Certificates and Encodings

At its core an X.509 certificate is a digital document that has been encoded and/or digitally signed according to RFC 5280.

In fact, the term *X.509 certificate* usually refers to the IETF's PKIX Certificate and CRL Profile of the X.509 v3 certificate standard, as specified in RFC 5280, commonly referred to as PKIX for *Public Key Infrastructure (X.509)*.

X509 File Extensions

The first thing we have to understand is what each type of file extension is. There is a lot of confusion about what DER, PEM, CRT, and CER are and many have incorrectly said that they are all interchangeable. While in certain cases some can be interchanged the best practice is to identify how your certificate is encoded and then label it correctly. Correctly labeled certificates will be much easier to manipulat

Encodings (also used as extensions)

- .DER = The DER extension is used for binary DER encoded certificates. These files may also bear the CER or the CRT extension. Proper English usage would be "I have a DER encoded certificate" not "I have a DER certificate".
- .PEM = The PEM extension is used for different types of X.509v3 files which contain ASCII (Base64) armored data prefixed with a "—– BEGIN …" line.

Common Extensions

- .CRT = The CRT extension is used for certificates. The certificates may be encoded as binary DER or as ASCII PEM. The CER and CRT extensions are nearly synonymous. Most common among *nix systems
- CER = alternate form of .crt (Microsoft Convention) You can use MS to convert .crt to .cer (.both DER encoded .cer, or base64[PEM] encoded .cer) The **.cer** file extension is also recognized by IE as a command to run a MS cryptoAPI command (specifically rundll32.exe cryptext.dll,CryptExtOpenCER) which displays a dialogue for importing and/or viewing certificate contents.
- .KEY = The KEY extension is used both for public and private PKCS#8 keys. The keys may be encoded as binary DER or as ASCII PEM.

The only time CRT and CER can safely be interchanged is when the encoding type can be identical. (ie PEM encoded CRT = PEM encoded CER)

Common OpenSSL Certificate Manipulations

There are four basic types of certificate manipulations. View, Transform, Combination , and Extraction

View

Even though PEM encoded certificates are ASCII they are not human readable. Here are some commands that will let you output the contents of a certificate in human readable form;

View PEM encoded certificate

Use the command that has the extension of your certificate replacing cert.xxx with the name of your certificate

```
openssl x509 -in cert.pem -text -noout
openssl x509 -in cert.cer -text -noout
openssl x509 -in cert.crt -text -noout
```

If you get the folowing error it means that you are trying to view a DER encoded certifciate and need to use the commands in the "View DER encoded certificate below"

```
unable to load certificate
12626:error:0906D06C:PEM routines:PEM_read_bio:no start line:pem_lib.c:647:Expecting: TRUSTED CERTIFICATE
```

View DER encoded Certificate

```
openssl x509 -in certificate.der -inform der -text -noout
```

If you get the following error it means that you are trying to view a PEM encoded certificate with a command meant for DER encoded certs. Use a command in the "View PEM encoded certificate above

```
unable to load certificate
13978:error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag:tasn_dec.c:1306:
13978:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error:tasn_dec.c:380:Type=X509
```

Transform

Transforms can take one type of encoded certificate to another. (ie. PEM To DER conversion)

PEM to DER

```
openssl x509 -in cert.crt -outform der -out cert.der
```

DER to PEM

```
openssl x509 -in cert.crt -inform der -outform pem -out cert.pem
```

Combination

In some cases it is advantageous to combine multiple pieces of the X.509 infrastructure into a single file. One common example would be to combine both the private key and public key into the same certificate.

The easiest way to combine certs keys and chains is to convert each to a PEM encoded certificate then simple copy the contents of each file into a new file. This is suitable for combining files to use in applications like Apache.

Extraction

Some certs will come in a combined form. Where one file can contain any one of: Certificate, Private Key, Public Key, Signed Certificate, Certificate Authority (CA), and/or Authority Chain.