March 8, 2017

Microchip Simplifies the Development of Smart, Connected and Secure Solutions with a Hardware Cryptography-Enabled Microcontroller

The CEC1702 Full-Featured Microcontroller Streamlines Security Implementation for an Increasingly Connected World

CHANDLER, Ariz., March 08, 2017 (GLOBE NEWSWIRE) -- The CEC1702 hardware cryptography-enabled microcontroller is now available from Microchip Technology Inc. (NASDAQ:MCHP), a leading provider of microcontroller, mixed-signal, analog and Flash-IP solutions. The CEC1702 addresses the increasing need for security measures, such as secure boot, driven by the continual growth of Internet of Things (IoT) applications. For more information about the CEC1702, visit: **http://www.microchip.com/promo/CEC1702**

The CEC1702 is a full-featured ARM® Cortex®-M4-based microcontroller with a complete hardware cryptography-enabled solution in a single package. This low-power but powerful, programmable 32-bit microcontroller offers easy-to-use encryption, authentication, private and public key capabilities and allows customer programming flexibility to minimize customer risk. The CEC1702 also provides significant performance improvements when compared to firmware-based solutions. The device's hardware cryptographic cipher suite reduces compute time by orders of magnitude over software solutions, and, as an example, provides 20-50x performance improvement for PKE acceleration as well as 100x improvement for encryption/decryption. This robust hardware-based feature set results in applications that can run security measures quickly, effectively and with significantly lower cost and power consumption.

Protecting system integrity has never been more important. Whether it's being used as a security coprocessor or a standalone microcontroller, the CEC1702 delivers a multi-dimensional defense against attacks, including:

- **Pre-boot authentication of system firmware**: Providing an immutable identity and a root of trust to ensure that the firmware is untouched and hasn't been corrupted
- **Firmware update authentication**: Verifying that the firmware update has not been corrupted and is from a trusted source
- **Authentication of system critical commands**: Attesting that any system-critical command is from a known source with authorization to make the given change, preventing potentially devastating actions
- **Protection of secrets with encryption**: Safeguarding code and data to prevent theft or malicious activities

"The acceleration of the Internet of Things has brought higher visibility to the security considerations of new designs," said, Ian Harris, vice president of Microchip's computing

products group. “One of the hardest challenges to solve in a connected system is the ability to ensure that the boot code has not been compromised. The CEC1702 eliminates this issue by making it easy for designers to verify pre-boot authentication and then provide firmware updated from known, trusted resources.”

Development Support
Microchip simplifies adding authentication and encryption to connected designs by offering a full development suite including hardware and software tools as well as peripheral libraries and crypto Application Program Interfaces (APIs) to speed up design cycles. For additional information on development tools and support, visit:
http://www.microchip.com/promo/CEC1702

Pricing and Availability
The CEC1702Q-B1- SX is available in production volume for $2.60 USD per device in 10k unit quantities.

For additional information, contact any Microchip sales representative or authorized worldwide distributor. To purchase products mentioned in this press release, go to the new, easier-to-navigate and mobile-optimized **microchipDIRECT (http://new.microchipdirect.com/productsearch.aspx?Keywords=cec1702)** or contact one of Microchip’s authorized distribution partners.

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

- Chip graphic: **www.flickr.com/photos/microchiptechnology/32908601380/**
- Block diagram: **www.flickr.com/photos/microchiptechnology/32448569264/**

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. 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

MICROCHIP

Source: Microchip Technology Incorporated