

DIFFERENCES BETWEEN PEM, DER, P7B/PKCS#7, PFX/PKCS#12 (PKI)

Different Platforms & Devices requires SSL certificates in different formats:

- A **Windows Server** uses **.pfx** files;
- An **Apache Server** uses **.crt, .cer** files;

NOTE: Only way to tell the difference between **PEM .cer** and **DER .cer** is to open the file in a text editor and look for the **BEGIN/END** statements.

PEM Format

It is the most common format that **Certificate Authorities** issue certificates in. It contains the “**--BEGIN CERTIFICATE--**” and “**--END CERTIFICATE--**” statements.

Several **PEM** certificates and even the **Private** key can be included in one file, one below the other. But most platforms (example: **Apache**) expects the certificates and **Private** key to be in separate files.

- They are **Base64** encoded **ASCII** files;
- They have extensions such as **.pem, .crt, .cer, .key**;
- **Apache** and similar servers uses **PEM** format certificates;

DER Format

It is a **Binary** form of **ASCII PEM** format certificate. All types of **Certificates & Private Keys** can be encoded in **DER** format.

- They are **Binary** format files;
- They have extensions **.cer & .der**;
- **DER** is typically used in **Java** platform;

P7B/PKCS#7

They contain “**--BEGIN PKCS--**” & “**--END PKCS7--**” statements. It can contain only **Certificates & Chain** certificates but *not the Private key*.

- They are **Base64** encoded **ASCII** files;
- They have extensions **.p7b, .p7c**;
- Several platforms supports it. For example: **Windows OS, Java Tomcat**;

PFX/PKCS#12

They are used for storing the **Server** certificate, any **Intermediate** certificates & **Private** key in one encryptable file.

- They are **Binary** format files;
- They have extensions **.pfx, .p12**;
- Typically used on **Windows OS** to import and export certificates and **Private** keys;