Product News

Date: May 18, 2021

Secure Thingz collaborates with NXP Semiconductors to enable enhanced protection of connected devices

The unique security tools from IAR Systems and Secure Thingz combined with Physical Unclonable Function (PUF) technology from NXP® offer strong IoT security implementation through combination of hardware and software-based protection

Cambridge, United Kingdom—May 18, 2021—Secure Thingz, an IAR Systems® Group company, announced enhancements to the secure development tools C-Trust® and Embedded Trust®, as well as the secure prototyping and production platform Secure Deploy, delivering enhanced protection of applications based on the NXP LPC55S6x MCU family featuring Physical Unclonable Function (PUF) technology for secure storage.

Security credentials and the implementation of unique identities are vital in ensuring the integrity of a device and form a vital part of the European Consumer IoT Security Standard EN 303 645, as well as the recent US Cybersecurity Improvement Act, which defines a minimal level of security for use of products within USA Government departments. The use of unique securely managed identities also enables organizations to protect their investment in intellectual property (IP) through tight control of provisioning credentials, both to control production quantities and prevent cloning.

Secure Thingz delivers a comprehensive secure supply chain solution through the security development tools Embedded Trust and C-Trust, which are completely integrated with the development toolchain IAR Embedded Workbench®, and the secure prototyping and production platform Secure Deploy. The Root of Trust and assets managed by Secure Thingz solutions for the LPC55S6x MCU family are encrypted during provisioning using the PUF as a key vault, which is used to protect secret credentials and keys. This process helps prevent application code or malware from accessing, modifying or impinging on the Root of Trust or assets. Furthermore, the process is uniquely tied to the device offering protection against cloning or counterfeiting.

"NXP has long recognized the increasing need of embedded security throughout the development and production cycle," said Cristiano Castello, Sr. Director Product Innovation for MCUs, NXP

– more –

Semiconductors. "Through our ongoing collaboration with IAR Systems and Secure Thingz, we continue to work together to address the security challenges our customers face by enabling global secure provisioning services."

"The need for unique device management, updates, and secure supply chains have been highlighted by the recent US Cybersecurity Improvement Act, alongside the EN 303 645 standard", said Haydn Povey, CEO, Secure Thingz. "Through our longstanding relationship with NXP, we are making the security implementation easier for every embedded developer and every application by utilizing even more of the secure capabilities offered in the NXP LPC55S6x MCU family. This capability, integrated into Embedded Trust and C-Trust, supports our focus on enabling customers to achieve and exceed the emerging standards."

In NXP's whitepaper Extend MCU Security Capabilities Beyond Trusted Execution, there is more information about NXP's approach to crypto acceleration and asset protection that help bring high levels of security to low-cost microcontrollers with minimal power and area penalty.

IAR Systems is a platinum member of the NXP Partner Program, a global network of engineering companies collaborating with NXP to bring exceptional software, tools, training and services, and ultimately speed time to market. More information about Secure Thingz and IAR Systems' security offering is available at www.iar.com/security.

Ends

IAR Systems/Secure Thingz Contacts

AnnaMaria Tahlén, Media Relations & Content 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.