CEC173x Trust Shield（信任盾）系列

概览

CEC173x Trust Shield系列是一款实时平台可信根解决方案，可实现数据中心、电信、联网、嵌入式计算和工业市场中终端设备的网络弹性。

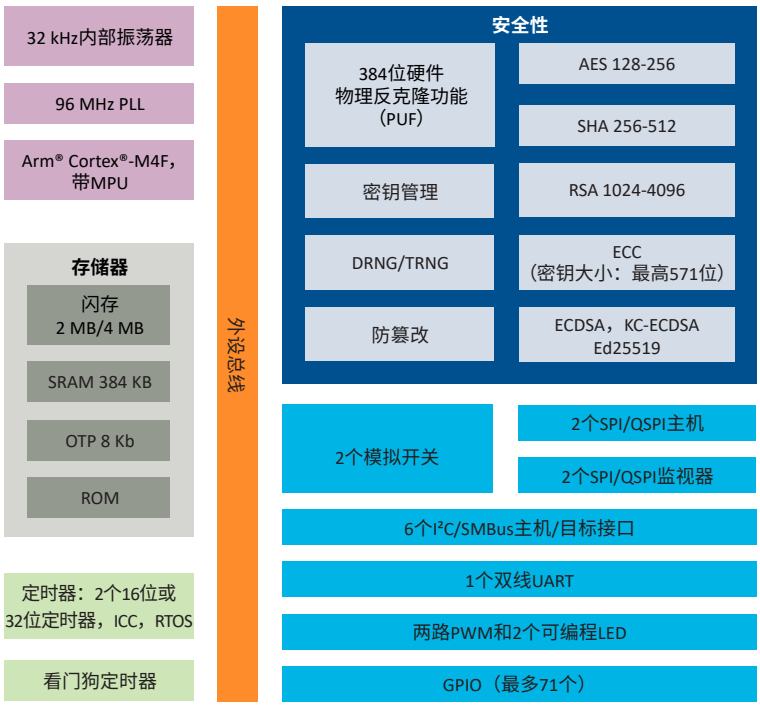
CEC173x Trust Shield系列包含易于使用的Soteria-G3固件、可信平台设计套件（TPDS）和MPLAB® Harmony，支持快速开发基于单片机的完全可配置可信根解决方案，从而将新设计更快推向市场。

CEC173x Trust Shield系列可满足NIST 800-193 PFR、Open Compute Project®（开放计算项目）安全指南、TCG DICE、HCD-CPP、FIPS 140-2、CAVP和第三方渗透测试的要求。

主要安全特性

- 硬件CNSA安全引导/安全更新
- 实时SPI总线监控，I²C/SMBus滤波
- 384位物理反克隆功能（PUF）
- 器件和固件认证
- 侧信道攻击对策
- 生命周期管理和所有权转移
- 高级硬件加密套件

CEC173x系列



目标应用

CEC173x Trust Shield系列非常适合从外部SPI闪存引导的处理器或图形处理单元。

目标市场

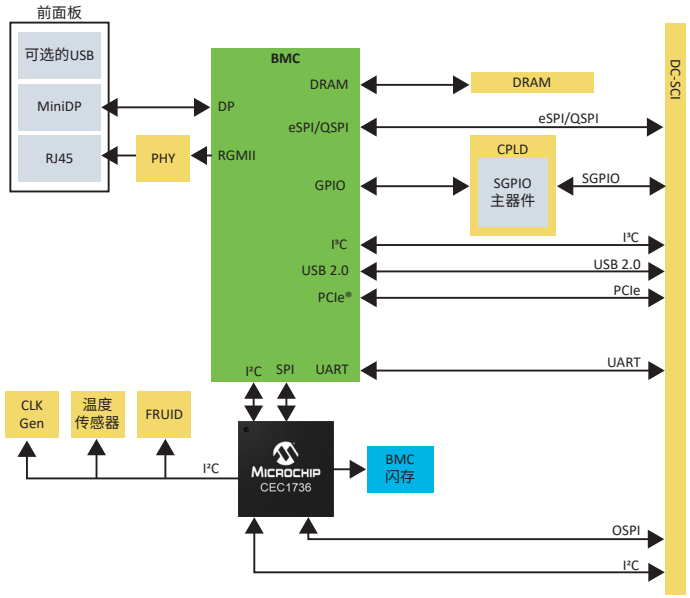
- 数据中心
- 电信/5G
- 嵌入式计算
- 联网/物联网（IoT）
- 工业

产品特性

- 96 MHz Arm® Cortex®-M4F微处理器（MPU）内核
- 2 MB/4 MB闪存
- 384 KB RAM
- 不可变的引导ROM
- 采用反熔丝技术的8 Kb OTP
- 2个SPI/QSPI控制器
- 6个I²C/SMBus主机和目标接口
- 1个UART，两路PWM和2个可编程LED
- 最多71个GPIO
- 64和84引脚WFBGA

OCP DC-SCM示例框图

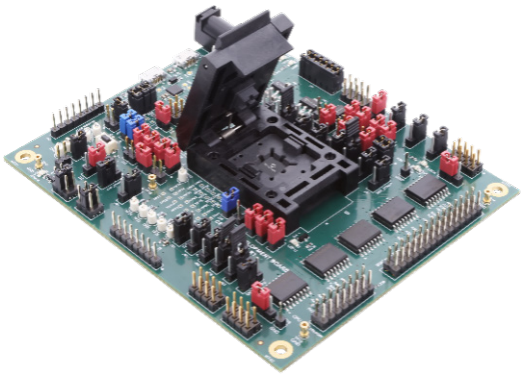
参阅下图，了解CEC173x系列如何将下一代实时平台可信根引入示例数据中心安全控制模块。



使用入门

下列便捷工具均支持CEC1736开发：

CEC1736开发板——EV19K07A



https://www.microchip.com/en-us/Development-Tool/EV19k07a---CEC1736-Development-Board

- 可信平台设计套件（TPDS）
- Soteria-G3固件
- MPLAB Harmony v3

购买渠道以及更多详情

访问以下CEC173x产品页面，了解有关该芯片的更多信息。CEC1736和CEC1734均采用64和84引脚WFBGA封装。

https://www.microchip.com/en-us/product/CEC1736

https://www.microchip.com/en-us/product/CEC1734