
Question

[Mathew Lambert](#) · Jul 20, 2020

Is PBKDF2 with HMAC-SHA at 512 bits encryption, in line with NIST / FIPS recommendations?

We are using the mentioned password function and we need to know if is in line with the NIST recommendations regarding strength, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>

Reading intersystems documentation is not 100% clear for me as it states "(See RSA Laboratories Public-Key Cryptography Standards #5 and Federal Information Processing Standards Publications 180-4 and 198-1 for more information.)"

[#InterSystems IRIS](#)

Source

URL: <https://community.intersystems.com/post/pbkdf2-hmac-sha-512-bits-encryption-line-nist-fips-recommendations>