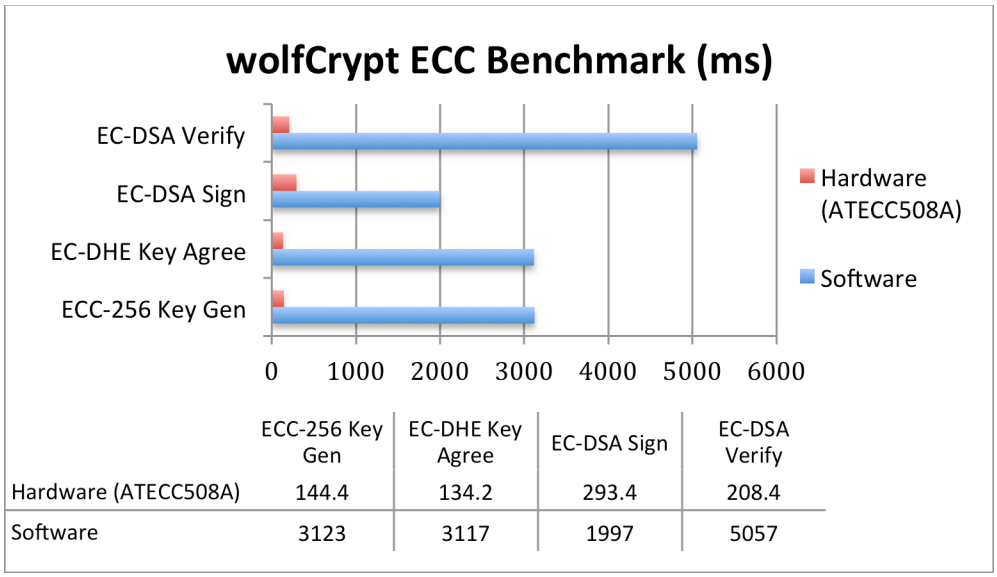
wolfSSL + Atmel

ATECC508A ECC Hardware Acceleration

The wolfSSL embedded SSL/TLS library now has support for the hardware-based ECC accelerator offered by the Atmel ATECC508A chip. The following benchmarks were gathered from the wolfCrypt benchmark application running on an ATSAMD21 Cortex-M0 at 48Mhz. This benchmark was created using the **Atmel Software Framework** and the **Atmel CryptoAuthLib**.



	ECC-256 Key Gen	EC-DHE Key Agree	EC-DSA Sign	EC-DSA Verify
Hardware (ATECC508A)	144.4	134.2	293.4	208.4
Software	3123	3117	1997	5057

ATECC508A Cryptographic Co-processor:

- ECC 256-bit
- ECDSA
- ECDH
- Secure HW Key Storage
- SHA-256 / HMAC
- RNG

ATECC508A Hardware Crypto Support

Using wolfSSL with the ATECC508A, implementations can now utilize hardware-based secure storage for private keys and authentication data and also allow resource-constrained nodes to implement full elliptic curve authentication and Diffie-Hellman key agreement and session key derivation. With the ATECC508A, TLS communications links can have hardened security even out to the smallest IoT edge node.

Applications will see substantial speed and code size improvements when using hardware accelerated cryptography versus using wolfSSL's standard software crypo implementation.

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 operating systems, it is the perfect solution for securing your embedded project today.

Learn More

For more information about using wolfSSL with the ATECC508A processor, please contact us at info@wolfssl.com, or visit our website www.wolfssl.com.