Veridify Security

RL78 Ecosystem Partner Solution

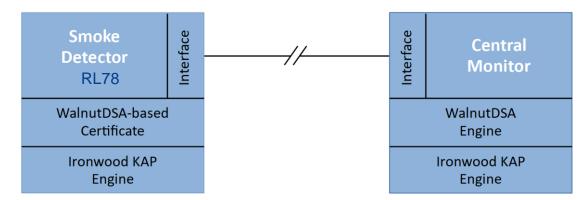# Future-Proof Security for RL78

IoT Edge Devices

Solution Summary

Veridify's security tools provide authentication and data protection solutions that are ideal for protecting connected low-resource microcontrollers like the RL78 Family MCUs. Our fast, small footprint, energy-efficient tools have a much lower RAM/ROM requirement than legacy methods, and our software-only protocols are easy and quick to implement without the hassle and cost of accelerators or additional processor support.

Features/Benefits

- Easily enables powerful security functions like secure boot and secure firmware update on RL78-based devices
- 2X faster than ECC for superior performance and lower energy consumption
- Compact and low-energy methods are ideal for the RL78 series and the low-resource IoT devices they connect to
- Quantum-resistance delivers future-proof authentication and data protection
- Available in today in software, reduces time and cost to market entry

Diagrams/Graphics

Wireless smoke, gas, and motion detectors are at risk for cyber attacks. Implementing security within the detectors enables the central monitoring station to authenticate them before acting on their messages, and to ensure that the messages they send have not been altered.

Target Applications

With Veridify's security tools, engineers can provide device-to-device authentication, identification, and data protection solutions including secure boot, secure firmware updates and command validation to ensure trusted communications between the RL78 and other Renesas MCUs.

www.veridify.com/renesas

2022.01

Fast, Small-Footprint Security for IoT Designs

Veridify Security provides fast, small footprint, low-energy, and quantum-resistant authentication and data protection solutions for 16- and 32-bit IoT endpoints like the Renesas RL78 and the RA, RX, and RE01 MCUs.

Implement a Strong Security in less than 8K of ROM

Our lightweight security tools, Walnut Digital Signature Algorithm™ (WalnutDSA™) and Ironwood Key Agreement Protocol™ (Ironwood KAP™), enable rapid and secure authentication of sensors, actuators, and other highly constrained devices.

- WalnutDSA™ - Verifies integrity and source authentication of digital data.

- Ironwood KAP™ - A Diffie-Hellman-like key agreement protocol that enables two parties to generate a shared secret over an open channel without any prior communication.

DOME Device Ownership Management and Enrollment™

DOME is a software-as-a-service that provides a cybersecurity platform that addresses security for all connected devices in a system including edge devices like the Renesas RL78. DOME enables a truly scalable solution that consolidates security functions and reduces costs and complexity for device owners.

Post-Quantum Ready

Quantum computers will become powerful enough to break popular security methods like ECC and RSA. Veridify's cryptography is resistant to all known quantum attacks making your solutions future-proof today.

ISO 26262 ASIL D Certified and PSA Certified Level 1

Our software development methods conform with the strictest requirements and are Automotive Safety Integrity Level (ASIL) D certified, the highest classification for safety-critical processes. In addition, our DOME Client recently received PSA Certified Level 1 accreditation.

Markets

- Smart Building
- Industrial/Home Automation
- Healthcare
- Metering
- Appliances
- Consumer

Applications

- Authentication
- Identification
- Data Protection

FREE Security Consultation

Our experts will provide an initial security consultation and can help accelerate time-to-market by creating a security solution design for your devices. Contact us at info@veridify.com

Request Your SDK to Get Started

Our IoT Embedded Security SDK allows easy implementation of our solutions. The toolkit includes: WalnutDSA, Ironwood KAP, sample source code and provides support for the Renesas e^2 studio.