Secure Thingz and Intrinsic ID partner to ensure supply chains of trust for the embedded industry

Partnership to enable rapid development, implementation, and provisioning of unique and secure identity for IoT applications

Cambridge, United Kingdom and Sunnyvale, California—December 15, 2021—Secure Thingz, an IAR Systems® Group company delivering advanced development and provisioning platforms to secure the IoT, today announced their partnership with Intrinsic ID, the leading provider of Physical Unclonable Function (PUF) security IP. By working together, the companies intend to provide strong integration of Intrinsic ID's physical unclonable functions (PUF) within Secure Thingz development and provisioning solutions.

Establishing a supply chain of trust has never been more important as products and devices share sensitive information and provide vital services. With this partnership, companies will be able to develop products with unique identities and integrated confidentiality. This can then be carried through the entire development, manufacturing, and lifetime of a product through a secure microcontroller execution environment and an immutable boot path to a root of trust boot manager that verifies subsequent software before execution.

"Physical unclonable functions are vital components in many modern devices, with leading vendors integrating them into their microcontroller offerings for IoT security," stated Haydn Povey, CEO, Secure Thingz. "Together with Intrinsic ID, we will enable this critical capability to be integrated into a wide array of embedded systems to deliver protection of provisioned data, together with the creation of root keys."

"We believe PUF technology is fundamental for the security of embedded applications in the IoT environment," said Pim Tuyls, CEO, Intrinsic ID. "Secure Thingz is a key player in delivering solutions to secure the IoT and this partnership will enable and support an accelerated adoption of PUF technology, providing a key differentiator for delivering chain-of-trust implementation across the embedded marketplace."

– more –

By using Secure Thingz' security solutions, companies can implement a robust root of trust as part of the development process and extended into programming and provisioning, supporting the use of PUF technology in volume programming and provisioning services across the world.

More information is available at www.securethingz.com

Ends

Editor's Note: IAR Systems, IAR Embedded Workbench, Embedded Trust, C-Trust, C-SPY, C-RUN, C-STAT, IAR Visual State, IAR KickStart Kit, I-jet, I-jet Trace, I-scope, IAR Academy, IAR, and the logotype of IAR Systems are trademarks or registered trademarks owned by IAR Systems AB. All other product names are trademarks of their respective owners.

Secure Thingz/IAR Systems 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 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 world-leading provider of software tools and services for embedded development. Secure Thingz is focused on delivering advanced security solutions into the industrial Internet of Things, critical infrastructure, automotive and other markets. The company 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.

About Intrinsic ID

Intrinsic ID is the world's leading provider of security IP for embedded systems based on physical unclonable function or PUF technology. The technology provides an additional level of hardware security utilizing the inherent uniqueness in each and every silicon chip. The IP can be delivered in hardware or software and can be applied easily to almost any chip – from tiny microcontrollers to high-performance FPGAs – and at any stage of a product's lifecycle. It is used as a hardware root of trust to validate payment systems, secure connectivity, authenticate sensors, and protect sensitive government and military data and systems. Intrinsic ID security has been validated for NIST CAVP and deployed and proven in millions of devices certified by EMVCo, Visa, CC EAL6+, PSA, IoXt, and governments across the globe. www.intrinsic-id.com