Elementos y carateriscias de un certificado

El formato mas popular de certificado publicos es el X.509 , que nos permite agrupar una serie de características y valores, que han sido verificados y aprobados por una entidad certificadora.

Los certificados se organizan de forma generarica, conteniendo una cadena de certificación, siento generalmente el certificado creado por un certifica intermedio y el certificaod intermedio por un certificado raíz (que representa una entidad certificadora).

Los certiciados raíces, confiand en si mismos, esto es, que no necesita de una entidad superior para ser confiable, generalmente estna instalados por defecto en los navegadores y los sistemas operativos (en los que confiamos), si instatalos navegadore o sistemas operativos de dudosa procencia, pude instalarlos certificados raíces apócrifos y podemos ser victimas de un ataque por parte de un intruso.

Elemetos de un certicicado

Fecha de validez, indica la fecha máxima en la que el certicifcado es valido

Suject:

Es la persona, empresa o servicio para el cual se creo el certiciado, tiene una estructura en forma de cadena que agrupa elementos como su nombre, su estado, su país, o su correcto electrónico, de la siquiente forma:

CN = ejemplohost

O = Capacitacion Criptografia Certificados Privacidad

L = Guadalajara

S = Jalisco

C = MX

CLR

KeyUsage

extendedKeyUsage

**OID**

An object identifier (OID) for the extension value. OIDs are strings of numbers separated by periods. The following OIDs are defined in RFC 3280 and RFC 5280.

* 1.3.6.1.5.5.7.3.1 (TLS\_WEB\_SERVER\_AUTHENTICATION)
* 1.3.6.1.5.5.7.3.2 (TLS\_WEB\_CLIENT\_AUTHENTICATION)
* 1.3.6.1.5.5.7.3.3 (CODE\_SIGNING)
* 1.3.6.1.5.5.7.3.4 (EMAIL\_PROTECTION)
* 1.3.6.1.5.5.7.3.8 (TIME\_STAMPING)
* 1.3.6.1.5.5.7.3.9 (OCSP\_SIGNING)
* 1.3.6.1.5.5.7.3.5 (IPSEC\_END\_SYSTEM)
* 1.3.6.1.5.5.7.3.6 (IPSEC\_TUNNEL)
* 1.3.6.1.5.5.7.3.7 (IPSEC\_USER)

Uso extendido.

Algoritmo de firma

Clave publica

Valid Values: DIGITAL\_SIGNATURE | NON\_REPUDIATION | KEY\_ENCIPHERMENT | DATA\_ENCIPHERMENT | KEY\_AGREEMENT | CERTIFICATE\_SIGNING | CRL\_SIGNING | ENCIPHER\_ONLY | DECIPHER\_ONLY | ANY | CUSTOM

<https://superuser.com/questions/738612/openssl-ca-keyusage-extension>