Secure Thingz contributes to Arm Platform Security Architecture portfolio with enhanced device security

Adding Secure Production to the Platform Security Architecture (PSA) portfolio

Cambridge, England, October 7, 2019 – Secure Thingz, a global domain expert in device security, embedded systems, and lifecycle management, is helping broaden the Platform Security Architecture (PSA) documentation. The new family of documentation, which has a working name of ‘PSA for Secure Production’, includes a Secure Production Threat Model and Security Analysis (TMSA) document, as well as a future specification, looking at the need to implement security integrated within silicon to protect intellectual property (IP) and protect revenue streams within the Internet of Things (IoT) supply chain.

With growing connectivity in almost every industry sector, from industrial automation and critical infrastructure to smart cities and smart consumer products, the potential risks of cyberattack and hacking increase unless protection is built into the system’s foundations. The impact of poor security is manifested at many levels. A hardware-based security mechanism is essential to protect intellectual property and revenue streams. PSA is a framework for designing more secure connected devices building upon security best practice from across the industry. It is aimed at different entities throughout the supply chain and includes a set of deliverables, including Threat Models and Security Analyses documentation, hardware and firmware architecture specifications, Trusted Firmware, plus APIs and an API test suite. This is all alongside PSA Certified™, which is an independent security evaluation and certification scheme. A Secure Production Threat Model identifies the assets to be protected, threats against these assets, along with the subsequent security objectives and requirements to mitigate against the identified threats.

“At Secure Thingz, we help our customers to ensure security and protect their IP through their supply chain and whole IoT device lifecycle. Arm provides the necessary hardware security foundation to offer our customers the means to secure their supply chain and valuable IP. Now we are working together to broaden the PSA family of specifications with security aspects related to the whole IoT supply chain,” commented Haydn Povey, CEO and Founder, Secure Thingz.

“As connected devices become more intelligent, we are constantly looking at ways to reinforce device security and expand the PSA framework,” said Andy Rose, chief system architect and fellow at Arm. “The new documentation from Secure Thingz will build on the available practical security implementation guides and open source trusted firmware, helping simplify the creation of more secure IoT devices.”

More information about Secure Thingz and IoT security is available at www.securethingz.com.

### Ends

– more –
Secure Thingz Contacts
Tora Fridholm, Chief Marketing Officer
Tel: +46 18 16 78 00
Email: tora.fridholm@iar.com

Haydn Povey, CEO and Founder
Email: haydn.povey@securethingz.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.