Javier García Tercero

Tarea 5 Ejercicios, tema 5

EJERCICIOS: 18

14 de abril, 2025

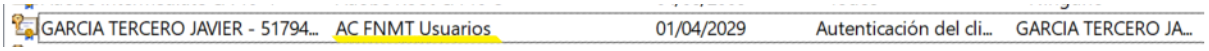
Curso 2024-2025. UCLM, Albacete
Aspectos profesionales de la informática
3º Curso del Grado en Ingeniería Informática
Grupo B de teoría y Grupo P5.02 de prácticas

Ejercicio 18

Apartado a)

¿Cuál es la Autoridad de Certificación (AC) de tu certificado digital?

La Autoridad de Certificación de mi certificado digital es la FNMT (Fábrica Nacional de Moneda y Timbre), apareciendo más concretamente como “AC FNMT Usuarios” para la firma electrónica. Para el DNI electrónico encontramos como AC al Ministerio del Interior a través de la Dirección de la Policía Nacional.

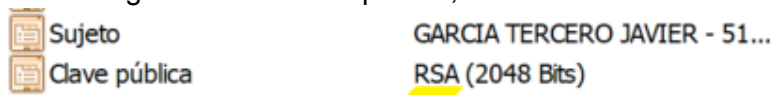


¿Cuál es el tamaño de la clave pública de tu certificado digital?

El tamaño de la clave pública para mi certificado digital es de 2048 Bits.

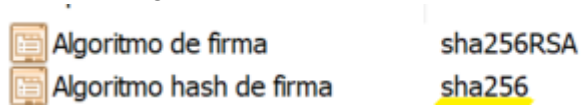
¿Cuál es el algoritmo de cifrado de clave pública utilizado?

El algoritmo de cifrado de clave pública usado para el certificado de la FNMT como para el DNIe es el RSA (Rivest-Shamir-Adleman), un algoritmo basado en la dificultad de factorizar grandes números primos, alrededor del orden de 10^300.



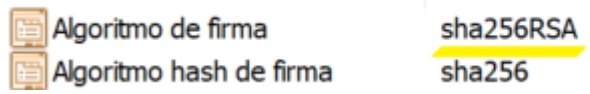
¿Cuál es el algoritmo de hash de firma?

El algoritmo hash de firma es el sha256 para ambas certificaciones.



¿Cuál es el algoritmo de generación de firma electrónica utilizado?

El algoritmo de generación de firma electrónica es el SHA256RSA, una combinación entre el algoritmo de cifrado y el algoritmo hash de firma.



Bibliografía

Portal del DNI Electronico, Cuerpo Nacional de Policía. (n.d.). Retrieved April 14, 2025, from https://www.dnielectronico.es/PortalDNIe/

Sede electrónica. (n.d.). Sede. Retrieved April 14, 2025, from https://www.sede.fnmt.gob.es/

Wikimedia, C. de los proyectos. (2024, December 29). *RSA*. Wikipedia. https://es.wikipedia.org/wiki/RSA