September 30, 2019

Microchip Simplifies Hardware-Based IoT Security with the Industry's First Pre-Provisioned Solutions for Deployments of Any Size

With a minimum orderable quantity of 10 units, Microchip's Trust Platform provides hardware-based secure key storage for low-, mid- and high-volume deployments

CHANDLER, Ariz., Sept. 30, 2019 (GLOBE NEWSWIRE) -- As the number and types of connected devices proliferates, market fragmentation and security vulnerabilities in the Internet of Things (IoT) have created significant challenges for developers. Hardware-based security is the only way to protect secret keys from physical attacks and remote extraction, but extensive security expertise, development time and costs are required to configure and provision each device. With companies producing anywhere from hundreds to millions of connected devices per year across the globe, scalability of architecture can be a major barrier to deployments. Manufacturers typically have only been able to support configuring and provisioning for high-volume orders, leaving companies with low- to mid-sized deployments with low performing options. To address this need in the mass market, Microchip Technology Inc. **(Nasdaq: MCHP)** today introduced the industry's first pre-provisioned solution that provides secure key storage for low-, mid- and high-volume device deployments using the ATECC608A secure element. **Microchip's Trust Platform for its CryptoAuthentication™ family** enables companies of all sizes to easily implement secure authentication.

Microchip's Trust Platform consists of a three-tier offering, providing out-of-the-box pre-provisioned, pre-configured or fully customizable secure elements, allowing developers to choose the platform best suited for their individual design. As the first solution to provide ready-to-go secure authentication for the mass market, the first tier – **Trust&GO** – provides zero-touch pre-provisioned secure elements with a Minimum Orderable Quantity (MOQ) as low as 10 units. Device credentials are pre-programmed, shipped and locked inside the ATECC608A for automated cloud or LoRaWAN™ authentication onboarding. In parallel, corresponding certificates and public keys are delivered in a "manifest" file, which is downloadable via Microchip's purchasing e-commerce store and select distribution partners. In addition to saving up to several months of development time, the solution significantly simplifies provisioning logistics, making it easy for mass market customers to secure and manage edge devices without the overhead cost of third-party provisioning services or certificate authorities.

With the ability to authenticate to any public or private cloud infrastructure, Microchip's Trust Platform is also flexible and customizable. For customers who want more customization, the program includes the TrustFLEX and TrustCUSTOM platforms. The second tier in the program, **TrustFLEX,** offers the flexibility to use the customer's certificate authority of choice while still benefiting from pre-configured use cases. These use cases include baseline security measures such as Transport Layer Security (TLS) hardened authentication for connecting to any IP-based network using any certificate chain, LoRaWAN authentication, secure boot, Over-the-Air (OTA) updates, IP protection, user data protection and key rotation. This reduces the time and complexity involved in customizing the device without requiring customized part numbers. For customers who would like to entirely customize their designs, the third tier in the program – **TrustCUSTOM** – provides customer-specific configuration capabilities and custom credential provisioning.

"The uptick in successful attacks on software-based security solutions underscores the need for companies to adopt industry best practices, including isolating private keys in secure elements," said Nuri Dagdeviren, vice president of Microchip's secure products business unit. "Microchip's Trust Platform makes hardware-based security simple and cost-effective for companies of all sizes to implement, removing the barriers traditionally associated with configuring and provisioning devices."

Microchip worked with Amazon Web Services (AWS) to enable a straightforward and simplified onboarding process into AWS IoT services for products designed with all variants of the Microchip Trust Platform.

The ATECC608A provides Common Criteria Joint Interpretation Library (JIL) "high"-rated secure key storage, giving customers confidence that devices implement industry-proven security practices and the highest level of secure key storage. With hardware-based root of trust storage and cryptographic countermeasures, the device protects against the widest classes of known physical attacks. Microchip's secure manufacturing facilities safely provision keys, ensuring that keys are never exposed to any party during provisioning or the lifetime of the device.

Development Tools
The ATECC608A can be paired with any microcontroller and microprocessor. For rapid prototyping of secure solutions, designers can use the Trust Platform Design Suite, which includes:

- A guided "use case tool"
- Executable Python tutorials running on Jupyter notebooks
- C code examples for each use case
- A "secret exchange" utility
- The Trust Platform hardware development kits

Pricing and Availability
Devices in Microchip's Trust Platform are available in volume production today with the following minimum order quantities (MOQ):

- **Trust&GO** for TLS (ATECC608A-TNGTLSx-B): $1.20 with a MOQ of 10 units*
- **Trust&GO** for TLS (ATECC608A-TNGTLSx-G): $0.77 with a MOQ of 2000 units*
- **Trust&GO** for LoRaWAN (The Things Industries ATECC608A-TNGLORAx-B and Actility ATECC608A-TNGACTU-B): $1.40 with a MOQ of 10 units*
- **TrustFLEX** for LoRaWAN any join servers (ATECC608A-TFLXLORAx): $0.938 with a MOQ of 2000 units*
- **TrustFLEX** (ATECC608A-TFLXTLSx): $0.845 with a MOQ of 2,000 units*

- **TrustCUSTOM** (ATECC608A-TCSTMx): $0.883 with a MOQ of 4,000 units*
  *uDFN (x = U) or SO8 (x = S)

Development tools in Microchip's Trust Platform are available at:

- CryptoAuth Trust Platform kit: $13
- ATECC608a Trust Platform kit: $14

For additional information and to purchase products mentioned here, visit Microchip's **purchasing portal** or contact a Microchip authorized distributor.

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

- Application image: **https://www.flickr.com/photos/microchiptechnology/48650099116**
- Tool photo: **https://www.flickr.com/photos/microchiptechnology/48631110133**

About Microchip Technology
Microchip Technology Inc. is a leading provider of smart, connected and secure embedded control solutions. Its easy-to-use development tools and comprehensive product portfolio enable customers to create optimal designs which reduce risk while lowering total system cost and time to market. The company's solutions serve more than 125,000 customers across the industrial, automotive, consumer, aerospace and defense, communications and computing markets. 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. All other trademarks mentioned herein are the property of their respective companies.

Editorial Contact:
Chelsey Kruger
480-792-5047
chelsey.kruger@microchip.com

Reader Inquiries:
1-888-624-7435

Source: Microchip Technology Inc.