June 5, 2018

Simplify the Development of Secure Connected Nodes Using Cryptography-Enabled Microcontroller with DICE Architecture

Easily create secure connected devices with new development kit for Microsoft Azure

CHANDLER, Ariz., June 05, 2018 (GLOBE NEWSWIRE) -- As the Internet of Things (IoT) accelerates and internet connectivity is deployed into virtually every industrial segment, security threats are escalating in quantity and scale. These threats can ruin the reputation of those attacked, impact company financials and allow intellectual property to be stolen or destroyed. While cryptography can be used to secure these connected nodes and the basis of the practice is understood, designers often do not know how to approach the implementation of such security. Microchip Technology Inc. (NASDAQ: MCHP) today announced that its CEC1702 hardware cryptography-enabled microcontroller (MCU) now supports the Device Identity Composition Engine (DICE) security standard, providing a simple way to add fundamental security to embedded products. A new **CEC1702 IoT development kit** for Microsoft Azure IoT is also available, offering designers everything needed to easily incorporate the DICE security standard in their products.

Hackers have become increasingly sophisticated, making it imperative that system designers apply sound security principles in the development of their product. Developed and backed by industry experts from the Trusted Computing Group (TCG), **DICE** is a simple and reliable method that can be implemented in the hardware of security products during manufacturing. The architecture breaks up the boot process into layers and creates unique secrets along with a measure of integrity for each layer, automatically re-keying and protecting secrets if malware is present. One of the key benefits of using the secure boot features of the CEC1702 with the DICE standard is that it enables equipment manufacturers to create a chain of trust for multiple loads of firmware, which is especially important for customers concerned with authenticating system-critical commands, such as in applications like power plants or online server databases.

“Designing and deploying secure devices remains a significant challenge for developers,” said Ian Harris, vice president of Microchip’s computing products group. “Implementing security with DICE gives designers confidence that the fundamental security of their device is based on principles that were developed and reviewed by industry experts. Combined with the DICE architecture, the full-featured CEC1702 provides an easy way to add the crucial security and privacy features required by embedded systems.”

Time and ease of use are top considerations for designers developing cloud-connected solutions. The CEC1702 IoT development kit with the DICE architecture helps designers speed up development cycles. The kit comes with a powerful, programmable 32-bit

ARM® Cortex®-M4 microcontroller and sample code to quickly develop a secure, cloud-connected solution. Certified by Microsoft Azure, customers can develop their product with the confidence that the necessary components to connect to the internet have been vetted and certified.

"As the IoT landscape continues to increase with security threats, customers can turn to Microchip's IoT development kit to quickly and easily connect devices to the cloud and incorporate DICE security standards in their product," said Sam George, director, Microsoft Azure IoT at Microsoft Corp. "The development kit enables customers to implement the DICE standard into a device's hardware while also benefitting from Microsoft Azure's security and privacy features."

Development Tools
Microchip simplifies adding authentication and encryption to connected devices with the CEC1702 IoT development kit. Key features of the kit include:

- CEC1x02 development board with a Plug-in Module (PIM) that contains the CEC1702 with integrated cryptography accelerators, saving code space and decreasing time to market
- Two headers compatible with MikroElektronika's extensive library of click boards™, allowing for flexible design requirements
- MikroElektronika Wi-Fi® 7 click board, equipped with Microchip's ATWINC1510-MR210PB IEEE 802.11 b/g/n module, optimized for low-power IoT applications
- MikroElektronika THERMO 5 click board, which can measure temperatures across four channels with ranges from 0 to 127 degrees Celsius and extended range of -64 to 191 degrees Celsius

Pricing and Availability
The CEC1702Q-B2-I/SX is available in production volume for $3.14 each in 5,000-unit quantities. The CEC1702 IoT development kit (DM990013-BNDL) is available for $199.99.

For additional information, contact any Microchip sales representative or authorized worldwide distributor, or visit Microchip's website. To purchase products mentioned in this press release, go to Microchip's full-service channel **microchipDIRECT** or contact one of Microchip's authorized distribution partners.

Resources
High-res images available through Flickr or editorial contact (feel free to publish):

- Application image: **https://www.flickr.com/photos/microchiptechnology/28562428548**
- Chip shot: **https://www.flickr.com/photos/microchiptechnology/28562428398**

About Microchip Technology
Microchip Technology Inc. (NASDAQ: MCHP) is a leading provider of microcontroller, mixed-signal, analog and Flash-IP solutions, providing low-risk product development, lower total system cost and faster time to market for thousands of diverse customer applications worldwide. Headquartered in Chandler, Arizona, Microchip offers outstanding technical support along with dependable delivery and quality. For more information, visit the Microchip website at **www.microchip.com**.

Editorial Contact:
Christie Haber
480-792-4386
christie.haber@microchip.com

Reader Inquiries:
1-888-624-7435

Source: Microchip Technology Inc