Renesas Ready Ecosystem Partner Solution

wolfBoot Secure Bootloader

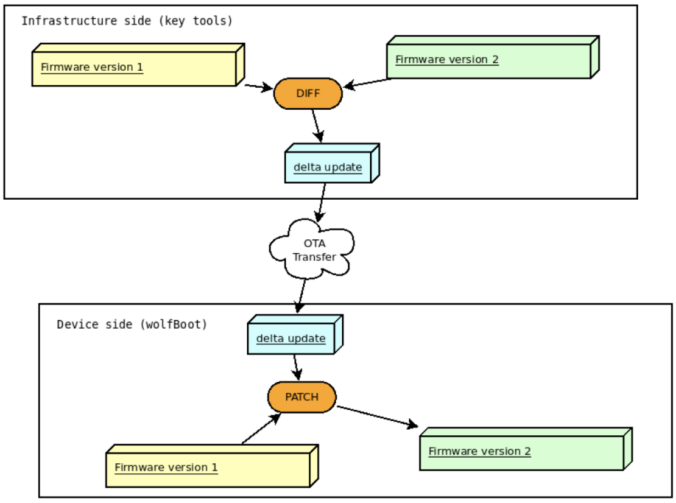
Solution Summary

wolfBoot will secure your device boot process against malicious attacks that seek to replace your firmware and take control of your device and/or steal its data. This portable secure bootloader solution offers authentication and firmware update mechanisms. With its minimalistic design and tiny HAL API, wolfBoot is completely independent from any OS or bare-metal application. wolfBoot supports Renesas RX72N, RA6M4 MCUs and RZ/N2L MPUs.

Features/Benefits

- Multi-slot partitioning of the flash device
- Integrity verification of the firmware image(s) using SHA2 or SHA3
- Authenticity verification of the firmware image(s) using wolfCrypt's digital signature algorithms
- Highly reliable, transport-agnostic firmware update mechanism
- Anti-rollback protection (via version numbering)
- Hardware-assisted dual-bank swapping
- Support for secure key storage, OTP memory, TPM 2.0

Diagrams/Graphics



Target Markets and Applications

- Smart Home, Energy, and Grid
- Industrial Automation – Controllers to Sensors

https://www.wolfssl.com/products/wolfboot/

2024.03

wolfBoot Secure Bootloader

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** and is in process of **FIPS 140-3 Level 1 validation.** 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, Azure RTOS (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