Microchip Brings Hardware Quantum Resistance to Embedded Controllers

The MEC175xB family features post-quantum cryptography, enhanced security features and low power consumption

CHANDLER, Ariz., May 15, 2025 (GLOBE NEWSWIRE) -- Driven by advancements in cryptographic research and the need for stronger security measures, the National Security Agency (NSA) introduced the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) to establish a set of quantum-resistant cryptographic standards. The NSA is now urging data center and computing markets to become post-quantum ready within the next two years. To help system architects meet evolving security demands, Microchip Technology **(Nasdaq: MCHP)** has developed its **MEC175xB embedded controllers** with embedded immutable post-quantum cryptography support.

As a standalone controller, the MEC175xB family employs a modular approach for developers to efficiently adopt post-quantum cryptography, helping ensure long-term data protection without compromising existing functionality. These low-power controllers are designed with National Institute of Standards and Technology (NIST) approved post-quantum cryptographic algorithms, configurable secure boot solutions and an advanced Enhanced Serial Peripheral Interface (eSPI).

"As the significance of potential, future attacks on cryptography using quantum computing is understood more widely, the cybersecurity landscape is already undergoing substantial transformations," said Nuri Dagdeviren, corporate vice president of Microchip's security products business unit. "Our MEC175xB controllers, featuring quantum-resistant cryptography implemented in immutable hardware with efficient power management, are designed to equip our customers with the tools they need to navigate increasingly complex digital security requirements."

MEC175xB controllers incorporate CNSA 2.0-compliant Module-Lattice-Based Digital Signature Algorithms (ML-DSA), Merkle stateful hash-based Leighton-Micali Signature (LMS) verification and Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) standardized by NIST. These new algorithms with quantum attack resistance are implemented in immutable hardware to block attack paths possible on software implementations.

The controllers feature secure boot and secure firmware update schemes configurable to use either CNSA 1.0 or 2.0 or hybrid-based signature verification. Attestation capabilities use ML-DSA for signing and key generation to enhance system integrity and authenticity. At the core is an Arm® Cortex®-M4F processor with a Memory Protection Unit (MPU) running at 96 MHz to deliver high performance for complex computations and real-time applications. The controllers include 480 KB of SRAM, I3C® host and client interfaces and an optional USB 2.0 Full-Speed interface for versatile connectivity.

Visit the website to learn more about Microchip's portfolio of **security products.**

Development Tools

MEC175xB controllers are compatible with MPLAB® X Integrated Development Environment (IDE), and supported by example projects, such as blinking LEDs, available in the Secure Document Extranet (SDE) and external tools such as Zephyr®. The controllers are also supported by the MEC1753-240 MECC (EV48H83A) development board.

Pricing and Availability

MEC175xB controllers are currently available as part of Microchip's early adopter program. For additional information, contact a Microchip sales representative, authorized worldwide distributor or visit Microchip's Purchasing and Client Services website, **www.microchipdirect.com**.

Resources

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

- Application image:
  https://www.flickr.com/photos/microchiptechnology/54456487663/sizes/o/

About Microchip Technology:

Microchip Technology Inc. is a leading provider of smart, connected and secure embedded control and processing 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 over 100,000 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, 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:
Amber Liptai
480-792-5047
amber.liptai@microchip.com

Reader Inquiries:
1-888-624-7435

Source: Microchip Technology Inc.