wolfSSL

Open Source Embedded Security

for Applications, Devices, IoT, and the Cloud

wolfSSL Embedded SSL/TLS Library:

- Minimum size of 20-100 kB, **perfect for secure firmware updates**
- Supports latest standards: SSL 3.0 and TLS 1.0, 1.1, 1.2, and 1.3!
- Runtime memory usage between 1-36 kB
- Stream Ciphers and DTLS (1.0, 1.2) support for **securing streaming media**
- Simple API
- Easily portable (OS, Custom I/O, Standard C library abstraction layers)
- Hardware / assembly optimizations: AES-NI, Cavium NITROX, STM32, Kinetis, PIC32MZ
- Supports most operating environments including **iOS** and **Android!**
- ECC/RSA Key Generation, X.509 v3 Signed Certificate Generation support
- Authenticated cipher suites using AES-GCM and AES-CCM-8
- Progressive cipher suites including ChaCha20 and Poly1305

wolfCrypt Embedded Crypto Engine:

- Lightweight, portable cryptography library written in C
- Portable across environments, modular in design
- Progressive algorithm and cipher support including ChaCha20, Poly1305, Ed/Curve25519
- Hardware cryptography module support
- FIPS 140-2 validated

If you have questions, or would like to set a time to speak with us in detail, email us at **info@wolfssl.com** or call +1 425-245-8247. Download evaluation copies at **wolfssl.com**.

Follow us on Twitter for security information and updates at: **http://twitter.com/wolfSSL**