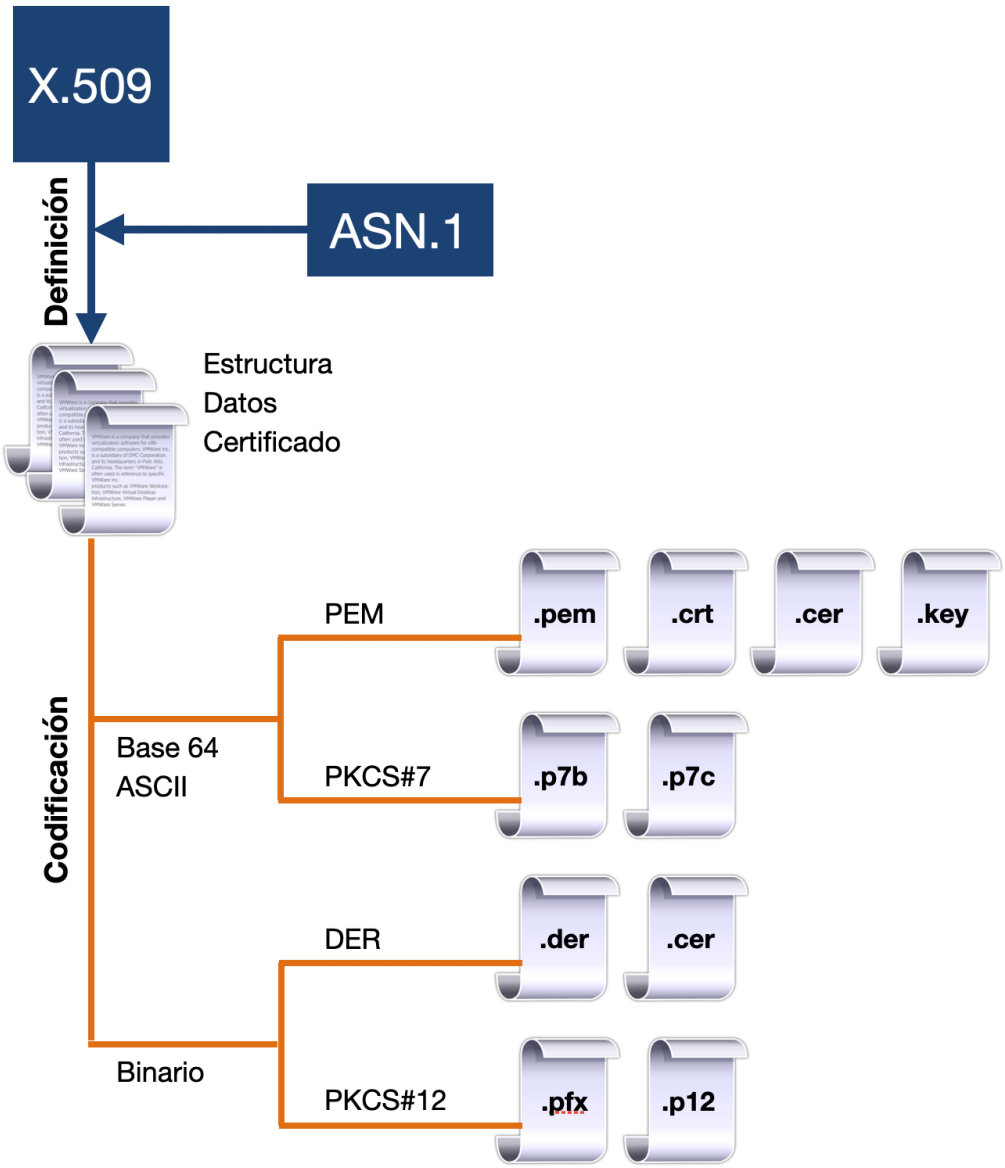
Formatos de los certificados

Un certificado SSL es esencialmente un certificado X.509. X.509 es un estándar que define la estructura del certificado. Define los campos de datos que deben incluirse en el certificado SSL. X.509 utiliza un lenguaje formal llamado notación de sintaxis abstracta uno (Abstract Syntax Notation One) o ASN.1, para expresar la estructura de datos del certificado.

Existen diferentes formatos de certificados X.509 como PEM, DER, PKCS # 7 y PKCS # 12. Los formatos PEM y PKCS # 7 usan codificación ASCII Base64 mientras que DER y PKCS # 12 usan codificación binaria. Los archivos de certificado tienen diferentes extensiones según el formato y la codificación que utilizan.

La siguiente figura ilustra los formatos de codificación del certificado X.509 y las extensiones de archivo



Formato PEM

La mayoría de las CA (Autoridad de certificación) proporcionan certificados en formato PEM en archivos codificados ASCII Base64. Los tipos de archivo de certificado pueden ser .pem, .crt, .cer o .key. El archivo .pem puede incluir el certificado del servidor, el certificado intermedio y la clave privada en un solo archivo. El certificado del servidor y el certificado intermedio también pueden estar en un archivo .crt o .cer separado. La clave privada puede estar en un archivo .key.

Los archivos PEM usan codificación ASCII, por lo que puede abrirlos en cualquier editor de texto, como el bloc de notas, MS word, etc. Cada certificado en el archivo PEM está contenido entre el ---- BEGIN CERTIFICATE ---- y ---- END CERTIFICATE ---- declaraciones. La clave privada está contenida entre las declaraciones ---- BEGIN RSA PRIVATE KEY ----- y ----- END RSA PRIVATE KEY -----. El CSR está contenido entre las declaraciones ----- BEGIN CERTIFICATE REQUEST ----- y ----- END CERTIFICATE REQUEST ----

Formato PKCS # 7

El formato PKCS # 7 es un estándar de sintaxis de mensajes criptográficos. El certificado PKCS # 7 utiliza la codificación ASCII Base64 con la extensión de archivo .p7b o .p7c. Solo los certificados se pueden almacenar en este formato, no las claves privadas. Los certificados P7B están contenidos entre las declaraciones "----- BEGIN PKCS7 -----" y "----- END PKCS7 -----".

Formato DER

Los certificados DER están en forma binaria, contenidos en archivos .der o .cer. Estos certificados se utilizan principalmente en servidores web basados en Java.

Formato PKCS # 12

Los certificados PKCS # 12 están en forma binaria, contenidos en archivos .pfx o .p12.

El PKCS # 12 puede almacenar el certificado del servidor, el certificado intermedio y la clave privada en un único archivo .pfx con protección por contraseña. Estos certificados se utilizan principalmente en la plataforma Windows.

Revision #1
Created 18 May 2022 07:19:26 by Admin
Updated 18 May 2022 07:20:38 by Admin