November 20, 2017

Protect IP and Deploy Secured Connected Systems with Microchip's New CryptoAuthentication™ Device and Security Design Partner Program

The ATECC608A secure element and new Security Design Partner Program provide the parts and partners needed for designing secure solutions

CHANDLER, Ariz., Nov. 20, 2017 (GLOBE NEWSWIRE) -- From remote cyber-attacks to the creation of counterfeit products, security threats are wide-spread and affect all industries. When carried out, these threats can translate into substantial losses in service revenue, recovery costs and, perhaps most significantly, in brand equity. Implementing robust security into new and existing designs to protect Intellectual Property (IP) and enable trusted authentication of connected devices is critical. To protect against these threats, Microchip Technology Inc. (NASDAQ:MCHP) has created the ATECC608A CryptoAuthentication™ device, a secure element that allows developers to add hardware-based security to their designs. Microchip has also established a Security Design Partner Program for connecting developers with third-party partners that can enhance and expedite secure designs. For more information on Microchip's latest security solutions, visit: **http://www.microchip.com/design-centers/security-ics/cryptoauthentication/overview**

The foundation of secured communication is the ability to create, protect and authenticate a device's unique and trusted identity. By keeping a device's private keys isolated from the system in a secured area, coupled with its industry-leading cryptography practices, the ATECC608A provides a high level of security that can be used in nearly any type of design. Primary features of the ATECC608A include:

- **Best-in-class key generation**: The Federal Information Processing Standard (FIPS)-compliant Random Number Generator (RNG) generates unique keys that comply with the latest requirements from the National Institute of Standards and Technology (NIST), providing an easier path to a whole-system FIPS certification.
- **Boot validation capabilities for small systems**: New commands facilitate the signature validation and digest computation of the host microcontroller (MCU) firmware for systems with small MCUs, such as an ARM® Cortex®-M0+ based device, as well as for more robust embedded systems.
- **Trusted authentication for LoRa nodes**: The AES-128 engine also makes security deployments for LoRa infrastructures possible by enabling authentication of trusted nodes within a network.
- **Fast cryptography processing:** The hardware-based integrated Elliptical Curve Cryptography (ECC) algorithms create smaller keys and establish a certificate-based

root of trust more quickly and securely than other implementation approaches that rely on legacy methods.
- **Tamper-resistant protections**: Anti-tampering techniques protect keys from physical attacks and attempted intrusions after deployment. These techniques allow the system to preserve a secured and trusted identity.
- **Trusted in-manufacturing provisioning**: Companies can use Microchip's secured manufacturing facilities to safely provision their keys and certificates, eliminating the risk of exposure during manufacturing.

"Security is essential for today's connected applications, especially for those spanning from hardware to the cloud," said Nuri Dagdeviren, vice president of Microchip's Secure Products Group. "This is why Microchip offers both proven hardware security solutions and an unprecedented level of partnership with leading cloud providers, giving our customers all the building blocks to create secure solutions that protect their IP, brand value and revenue streams."

In addition to providing hardware security solutions, customers have access to Microchip's **Security Design Partner Program**. These industry-leading companies, including Amazon Web Services (AWS) and Google Cloud Platform, provide complementary cloud-driven security models and infrastructure. Other partners are well-versed in implementing Microchip's security devices and libraries. Whether designers are looking to secure an Internet of Things (IoT) application or add authentication capabilities for consumables, such as cartridges or accessories, the expertise of the Security Design Partners can reduce both development cost and time to market.

"The work done on the ATECC608A chip through our collaboration with Microchip enables Google IoT customers to get a new offering that provides high levels of security with a seamless onboarding experience," said Antony Passemard, Product Management Lead for Google Cloud IoT.

Development Tools
For rapid prototyping of secure solutions, designers can use the new CryptoAuth Xplained Pro evaluation and development kit (ATCryptoAuth-XPRO-B) which is an add-on board, compatible with any Microchip Xplained or Xplained Pro evaluation boards.

Pricing and Availability
The ATECC608A is available for $0.56 each in 10,000 unit quantities. The ATCryptoAuth-XPRO-B add-on development board is available for $10.00 each.

For additional information, contact any Microchip sales representative or authorized worldwide distributor. To purchase products mentioned in this press release, go to Microchip's easy-to-use online sales 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):

- PR graphic: **www.flickr.com/photos/microchiptechnology/38318249271**
- Chip shot: **www.flickr.com/photos/microchiptechnology/38318249941**
- Block diagram: **www.flickr.com/photos/microchiptechnology/38318249431**

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**.

Note: The Microchip name and logo and the Microchip logo are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries. ARM and Cortex are the registered trademarks of ARM Limited in the EU and other countries. All other trademarks mentioned herein are the property of their respective companies.

Editorial Contact:
Kimberly Kulesh
480-792-4531
Kimberly.kulesh@microchip.com

Reader Inquiries:
1-888-624-7435

Source: Microchip Technology Incorporated