Certificate File Formats

The file formats and naming convention of extensions is all over the place.

PEM (Privacy Enhanced Mail) Format

The most common format that CAs issue certificates in. The extension can be,

- crt
- cer
- cert
- pem
- key

The file is also Base64 encoded ASCII and with general certificates contains "BEGIN CERTIFICATE" and "END CERTIFICATE". The following certificates can be stored as PEM,

- Server Certificates (this the CA signed public key certificate)
- Intermediate Certificates
- Private Keys

> The BonsaiFramework uses the extension **format.crt** for the following certificates because the extension is recognized by Windows. Double-clicking on a crt file in Windows will show details about the certificate. We use the format.crt extension for the following,
>
> - Server Certificates for example, www.krypton.com*.crt*
> - Intermediate Certificates for example, www.krypton.com**_signed_cert.crt**
>
> By convention and because these keys do not work in Windows we use the following extensions,
>
> - key - Private Server Key for example, www.krypton.com.key
> - csr - Certificate Signing Requests must be decoded, www.krypton.com.csr

DER Format

The DER format is a binary form of the certificate. It is best to use the.der extension but sometimes the .cer extension is used. In that case you must open the with a text editor and look for BEGIN/END statements.

All types of certificates and private keys can be encoded in DR. DER is typically used with Java.

P7b Format

Converting from Open SSL to IKeyman

> This has not been verified. I ended up recreating my certificate as the version of IKeyman had a bug exporting certificates from the key database.

Import OpenSSL to IKeyman - http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itame.doc/ss7cumst46.htm

IBM IHS import experience - http://luskwater.blogspot.com/2009/04/importing-certificates-from-openssl.html

Import OpenSSL to IKeyman (this doc looks complete) - http://i-proving.ca/space/Brett+Dubroy/blog/2008-08-07_1

References

Good description of formats - https://www.sslshopper.com/ssl-converter.html

OpenSSL uses PKCS#12 (what is this a format?) as input and PEM as output - http://www.openssl.org/docs/apps/pkcs12.html#COMMAND_OPTIONS

More discussion on formats - http://www.bo.infn.it/alice/introgrd/certmgr/node2.html

Converting between formats - http://support.sas.com/documentation/cdl/en/secref/62092/HTML/default/viewer.htm#a002815156.htm

See what is in a cert - http://www.sslshopper.com/certificate-decoder.html

A great decoder that shows encryption and key size along with the certificate information - https://certlogik.com/decoder/