wolfSSL Embedded SSL/TLS Library

Current Version: 4.0.0
Release Date: 3/21/2019

Description

The wolfSSL library is a lightweight SSL/TLS library written in ANSI C and targeted for embedded, RTOS, and resource-constrained environments - primarily because of its small size, speed, and feature set. It is commonly used in standard operating environments as well because of its royalty-free pricing and excellent cross platform support. wolfSSL supports industry standards up to the current **TLS 1.3** and **DTLS 1.2** levels, is up to *20 times smaller* than OpenSSL, and offers progressive ciphers such as ChaCha20, Curve25519, NTRU, Blake2b, and SHA-3 (Keccak). User benchmarking and feedback reports dramatically better performance when using wolfSSL over OpenSSL.

wolfSSL is powered by the wolfCrypt library. wolfCrypt is **FIPS 140-2 Level 1 validated**, with certificates **#2425** & **#3389**. For additional information, visit our FIPS FAQ page or contact **fips@wolfssl.com**.

wolfSSL is built for maximum portability, and is generally very easy to compile on new platforms. If your desired platform is not listed under the supported operating environments, please contact wolfSSL.

wolfSSL supports the C programming language as a primary interface. It also supports several other host languages, including Java (wolfSSL JNI), C# (wolfSSL C#), Python (wolfSSL Python), and PHP and Perl (through a SWIG interface). If you have interest in using wolfSSL in another programming language that it does not currently support, please contact wolfSSL at **facts@wolfssl.com**.

Features

- SSL 3.0 and TLS 1.0, 1.1, 1.2 and **TLS 1.3!** (client and server)
- DTLS 1.0 and 1.2 support (client and server)
- Minimum size of **20-100kb**
- Runtime memory usage between **1-36kb**
- FIPS Ready
- OpenSSL compatibility layer
- OCSP, OCSP Stapling, and CRL support
- Multiple Hashing Functions:
  MD2, MD4, MD5, SHA-1, SHA-2 (SHA-256, SHA-224, SHA-384, SHA-512), SHA-3 (Keccak), BLAKE2b, RIPEMD-160, Poly1305
- Block and Stream Ciphers:
  AES (CBC, CTR, GCM, CCM, GMAC, CMAC), Camellia, DES, 3DES, IDEA, ARC4, RABBIT, HC-128, ChaCha20
- Public Key Options:
  RSA, DSS, DH, EDH, ECDH-ECDSA, ECDHE-ECDSA, ECDH-RSA, ECDHE-RSA, NTRU
- Password-based Key Derivation:
  HMAC, PBKDF2, PKCS#5
- Curve25519 and Ed25519
- ECC and RSA Key Generation
- X.509v3 RSA and ECC Signed Certificate Generation
- Mutual authentication support (client/server)
- PSK (Pre-Shared Keys)
- Simple API
- Persistant session and certificate cache
- PEM and DER certificate support
- Certificate Manager
- Hardware crypto support
  Intel AES-NI, AVX1/2, RDRAND, RDSEED, SGX, Cavium NITROX, Intel QuickAssist, STM32F2/F4, NXP (CAU, mmCAU, SEC, LTC), Microchip PIC32MZ, ARMv8
- SSL Sniffer (SSL Inspection) Support
- MySQL integration
- much more...

Supported Chipmakers

wolfSSL has support for chipsets including ARM, Intel, Motorola, mbed, NXP/Freescale, Microchip/Atmel, STMicro, Analog Devices, Texas Instruments, and more.

- If you would like to use or test wolfSSL on another chipset or OS, let us know and we'll be happy to support you.

Supported Operating Environments

Win32/64, Linux, Mac OS X, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD, embedded Linux, WinCE, Haiku, OpenWRT, iPhone (iOS), Android, Nintendo Wii and Gamecube through DevKitPro, QNX, MontaVista, OpenCL, NonStop, TRON/ITRON/µITRON, Micrium's µC/OS, FreeRTOS, SafeRTOS, Freescale MQX, Nucleus, TinyOS, HP/UX, ARC MQX, TI-RTOS, uTasker, embOS, INtime, Mbed, uT-Kernel, RIOT, CMSIS-RTOS, FROSTED, Green Hills INTEGRITY, Keil RTX, TOPPERS

wolfssl.com
github.com/wolfssl