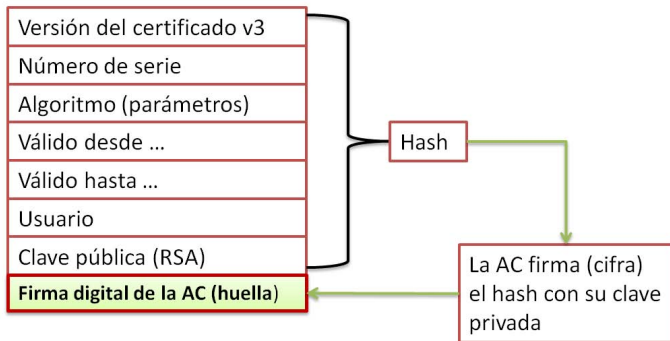
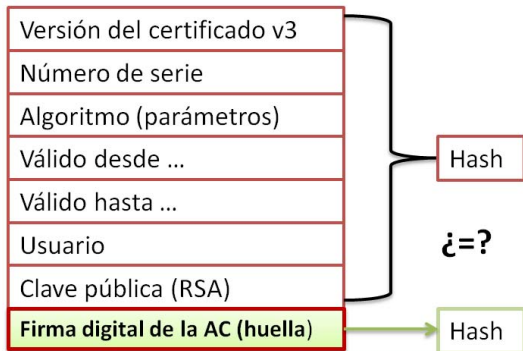


Certificado digital: norma X.509

Basado en RSA-estándar PKCS #1v1.5.
Firma digital RSA con hash SHA-256



Certificado digital X.509- verificación



Se verifica (descifra) la firma con la clave pública de la CA, si coincide con el hash de los datos la firma es válida