Veridify Security

RA Ecosystem Partner Solution

Veridify's Future-Proof Security for RA2 IoT Edge Devices

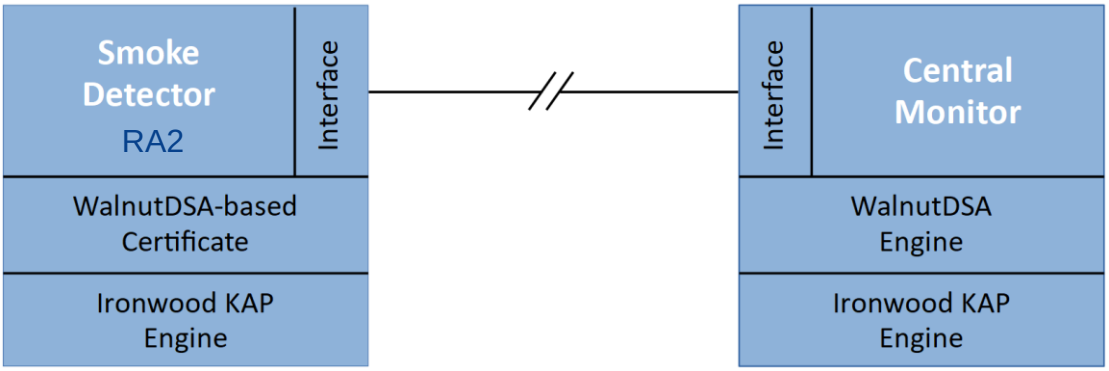
Solution Summary

Veridify Security's fast, small footprint, energy-efficient security methods are ideal for protecting RA2 devices and the low resource IoT points they connect to. Veridify's methods perform 9X faster than Elliptic Curve Cryptography (ECC).

Features/Benefits

- Easily implement secure boot, secure firmware update, remote authentication and other common security features on RA series devices
- Compact and ultra-low-energy methods are ideal for the RA series and the low-resource IoT devices they connect to
- Quantum-resistance delivers future-proof authentication and data protection
- 9X faster than ECC for superior performance and lower energy consumption
- Available in software or hardware; reduces time and cost to market entry

Sample Use Case



Wireless smoke and gas detectors are at risk for cyber attack. 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

- Secure boot
- Secure firmware update
- Remote authentication
- Identification
- Data integrity
- Data confidentiality

Award Winning Security for IoT Designs

Veridify Security (formerly SecureRF) provides fast, small footprint, ultra-low-energy, and quantum-resistant authentication and data protection solutions for 16- and 32-bit IoT endpoints like the Renesas RL78 and the new RA series.

Authenticate up to 45x Faster Than Other Methods

Our ultra-lightweight protocols, 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 provides a comprehensive device provisioning and ownership platform that simplifies security, management and provisioning of IoT devices in the field without needing a pervasive cloud or network connection. DOME enables a truly scalable platform 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

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.

Markets

- Automotive
- Consumer
- Industrial Process Controls
- Smart Building/Smart Grid
- Embedded Medical Devices
- Payments

Applications

- Authentication
- Identification
- Data Protection
- Secure Boot
- Secure Firmware Update
- Command Validation

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

Free SDK to Get Started

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

Corporate Headquarters: 100 Beard Sawmill Road, Suite 350, Shelton, Connecticut, 06484 USA
Silicon Valley Office: 75 East Santa Clara Street, San Jose, California, 95113 USA

1.888.272.1977 ● www.veridify.com/renesas