CEC173x Trust Shield Family

Summary

The CEC173x Trust Shield family is a real-time platform root of trust solution that enables cyber resiliency of end equipment in the data center, telecom, networking, embedded computing and industrial markets.

Containing the easy-to-use Soteria-G3 firmware, Trust Platform Design Suite (TPDS) and MPLAB® Harmony, the CEC173x Trust Shield family enables fast development of the fully configurable micro-controller-based root of trust solution to get your design to market quickly.

The CEC173x Trust Shield family meets NIST 800-193 PFR, Open Compute Project® security guidelines, TCG DICE, HCD-CPP, FIPS 140-2, CAVP and third-party penetration tests.

Target Application

The CEC173x Trust Shield family is best suited for any processors or graphic processing units that boot from external SPI Flash.

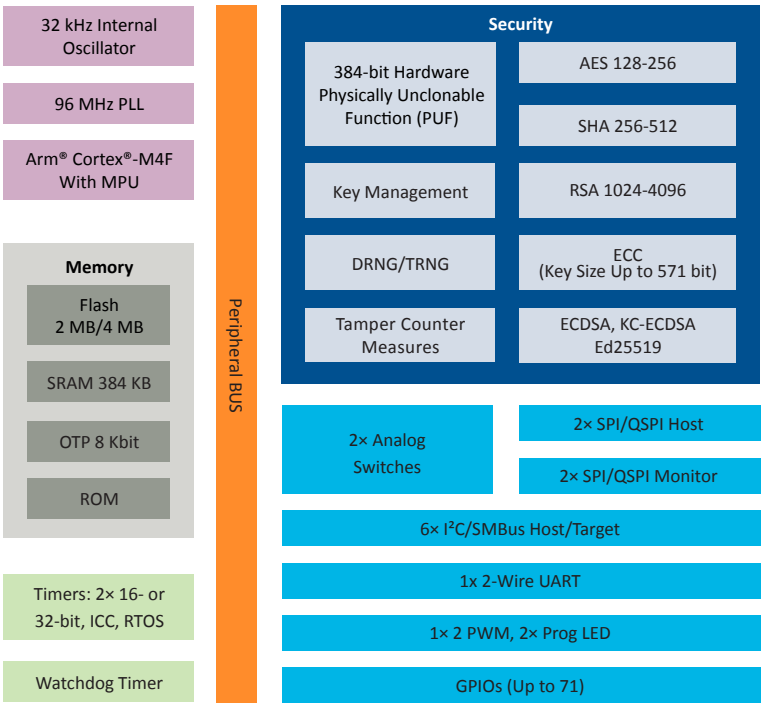
Target Markets

- Data centers
- Telecom/5G
- Embedded computing
- Networking/Internet of Things (IoT)
- Industrial

Key Security Features

- Hardware CNSA secure boot/secure updates
- Real-time SPI bus monitoring, I²C/SMBus filtering
- 384-bit Physically Unclonable Function (PUF)
- Device and firmware attestation
- Side-channel attack countermeasures
- Lifecycle management and ownership transfer
- Advanced hardware crypto cipher suite

CEC173× Family

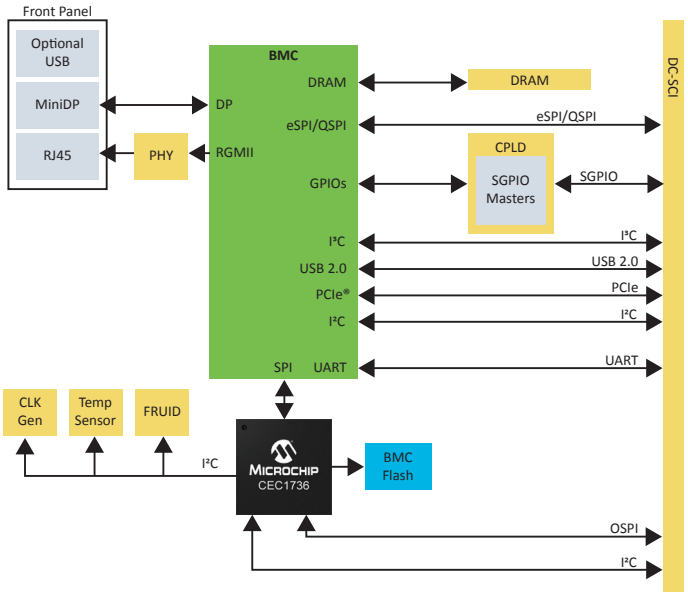


Product Features

- 96 MHz Arm® Cortex®-M4F microprocessor (MPU) core
- 2 MB/4 MB Flash
- 384 KB RAM
- Immutable boot ROM
- 8 Kb OTP with antifuse technology
- 2× SPI/QSPI controllers
- 6× I2C/SMBus host and target
- 1× UART, 2× PWMs and 2× Prog LEDs
- Up to 71 GPIOs
- 64- and 84-pin WFBGA

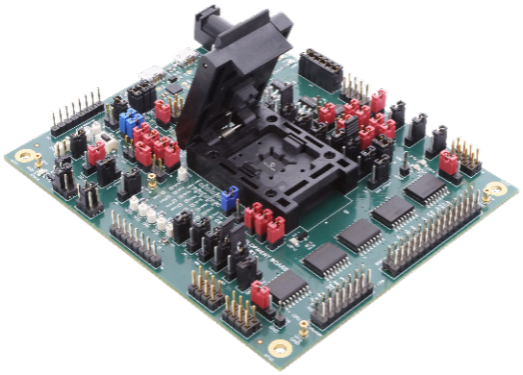
OCP DC-SCM Example Block Diagram

Refer to the diagram below to learn how the CEC173x family brings next-generation, real-time platform root of trust to the example data center secure control module.



Getting Started

The CEC1736 development board is ready to use out of the box and contains the following tools:



- Trust Platform Design Suite (TPDS)
- GUI for security provisioning
- MPLAB Harmony tools

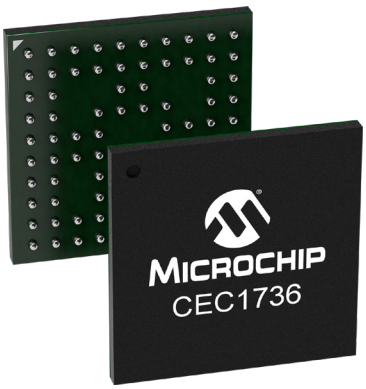
https://www.microchip.com/en-us/development-tool/ev19k07a---cec1736-development-board

Where to Buy and Learn More

Visit the CEC173x product pages below to learn more about the silicon. Both the CEC1736 and CEC1734 come in 64- and 84-pin WFBGA packages.

https://www.microchip.com/en-us/product/cec1736

https://www.microchip.com/en-us/product/cec1734



DS00004516A