem.cer to server.pem
- 9. This is used in the Load Certificates and Keys Onto Expressway section of this document.