

CEC1702和CEC1302

针对IoT实现硬件加密的32位MCU

为您保驾护航

安全威胁的频率、复杂性和广泛性正呈爆炸式增加。为确保宝贵资产的安全，产品设计时必须侧重于提供稳健而安全的互联系统。

Microchip提供CEC1702和CEC1302这两款多功能的解决方案来防范复杂攻击。两者都是将一整套加密机制嵌入单个封装的低功耗MCU。

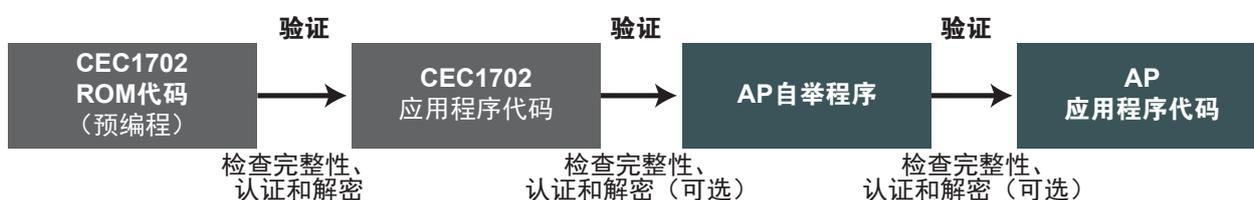


主要优点

- 提供稳定的安全引导平台
- 有效充当独立的MCU或安全协处理器
- 显著提高安全防范的响应速度和成本效益
- 为稳定的信任链奠定基础
- 无缝实现认证和加密
- 允许客户编程以最大程度降低实现风险

产品功能

- 安全引导提供基于硬件的信任链
- ARM® Cortex®-M4处理器内核，以48 MHz的速度运行
- 128 KB至480 KB的SRAM，用于代码和数据存储
- 支持一系列硬件加速的加密函数
 - 加密
 - 认证
 - 椭圆曲线加密
 - 真随机数发生



CEC1702产品功能

- 用于防止代码损坏的集成式存储器保护单元
- 提速8倍以上的公共密钥引擎，以改进实时性能
- 2.5 Kb的用户可编程OTP
- 其他加密函数，包括：
 - SHA-224、SHA384和SHA-512
 - 高达4096位的RSA密钥
 - ECDSA、EC-KCDSA和ED25519

CEC1702系统框图



开发工具

SecureloT1702演示板 (DM990012)

SecureloT1702演示板是一款外形小巧的评估板，可演示CEC1702 MCU的功能。该演示板中内置了很多硬件功能，例如LCD显示屏、USB micro-B连接器、调试接口、晶振和串行闪存。这款功能强大的器件可用于多种应用，包括Apple® HomeKit™、Microsoft Azure和Amazon Web Services。



Apple HomeKit

SecureloT1702演示板通过基于硬件的安全引擎使能，它证实了HomeKit的非凡速度；事实上，像配对这样的关键命令只需不到十分之一秒即可完成。开门和开灯等操作可立即执行，从而开创无缝用户体验。

Microsoft Azure

使用SecureloT1702演示板，用户可以对连接到Microsoft Azure的IoT设备的安全性和效率充满信心。演示板有助于创建顺畅、安全的通信和自适应系统网络，从而满足用户的最佳需求。

Amazon Web Services

Amazon Web Services是最大型的云计算平台之一。使用SecureloT1702演示板，用户可以轻松安全地将设备连接到云。该演示板使用户能够深入了解CEC1702 MCU在连接云的系统中的效用。

CEC1702和CEC1302 Clicker板

可信的第三方工具提供商MikroElektronika为CEC1702和CEC1302提供紧凑的开发工具包。每个工具包还分别配备了一个（CEC1X02 Clicker）或两个（CEC1X02 Clicker 2）mikroBUS™插槽。用户可以快速构建自己的装置，用于一键生成密钥、加密和解密文件以及创建SPI图像。您可在www.mikroe.com上查看这些板。

Microchip的名称和徽标组合以及Microchip徽标均为Microchip Technology Incorporated在美国和其他国家或地区的注册商标。ARM和Cortex是ARM Limited（或其子公司）在欧盟和其他国家或地区的注册商标。在此提及的所有其他商标均为各持有公司所有。© 2017, Microchip Technology Incorporated。版权所有。8/17 DS00002284B_CN