



Secure Thingz supports the acceleration of IoT market growth by making security easier to implement

Embedded Trust and C-Trust solutions take security implementation directly into the embedded workflow

CAMBRIDGE, UK, February 13, 2019 -- Secure Thingz, a global domain expert in device security, embedded systems, and lifecycle management, is addressing the security gap in the IoT market by making best-in-class security solutions easier to implement, starting with availability of its Embedded Trust and C-Trust software tools.

Building in security from the start of the design process is widely acknowledged as the optimal approach to tackling security challenges, and it starts with the creation of a security context that defines the application security. Embedded Trust is a security development environment, which simplifies the configuration of security, from the root of trust and key storage for a connected device to the creation of security profiles and projects. It leverages the secure hardware created by leading silicon providers, such as Microchip Technology Inc., Renesas Electronics Corporation, NXP Semiconductors N.V., and Cypress Semiconductor Corp., to provide the low-level trust anchors and secure services needed for trustworthy IoT solutions.

Implementation of good security has traditionally been a challenge as it is not a core competency of most developers. With that in mind, Secure Thingz and IAR Systems are introducing C-Trust, a new product that streamlines security implementation by making it part of a developer's existing workflow. Extending security implementation from Embedded Trust to every application developer, C-Trust is offered as an extension to the industry-leading embedded development toolchain IAR Embedded Workbench. The integration enables designers to include security development as part of their day-to-day development workflow and more easily implement "security from inception" into their IoT device design.

"More and more companies are recognizing that the continued growth and success of the IoT market is predicated on a need for increased, scalable security," said Haydn Povey, founder and CEO of Secure Thingz. "With Embedded Trust, we are providing a state-of-the-art security solution, then making it easier for developers to implement through C-Trust. Leveraging the expertise of Secure Thingz, IAR Systems and leading semiconductor companies, we are building a secure and sustainable future for connected devices, and transforming an entire industry."

Currently, a lack of strong security is seen as inhibiting broader proliferation and adoption of IoT devices. According to ABI Research, by 2022, an estimated 70 percent of the world's 57 billion connected devices will be targeted for the IoT, yet today, less than four percent of new devices have embedded security. Furthermore, the huge lack of availability of software developers with cybersecurity skills continue to limit the availability of solutions, better tools and infrastructure for the engineering majority to leverage.

To address these next-generation security requirements, Embedded Trust delivers a set of security features and capabilities at the inception of the project, including:

- Secure device support leveraging hardware trust anchors
- Integrated identity, ownership and certificate management



- Scalable Secure Boot Manager enabling secure lifecycle management
- Secure deployment with integrated manufacturing mastering
- Release management with versioning and update infrastructure

Embedded Trust enables companies to define how their certificate hierarchies will span across multiple product ranges, while enabling the creation of a product device framework that can be dynamically resolved and injected at manufacturing time. It enables customization of a Secure Boot Manager to achieve the level of security suitable necessary for all kind of device applications.

C-Trust enables application developers to deliver code that is secured and encrypted. The broad development team leverages C-Trust to easily import the organization's security configuration profile, without potentially compromising it.

By enabling security implementation into the workflow and supporting the hardware of various semiconductor providers, the Secure Thingz solutions gives choice to the device companies and their developers to define the security that is best suited for their intended application. This approach will lead to a more secure IoT.

“With the rapid proliferation of IoT nodes, the pressure on time to market leaves customers limited opportunity to sufficiently explore their options for security,” said Rod Drake, vice president of Microchip's MCU32 business unit. “Microchip recognizes customers have scalable requirements when it comes to securing applications, and we are working with them to integrate security early in the design cycle. Our partnership with Secure Thingz eases and expedites the security design process for customers.”

“Security is the biggest design challenge facing our customers today. Designing a reliable and secure complex embedded system brings many challenges, and companies will increasingly need to make security a foundation of their product and design philosophy,” said Daryl Khoo, vice president of Product Marketing, IoT Platform Business Division, Renesas Electronics Corporation. “The Renesas and Secure Thingz partnership actually starts with having robust, safe and secure MCUs from Renesas, along with Secure Thingz solutions to help our customers accelerate IoT growth by enabling collaboration across the supply chain for easier delivery and implementation of secure, embedded applications through an end-to-end solution.”

“The internet is changing the way we interact with devices, and NXP wants to ensure our customers are prepared with everything they need to develop smart, connected and secure things for the IoT,” said Joe Yu, vice president and general manager, Low-power MPU and MCU product lines at NXP. “NXP's end-to-end portfolio, insight and partner ecosystem empower our customers to design cutting-edge solutions. NXP is committed to enabling secure connections for a smart world, and we are pleased to work with Secure Thingz to make security easier to implement.”

Getting Started/Availability

Embedded Trust and C-Trust for IAR Embedded Workbench are shipping worldwide this month. To get a quote, please visit <https://www.iar.com/buy/>. The products will be showcased at the IAR Systems booth (4-216) and at the Secure Thingz booth (4A-104) at embedded world 2019 in Nuremberg, Germany on February 26-28.



About Secure Thingz

Secure Thingz, Inc. is the global domain expert in device security, embedded systems, and lifecycle management. In 2018, the company was acquired by [IAR Systems Group AB](#), the future-proof supplier of software tools and services for embedded development. Secure Thingz is focused on delivering advanced security solutions into the emerging industrial Internet of Things, critical infrastructure, automotive and other markets. The Secure Deploy™ architecture has been developed to solve the major security issues challenging the IoT. Secure Thingz solutions ensure a cost-efficient root of trust in low-cost microcontrollers to deliver a core set of critical services through the product lifecycle, alongside secure deployment, production and update infrastructure. Secure Thingz is a founding member and Executive Board member of the Internet of Things Security Foundation (www.ietfsecurityfoundation.org), the leading global organization for IoT Security.

Media Contact:

Tiffany Sparks
Secure Thingz
tiffany.sparks@securethingz.com
+1 (408) 858 1892