Product News

Date: April 1, 2020

IAR Systems enables secure applications based on NXP's LPC55S6x Arm Cortex-M33 MCUs

The security development tool C-Trust, an extension to the complete development toolchain IAR Embedded Workbench, now supports LPC55S6x MCUs from NXP

Uppsala, Sweden—April 1, 2020—IAR Systems, the future-proof supplier of software tools and services for embedded development, announces support in its security tool C-Trust® for the Arm® Cortex®-M33 based LPC55S6x MCUs from NXP® Semiconductors, which will assist companies in easing the implementation of security in their applications.

NXP's LPC55S6x MCUs are dual-core Arm Cortex-M33 MCUs, which leverage the Armv8-M architecture to introduce new levels of performance and advanced security capabilities. One of the cores includes Arm TrustZone® technology and a memory protection Unit. The MCU is equipped with crypto accelerators for symmetric and asymmetric cryptography and a PUF (Physically Unclonable Function) to fight cloning and counterfeiting. It has a True Random Number Generator (TRNG), a Unique Device Identifier, Secure GPIOs, secure authenticate debug capabilities, a secure boot with root-of-trust keys and anti-rollback protection, real-time PRINCE encryption/decryption of the on-chip flash and it supports the Device Identification Composition Engine (DICE) as specified by the TCG (Trusted Computing Group).

C-Trust is as an extension of the complete development toolchain IAR Embedded Workbench® for Arm and enables developers to easily protect an existing or new application, and ease mastering the deeper complexities of security, through the use of Security Context Profiles. These Security Context Profiles are developed by Secure Thingz, a global domain expert in device security, and include all the necessary security and encryption settings, such as cryptographic keys and certificates, Secure Boot Manager

– more –

configuration, access to platform security features, application update process and policy, and device memory layout. C-Trust provides the application with a robust protection against Intellectual Property (IP) theft, malware injection, counterfeiting and overproduction. This technology takes advantage of the hardware security features of Arm TrustZone technology to protect both the included Secure Boot Manager and the cryptographic keys needed to protect software IP.

To further help companies in building the right level of security for their needs, IAR Systems and Secure Thingz offer the Security from Inception Suite which is a unique set of tools and services for implementing and customizing security in embedded applications. To enable secure transferring of designs into production in an easy way, the Security from Inception Suite includes Secure Desktop Provisioner. Together with C-Trust, Secure Desktop Provisioner delivers ground-breaking improvements on the ease of implementation of security across the supply chain. The entire offering supports many mainstream devices as well as devices secured by Arm TrustZone technology, such as the NXP LPC55S6x MCUs.

“The support of NXP’s LPC55S6x Arm Cortex-M33 MCUs in our security offering adds extended possibilities for the joint customers of IAR Systems and NXP,” said Clive Watts, Security Products Manager at Secure Thingz/IAR Systems. “With the right tools, you can translate your security design in a reliable implementation leveraging the right security features of the selected MCUs, and we will continue to leverage our strong industry relationships to expand our device support and help organizations both in creating new secure applications easier as well as implementing security in existing applications.”

“The support of NXP’s Arm Cortex-M33 based LPC55S6x MCUs paired with IAR Systems’ security solutions helps developers bring secure applications to market quickly,” said Brendon Slade, director MCU ecosystem at NXP Semiconductors. “We are pleased to work with IAR Systems and Secure Thingz to improve the ease of use of underlying security features for secure industrial and IoT solutions.”

“As we head towards a world of a trillion connected devices, security must be a fundamental part of embedded design,” said Thomas Ensergueix, senior director, Automotive and IoT Line of Business at Arm. “We are working closely with our partners to ensure security is built in from the ground up, and NXP’s LPC55S6x family based on Cortex-M33, combined with security development tools from IAR Systems, will enable companies to create secure IoT applications with new levels of performance.”

More information about IAR Systems’ complete security offering, as well as details about the security tool C-Trust, is available at www.iar.com/security.

### 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

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.