

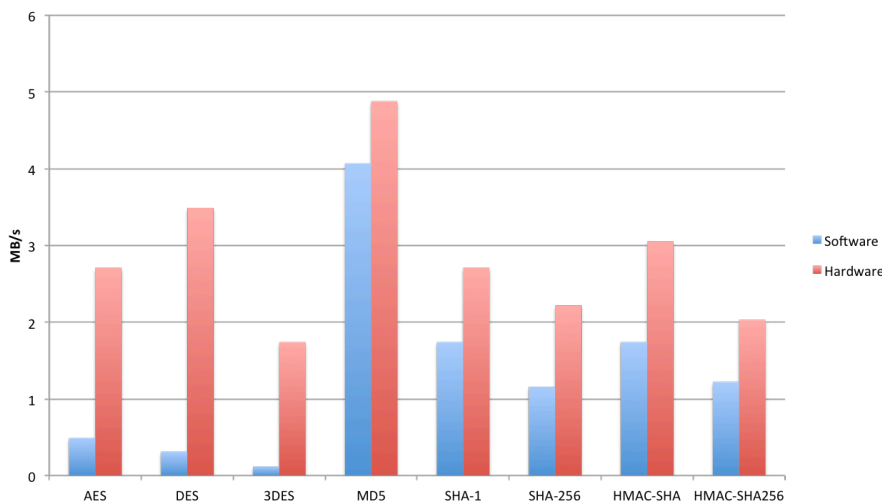


wolfSSL + NXP Kinetis

Kinetis Hardware Encryption and RNG Support

The wolfSSL embedded SSL/TLS library now has support for the CAU, mmCAU, and LTC hardware-based cryptography and random number generators offered by the NXP Kinetis processors.

NXP K60 TWR Platform (100MHz)



K60 Hardware Crypto:

- AES (CBC)
- DES (CBC)
- 3DES
- MD5
- SHA
- SHA-256



NXP Kinetis Hardware Crypto Support

Using wolfSSL with NXP Kinetis processors, applications are able to easily and seamlessly leverage the performance gain and code size reduction of NXP's mmCAU, CAU, SEC, or LTC hardware cryptography modules. In addition, wolfSSL fully supports both the NXP RNGA and RNGB hardware-based random number generators and KSDK – out of the box!

The above benchmarks were gathered from the wolfCrypt benchmark application running on the NXP Kinetis K60 processor using the mmCAU interface library.

Perfect for your Embedded Device

wolfSSL is a fully-featured, progressive, and easy-to-use SSL/TLS library perfect for resource constrained systems. With a footprint size of **20-100kB**, runtime memory usage of **1-36 kB**, and support for a large number of platforms, it is the perfect solution for securing your embedded project today.

Learn More

For more information about using wolfSSL with the Kinetis processors, please contact us at info@wolfssl.com, or visit our website www.wolfssl.com.

www.wolfssl.com

Copyright © 2017 wolfSSL Inc. All Rights Reserved