

RA Ecosystem Partner Solution

Veridify Security's DOME™ (Device Ownership Management and Enrollment™)



Solution Summary

Veridify's new DOME™ solution delivers a flexible onboarding and ownership management blockchain platform for low-resource IoT edge devices. Learn more at www.securerf.com/dome.

Features/Benefits

- Comprehensive device onboarding
- Device-level security management
- Can be implemented in software only
- One-way and mutual authentication
- Supports higher level services
- Solves the “last mile” key management problem
- Manage/upgrade firmware in edge devices
- Does not require persistent Cloud/Network connection
- Quantum-resistant to all known attacks

Diagrams/Graphics

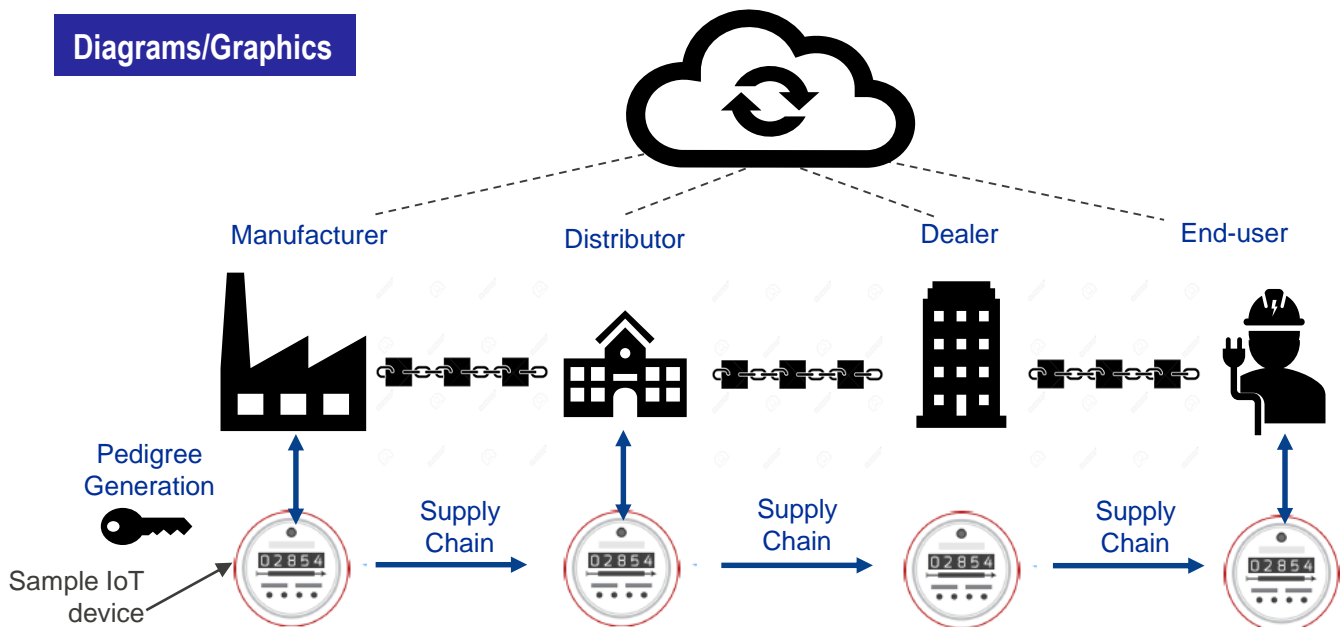


Figure: Veridify's DOME solution architecture

Target Markets and Applications

- Industrial Process Controls
- Smart Buildings
- Utilities and Smart Grid
- Embedded Medical Devices



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 MCU, CPU, ASIC, FPGA devices and the 8-, 16-, and 32-bit IoT endpoints they connect to.

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. Our 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 e² 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