

Log in to myMicrochip to access tools and benefits. [Sign up in just one minute.](#)



All



E



my Microchip

[Overview](#)[Documentation](#)[Software](#)

Part Number: **MA990004**

# CEC1702Q-B2 PIM

- Standard 100-pin connector for Plug in Module (PIM) for the CEC1702 family
- Immutable secure bootloader, implemented in ROM, serves as the system Root-of-Trust (RoT)
- Robust hardware cryptography cipher suite for encryption, decryption, authentication, key management and secure boot
- CEC1702 hardware security accelerators support
  - AES-256
  - SHA-256
  - ECDSA
- CEC1702 immutable Boot ROM decrypts and authenticates EC firmware image while application processor is in reset
- Authenticate up to 31 application firmware images while application processor in in reset

 [Collapse](#)

## Overview

[Skip to footer](#)

DM990013 and DM990013-BNDL are successful evaluation and development boards for the CEC1702 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 CEC1702. The CEC1702Q-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 CEC1702, including the OTP.

Benefits:

- CEC1702 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

## All Application Notes

# Documentation

---

[Skip to footer](#)