Software Assurance Tips

A product of the Software Assurance Tips Team[3]

Jon Hood

Monday 28th March, 2022

1 Ever-Changing Encryption Standards

Updated Monday 12th September, 2022

UPDATE: CNSA 2.0 information has been released, and `https://www.SwATips.com/articles/20220919.html` has been updated with the latest recommendations.

Since 2016, National Security Systems (NSS) have been required to implement the policies put forward by the Committee on National Security Systems (CNSS). CNSS Policy 15 details key sizes that are required to protect national security information.[2] To comply with CNSSP 15, system architects should use an algorithm approved in the Commercial National Security Algorithm (CNSA) suite at a key size defined by CNSSP 15. At the time of this writing, the following algorithms are permitted for encrypting data:

- AES with 256-bit keys
- RSA with at least 3072-bit modulus
- ECC with P-384

Additional requirements for key exchange and digital signatures are also provided in the policy.

Not only must the CNSSP 15 standards be implemented, but also the recommendations of NIST SP 800-57.[1] Currently, the following algorithms are allowed by SP 800-57 Part 1 Rev. 5:

- AES with 128, 192, or 256-bit key sizes
- RSA with at least 3072-bit modulus
- ECC with a range of at least 256 (i.e. P-256, P-384, and P-512)

NIST SP 800-57 further details that RSA with a 15360-bit modulus and an Elliptic Curve of at least 512 bits are required to reach the security afforded by AES-256 (the minimum AES key size allowed by CNSSP 15). While RSA15360 is permitted under CNSSP 15, P-512 is not.

For the near future, AES-256, RSA3072, and P-384 are the permitted minimum standards for cryptography. Engineers implementing RSA3072 or P-384 for their encryption should be ready to move to RSA15360 and P-512 respectively in anticipation of updated CNSS standards.

References

[1] Elaine Barker. Recommendation for Key Management. Part 1 – General. Tech. rep. Special Publication (SP) 800-57 Part 1 Revision 5. Washington, D.C.: National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.SP.800-57pt1r5. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf.

[2] Committee on National Security Systems. Use of Public Standards for Secure Information Sharing. Tech. rep. CNSSP 15. Ft. Meade, MD: NSA, 2016. URL: https://www.cnss.gov/CNSS/issuances/Policies.cfm.

[3] Jon Hood, ed. SwATips. https://www.SwATips.com/.