
Pregunta

[Mathew Lambert](#) · 20 jul, 2020

El modo de encriptación PBKDF2 con HMAC-SHA a 512 bits, es acorde con las recomendaciones NIST / FIPS?

Usamos el método de encriptación de contraseñas mencionado y necesitamos saber si la implementación es acorde con las recomendaciones NIST / FIPS <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>

Leyendo la documentación no me queda 100% claro ya que dice "(See RSA Laboratories Public-Key Cryptography Standards #5 and Federal Information Processing Standards Publications 180-4 and 198-1 for more information.)"

[#Documentación](#)

URL de

fuelle:<https://es.community.intersystems.com/post/el-modo-de-encriptacion-pbkdf2-con-hmac-sha-512-bits-es-acorde-con-las-recomendaciones-nist>