March 26, 2024

Microchip Technology Expands TrustFLEX Family with CEC1736 Real-time Platform Root of Trust Devices

TrustFLEX devices along with the Trust Platform Design Suite tool will simplify the enablement of root of trust from concept to production in wide range of applications

CHANDLER, Ariz., March 26, 2024 (GLOBE NEWSWIRE) -- As technology and cybersecurity standards continue to evolve, Microchip Technology **(Nasdaq: MCHP)** is helping make embedded security solutions more accessible with its **CEC1736 TrustFLEX devices**. The CEC1736 Trust Shield family is a microcontroller-based platform root of trust solution enabling cyber resiliency for data centers, telecom, networking, embedded computing and industrial applications. Now, as part of the TrustFLEX platform, the devices are partially configured and provisioned with Microchip-signed Soteria-G3 firmware to reduce the development time needed to integrate platform root of trust. These devices also help fast-track the provisioning of required cryptographic assets and signed firmware images, simplifying the process of secure manufacturing as required by the National Institute of Standards and Technology (NIST) and Open Compute Project (OCP) standards.

Specifically designed to meet NIST 800-193 platform resiliency guidelines, as well as OCP requirements, CEC1736 TrustFLEX devices can support security features necessary to enable hardware root of trust across various markets. The **Trust Platform Design Suite** tool will allow customers to personalize platform-specific configuration settings, including unique credentials, to support any application, host processor or SoC that boots out of an external SPI Flash device to extend the root of trust in the system.

“Microchip has led our industry in streamlining secure provisioning from design to deployment for devices and platforms of all scales. This rich range of solutions now include OCP-compliant root of trust devices,” said Nuri Dagdeviren, corporate vice president of Microchip’s secure computing group. “With the pre-configured CEC1736 TrustFLEX family, we are helping lower the barrier of entry and making it easier for customers to implement platform root of trust and enable faster prototyping and speed to market.”

Modern firmware security features enabled on the CEC1736 TrustFLEX—like SPI bus monitoring, secure boot, component attestation and lifecycle management—can keep both the pre-boot and real-time (time of check and time of use) environments shielded from both in-person and remote threats.

The highly configurable, mixed-signal, advanced I/O CEC1736 controllers integrate a 32-bit 96 MHz Arm® Cortex®-M4 processor core with closely coupled memory to offer optimal code execution and data access.

Development Tools
Microchip's comprehensive tool ecosystem makes it easy to get started with designs. The CEC1736 TrustFLEX Configurator, part of the Trust Platform Design Suite, provides a visual view of different use cases to select, configure and generate a provisioning package for development, prototyping and production. The CEC1736 development board is equipped with a socket for easier evaluation and development.

Pricing and Availability
For additional information and to purchase, 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/53571550296/sizes/l/**
- Video available through YouTube (feel free to post)**: https://youtu.be/iaaCSdXqPcI**

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 approximately 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, the Microchip logo and MPLAB 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.