

Certificado digital X.509

Un certificado digital es una credencial utilizada para autenticar la identidad de una persona o entidad en el entorno digital.

Contiene información como el nombre de la entidad, su clave pública y la firma digital de una autoridad confiable. Se utilizan en diversas aplicaciones, como cifrado de datos, autenticación de sitios web y firmas electrónicas, para garantizar la seguridad y la confianza en las comunicaciones y transacciones en línea.

Se utiliza el estandar X.509 para certificados digitales, se divide en:

Subject (sujeto): Identifica a la entidad o sujetos al que se emite el certificado. Contiene información como el nombre, la organización y la ubicación del sujeto.

Issuer (emisor): Es la entidad emisora CA

Validity (validad): Es el campo que indica el periodo de tiempo durante el cual el certificado es válido.