Renesas Ready Ecosystem Partner Solution

wolfSSL Embedded SSL/ TLS Library

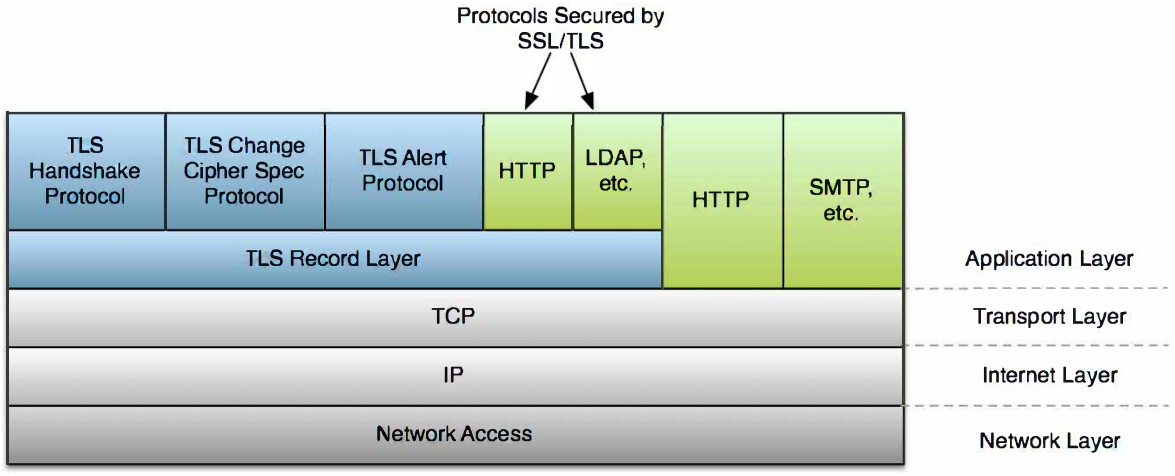
Solution Summary

The wolfSSL library, which provides network security for embedded systems and IoT devices, is lightweight and compact to meet stringent resource requirements, and is integrated to take full advantage of the hardware capabilities of MCUs and MPUs. Renesas' supported devices include the RA family, RX family and RZ/N2L.

Features/Benefits

- Support TLS 1.2, 1.3 and DTLS 1.2, 1.3
- Small footprint of 20-100 kB, varies according to build options and operating environment
- Runtime memory usage between 1-36 kB (depending on I/O buffer sizes, public key algorithm, and key size)
- Modular Design – build up to full TLS 1.3 stack or down to a single algorithm.
- Crypto Certifications to FIPS 140-2 Level 1 Certified, DO 178 DAL A, and MISRA C
- Post-Quantum Crypto Support
- Lightweight and fully featured MQTT Client with examples for AWS and Azure
- Secure Bootloader – built for safety critical applications.
- Support over 20 different operating systems including Bare-Metal.

Diagrams/Graphics



Target Markets and Applications

- Industrial/Business Equipment
- Medical
- Railroad
- Smart Home
- Avionics – Engine Controllers

wolfSSL – Embedded SSL/TLS Library

2023.12

wolfSSL Embedded SSL/TLS Library

Current Version: 5.6.3
Release Date: 06/16/2023

About Us

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 1.3** 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**

Supported Operating Environments

Win32/64, Linux, Mac OS X, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD, embedded Linux, Yocto Linus, OpenEmbedded, 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, PetaLinus, Apache Mynewt, PikeOS

Products

SSL/TLS Libraries
- **wolfSSL**

Crypto Engines
- **wolfCrypt**
- **wolfCrypt FIPS**

TPM Libraries
- **wolfTPM**

MQTT Libraries
- **wolfMQTT**

SSH Libraries
- **wolfSSH**

Secure Bootloaders
- **wolfBoot**

Data Transfer Tools
- **cURL**

Wrappers
- **wolfSSL JNI**
- **wolfCrypt JNI and JCE Provider**
- **wolfSSL C#**

Certified/Validated Products
- **wolfSSL Support for DO-178 DAL A**
- **wolfCrypt FIPS**

wolfssl.com
github.com/wolfssl