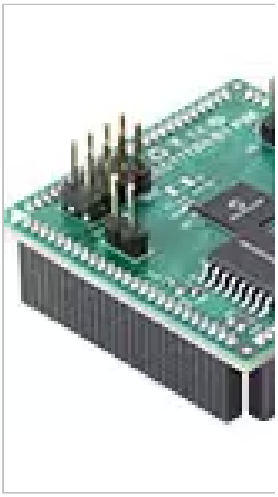

Part Number: MA990001

CEC1712H-B2 PIM ☆

- Secure boot provides a hardware-based root of trust
- Easy-to-use, seamless authentication and encryption capabilities for connected applications
- Key Revocation
- Code Rollback
- Meets NIST800-193 Platform Firmware Resiliency guidelines
- Robust hardware cryptography cypher suite
- 2.5K bits User Programmable OTP
- AES128, AES192, AES256SHA-1, SHA-256, SHA-512
- RSA-1024 to RSA-4096
- ECDSA, EC-KCDSA, Ed25519
- True Random Number

Skip to footer

- Monotonic Counter

Collapse

Overview

DM990013 and DM990013-BNDL are successful evaluation and development boards for the CEC1712 32-bit ARM® Cortex®-M4 Controller with Integrated Crypto Accelerators. These boards ship with one CEC1702Q-B2 Plug in Module (PIM). As customers evaluate the CEC1702 and develop their projects, they require the ability to program the OTP (one-time-programmable) memory in the CEC1712. The CEC1712H-B2 Plug-In-Module (PIM) is designed to mate with the CEC1x02 Development Boards (#DM990013 and #DM90013-BNDL) to enable customers to evaluate, develop and program all aspects of the CEC1712, including the OTP.

Benefits:

• CEC1712 secure boot provides a HW-based root of trust. This is a critical feature for customers concerned about protecting their brand and revenue stream from the adverse effects of a pre-boot or root security breaches. An immutable identity and a root of trust ensure that the firmware is untouched and hasn't been corrupted

• Firmware update authentication: Verifying that firmware updates have not been corrupted and are 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

Package Contents

N/A

Skip to footer