Veridify Security

Company Overview

RENESAS RA READY

Authentication and Identification
for the Smallest IoT 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 low resource IoT devices.

Up to 45x Faster Than Other Methods

We provide security solutions for device-to-device communication, authentication, and identification; including secure boot and secure firmware update functions. Our methods run up to 45x faster than current solutions.

Compact Enough to Fit on the Smallest Processors

Our key agreement protocols and digital signature algorithms feature low RAM and ROM requirements and fit even the smallest 8, 16, and 32-bit processors.

Easy to Implement

While most current security technology requires costly and time-consuming hardware implementations or accelerators to achieve satisfactory execution, our methods can be deployed in software, with great performance, on a wide range of processors.

Future-Proof

Devices expected to be in the field for ten years or more will likely be vulnerable to threats from algorithms that will run on larger quantum computers. All our methods are quantum-resistant against all known attacks.

Markets and Applications

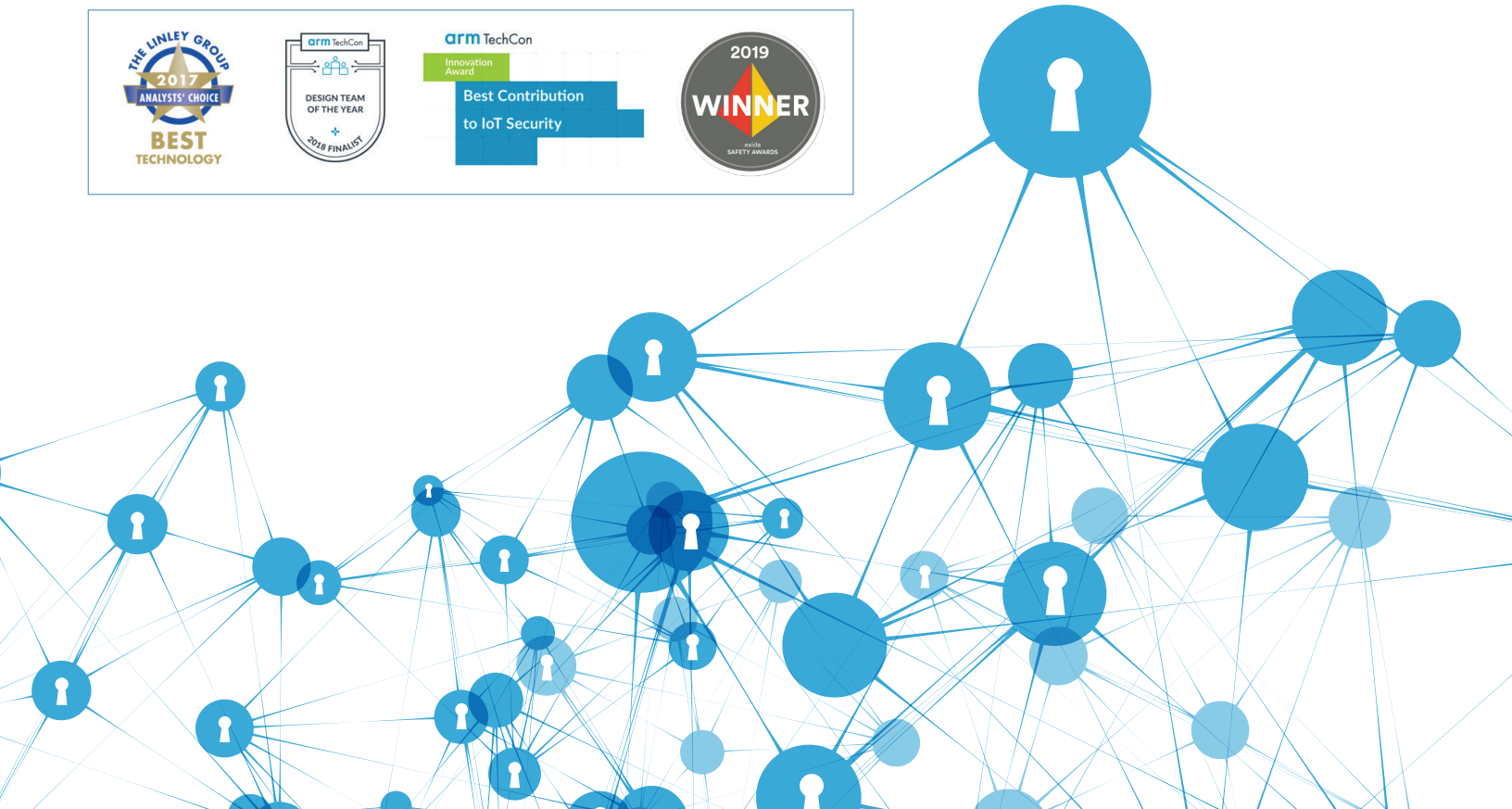
Our methods are ideally suited for a broad range of markets including IoT, smart grid, automotive, medical devices and more.

THE LINLEY GROUP 2017 ANALYSTS' CHOICE BEST TECHNOLOGY

arm TechCon DESIGN TEAM OF THE YEAR 2018 FINALIST

arm TechCon Innovation Award Best Contribution to IoT Security

2019 WINNER exida SAFETY AWARDS



Company Overview

Veridify 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™: A Device Ownership Management and Enrollment™ Platform

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

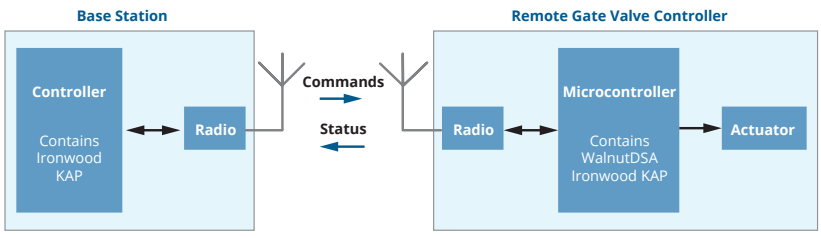
Quantum computers will become powerful enough to break popular security methods like ECC and RSA. Veridify's cryptography is resistant to all known quantum attacks making your solutions future-proof today.

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.

Example Use Case – Industrial IoT

Veridify ensures firmware on an industrial device has not been modified. Here, an MCU running Veridify methods can validate firmware that has been signed by a trusted party. Veridify enables these functions to be delivered in software, which performs faster, uses less energy and is resistant to quantum attacks.



Markets

- Automotive
- Industrial IoT
- Transportation
- Healthcare
- Energy/Smart Grid
- Payments

Applications / Security Functions

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

Faster Execution

	ARM Cortex – M23
Test Platform	EK-RA2A1
Clock Speed	48 MHz
Ironwood Runtime	**8.4 ms**
ECDH Runtime	**335 ms**
Ironwood Improvement	**40x**

Smaller Footprint

	ARM Cortex – M23
Test Platform	EK-RA2A1
Ironwood - ROM	1,883 bytes
ECDH - ROM	6,872 bytes
Ironwood Improvement	**3.6x**
Ironwood - RAM	540 bytes
ECDH - RAM	840 bytes
Ironwood Improvement	**1.5x**

RENESAS RA READY

Veridify Security

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