IAR Systems updates security products for simplified protection against cloning and overproduction

Stockholm, Sweden—February 20, 2020—IAR Systems, the future-proof supplier of software tools and services for embedded development, announces version 1.40 of the security development tool C-Trust, further simplifying the implementation of security features into the development workflow. New device support includes mainstream devices as well as Arm® TrustZone® for Arm Cortex®-M devices from STMicroelectronics and NXP.

As embedded applications require additional security and companies try to meet the ongoing changes in IoT device legislations, there is a growing need to both protect the Intellectual Property (IP) and to ensure that product integrity is not compromised by counterfeiting and cloning during production. C-Trust works as an extension to the development toolchain IAR Embedded Workbench® and enables developers to easily build security into their applications, without having to master the deeper complexities of security, through the use of innovative Security Context Profiles. In addition to ready-made Security Context Profiles for IP protection, version 1.40 of C-Trust adds Security Context Profiles for production control. This new feature empowers developers to pre-define how many end products can be provisioned during production, preventing damaging cloning and counterfeiting.

"Our customers are telling us they are ready to start their transition into developing with security," says Stefan Skarin, CEO and President, IAR Systems. "Security is their top priority, but there is also a frustration over the complexity of trying to implement security features. By providing integrated, simplified security development workflows with extended device support, we enable them to get started immediately, and reach a level of security that is sufficient as a starting point."

C-Trust delivers ground-breaking security across the supply chain when coupled with the new Secure Desktop Provisioner by Secure Thingz, also announced today. Additionally, in the fast changing IoT market, there is a wide array of emerging security technologies in semiconductor devices. These technologies range from physical protection mechanisms in next generation devices, through to hardware memory enforcement techniques, plus the ability to design and deploy devices with keys and other secrets securely provisioned.

– more –

"Implementing security in advanced embedded devices is critical in meeting upcoming legislative requirements", said Haydn Povey, CEO Secure Thingz. "The newly supported Arm TrustZone devices, coupled with our security tools, enable developers to rapidly deliver advanced applications with security from inception, providing the robustness and availability end users demand, and providing a secure foundation for the future of IoT."

Ends

Editor's Note: *IAR Systems, IAR Embedded Workbench, Embedded Trust, C-Trust, IAR Connect, 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.*

IAR Systems Contacts

Josefin Skarin, Investor Relations, IAR Systems Group AB
Email: josefin.skarin@iar.com

Stefan Skarin, CEO and President, IAR Systems Group AB
Email: stefan.skarin@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, a provider of advanced security solutions for embedded systems in the IoT, is part of IAR Systems. IAR Systems Group AB is listed on NASDAQ OMX Stockholm, Mid Cap. Learn more at www.iar.com.