Product News

Date: February 24, 2021

Secure Thingz announces significant enhancements to protect critical IoT assets and aid companies in achieving legislative compliance

In collaboration with Renesas, and in support of the 10th Anniversary of the Renesas RX family, Secure Thingz proudly announces support of Renesas Trusted Secure IP (TSIP) technology in Embedded Trust and Secure Deploy

Cambridge, United Kingdom / Uppsala, Sweden—February 24, 2021—Secure Thingz, an IAR Systems® Group company, announced enhancements to the secure development tool Embedded Trust and the secure prototyping and production platform Secure Deploy, delivering enhanced protection of critical security assets during development, provisioning, and in-service as the foundation of a secure electronics supply chain.

The need for protection of security assets is widely accepted by the consumer and industrial IoT markets as a fundamental part of a “whole-product” security strategy and form a baseline across the European EN 303645 standards, and the recent US Cybersecurity Improvement Act. The assets are used in the creation and implementation of unique identities and ensure the integrity of the product both at the point of manufacture and later whilst in service in the end user’s systems. Critically many organizations also seek to protect their investment in intellectual property (IP) through tight control of provisioning credentials, both to control production quantities and preventing cloning. The updated solutions announced today further secure these credentials within secure enclaves, or vaults, inside of the microcontrollers, ensuring the highest level of security the devices can achieve, without escalating cost or complexity.

Renesas, a leading supplier of advanced semiconductor solutions, has a strong track record of providing advanced security solutions in the RX Family of 32-bit MCUs. A cornerstone of the Renesas security offering is the Trusted Secure IP (TSIP & TSIP-Lite) block included in many RX Family devices. The TSIP offers multiple security features including robust key management, highly secured on-device storage, encryption/decryption, and a wide array of integrated countermeasures. Importantly, the TSIP contents cannot be accessed from elsewhere within the device, so key data and the cryptographic engine are strongly protected.

– more –

“With the number of connected devices continuing to rise, Renesas recognizes the growing need of embedded security throughout the development and production cycle; most of our customers are faced with challenges to realize robust security in their systems,” said Daryl Khoo, Vice President, Marketing, IoT Platform Business Division at Renesas. “We have been collaborating with IAR Systems and Secure Thingz to strengthen security features in IoT devices by ensuring secure development flows and enabling global secure provisioning services. With the Embedded Trust and Secure Deploy now supporting RX MCU’s TSIP, we are poised to deliver enhanced protection of critical assets for any IoT product development and production, which eases and expedites the security design process for our customers.”

Secure Thingz delivers a comprehensive secure supply chain solution through the Embedded Trust and C-Trust security development tools, and the Secure Deploy secure prototyping and production platform. A critical component of a security development workflow is the generation and installation of a vendor-specific Secure Boot Manager (SBM), which is installed in the product as part of a robust Root of Trust. Announced today with the releases of Embedded Trust v1.52 and Secure Deploy v3.22, the Root of Trust and assets managed by the SBM are encrypted during provisioning and stored securely with Renesas TSIP enclave. This process prevents application code or malware from accessing, modifying or impinging the Root of Trust or assets. Furthermore, the process is uniquely tied to the device ensuring that it is not possible to intercept the production to clone or counterfeit devices.

“The recent US Cybersecurity Improvement Act, alongside the European EN 303645 standards, highlight the need for both unique device management, updates, and secure supply chains”, said Haydn Povey, CEO of Secure Thingz. “Through our cooperation with Renesas we are now bringing the strongest device security within the reach of every embedded developer and every application, substantially reducing the device attack surface and ensuring OEMs and end users are protected with best-in-class security.”

Learn more about why and how to protect stored data in the MCU or application in the whitepaper Securing your IP and Protecting Sensitive Data (Renesas, 2020).

More information about IAR Systems’ security offering is available at www.iar.com/security.

Ends

IAR Systems/Secure Thingz Contacts

AnnaMaria Tahlén, Content & Media Relations Manager, IAR Systems
Tel: +46 18 16 78 00 Email: annamaria.tahlen@iar.com

Tora Fridholm, Chief Marketing Officer, IAR Systems
Tel: +46 18 16 78 00 Email: tora.fridholm@iar.com

About IAR Systems

IAR Systems supplies future-proof software tools and services for embedded development, enabling companies worldwide to create the products of today and the innovations of tomorrow. Since 1983, IAR Systems' solutions have ensured quality, reliability, and efficiency in the development of over one million embedded applications. The company is headquartered in Uppsala, Sweden and has sales and support offices all over the world. Since 2018, Secure Thingz, the global domain expert in device security, embedded systems, and lifecycle management, is part of IAR Systems Group AB. IAR Systems Group AB is listed on NASDAQ OMX Stockholm, Mid Cap. Learn more at www.iar.com.

About Secure Thingz

Secure Thingz 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.iotsecurityfoundation.org), the leading global organization for IoT Security.