支持硬件加密的32位MCU适用于物联网

集成加密功能的CEC1302 32位ARM® Cortex® M4控制器

让您的世界安全无虑

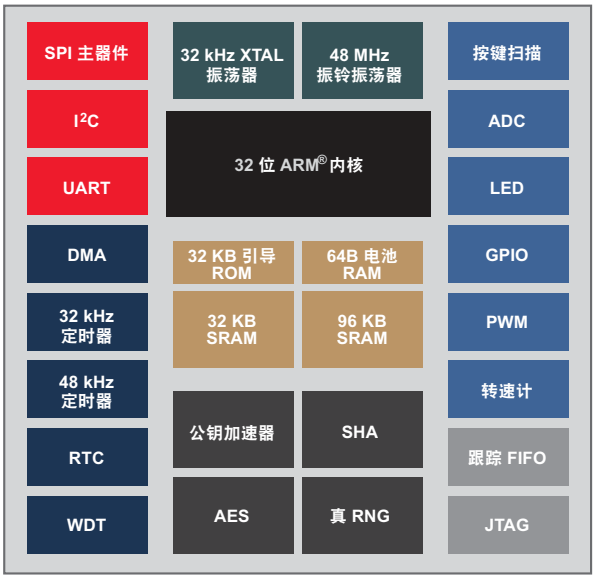
无论是从攻击的频率、目标设备和恶意程度，还是从造成的损失大小上来看，安全威胁都呈爆炸式增长。在当今庞大的互联世界中，在产品或系统中提供更高的安全性，已经成为一种标准要求。想要在与犯罪份子的对抗中抢占先机，产品设计中就必须采用稳健而安全的互联系统。这有助于防止软件/硬件、知识产权、数据或通信服务遭窃取。

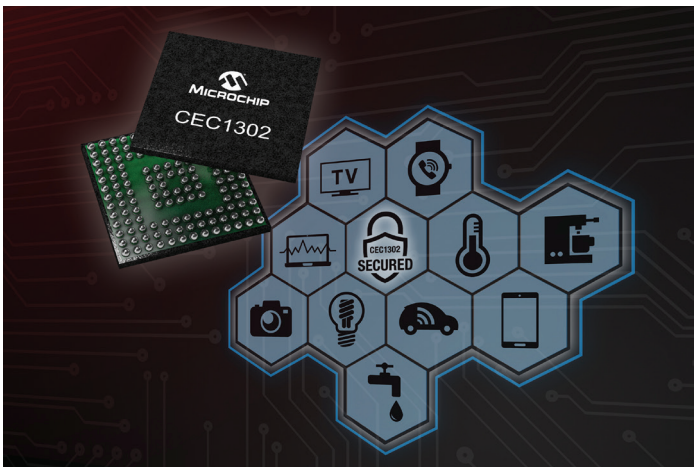
Microchip的CEC1302是一款低功耗嵌入式加密控制器，能够轻松快速地对系统固件进行启动前身份验证。这样可以确保固件不会外泄和遭到破坏，进而抵御中间人攻击、拒绝服务攻击和后门漏洞等安全攻击。这款控制器还可用于对任何固件更新进行身份验证，从而保护系统免受恶意软件破坏或防止内存崩溃。

主要优势

- 相较于固件安全解决方案，性能大幅提升
- 32位ARM® Cortex® M4处理器内核可用作独立单片机
- 易于使用的身份验证、私钥和客户编程灵活性，可最大程度地降低客户风险

框图





CEC1302产品特性

- ARM Cortex-M4处理器内核，运行于48 MHz频率
- 128 KB SRAM（用于存储代码和数据）
  - 96 KB（针对代码进行了优化）
  - 32 KB（针对数据进行了优化）
- 多功能AES加密引擎
  - 通过对称加密保护隐私
  - 为ECB、CTR、CBC和OFB AES模式提供硬件支持
- 256位密钥长度
  - DMA与SRAM接口，与Hash引擎共享
- 采用公钥算法（RSA-2048）进行身份验证
- 使用真随机数发生器（RNG）进行加密
- 使用安全的Hash算法确保完整性
  - 支持SHA-1和SHA-256
  - DMA与SRAM接口，与AES引擎共享

典型应用

- 启动前身份验证
- 外设身份验证
- 防止固件更新引入恶意软件
- 对固件更新进行身份验证
- 对系统关键命令进行身份验证

MICROCHIP

第三方开发工具

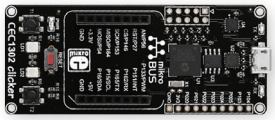
CEC1302集成了高性能的32位ARM Cortex-M4嵌入式单片机，并带有128 KB SRAM和32 KB引导ROM。它使用I²C总线与系统主机进行通信。CEC1302带有两个SPI存储器接口，让EC能够从外部SPI闪存（专用SPI和/或共享SPI）读取代码。共享SPI接口可将EC代码存储在共享SPI芯片中。专用SPI存储器接口则是为专用SPI闪存提供的，只有EC才能访问该闪存。

CEC1302支持在Vcc1上电时从专用或共享SPI闪存器件载入EC代码。在执行从SPI闪存器件载入的EC代码之前，CEC1302会使用根据PKCS #1编码的数字签名来验证EC代码。该签名采用RSA-2048加密和SHA-256哈希算法，可自动检测因恶意或无意破坏而导致的无效EC代码。这种检测会在每次主机处理器启动之前进行，从而确保基于硬件的信任根不会轻易遭到物理更换攻击的威胁。

适用于ARM的嵌入式开发工具链IAR Embedded Workbench支持CEC1302。这个工具链集成了高度优化的编译工具，可为物联网应用快速撰写简洁的代码，同时还带有功能全面的C-SPY调试器，其中提供了高级调试功能。IAR系统还集成了代码分析工具，以及即插即用型调试和跟踪探针。

我们提供了一整套的工具来帮助您的设计上市。

CEC1302 Clicker



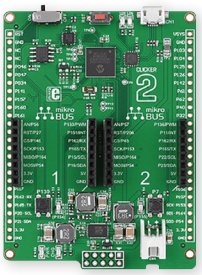
CEC1302 Clicker是极为精简的入门级开发工具包，为这款支持硬件加密的单片机带来了创新的mikroBUS™主机插槽。通过连接您选择的Click™电路板，可进一步强化功能。这个工具已预先烧写了快速USB HID自举程序。只需上传您的固件，Clicker即会成为工作器件。这款小型电路板具备您所需的全部入门级功能：CEC1302低功耗嵌入式加密控制器、USB连接、两个LED和按钮、复位按钮、编程器连接器，以及用于与外部电子设备连接的接口。

由MikroElektronika提供的产品：MIKROE-1970

mikroC PRO for ARM

mikroC PRO for ARM是一款功能全面的ANSI C编译器，适用于ARM Cortex-M4器件。这款编译器采用行业标准C语法，并提供先进的优化功能、大量的资源库和直观的用户界面，可帮助您轻松完成项目。它由受信任的第三方工具提供商MikroElektronika提供。

Clicker 2 for CEC1302



Clicker 2 for CEC1302是一款紧凑型开发工具包，带有两个mikroBUS插槽，可用于连接Click电路板。借助这个工具包的独特功能和特性，您可以快速构建自己的安全小工具。该工具包搭载了CEC1302低功耗嵌入式加密控制器，并提供mikroProg™连接器，可让您轻松编程。其他特性包括电路板两侧的2 x 26脚连接槽、按钮、开关和LED。

由microchipDIRECT提供的产品：TMIK011
由MikroElektronika提供的产品：MICROE-1969

mikroBasic PRO for ARM

mikroBasic PRO for ARM是一款功能全面的Basic编译器，适合所有用户进行ARM M4开发。流行的Basic编程语言是新手的最好选择，因为它语法简单，代码简洁。它由受信任的第三方工具提供商MikroElektronika提供。

适用于CEC MCU的mikroProg™编程器和调试器

mikroProg for CEC1302是一款快速编程器和硬件调试器。凭借智能工程设计，mikroProg能够支持具有安全固件更新功能的CEC1302加密引擎。它拥有众多重要特性，包括卓越的性能、易操作性、优雅的设计和实惠的价格。MikroElektronika ARM编译器支持这款工具。mikroProg内置了快速硬件调试器。您可以对芯片本身调试代码并监控代码执行。mikroProg技术将强大的硬件调试功能融入到您喜爱的编译器中。这款工具由受信任的第三方工具提供商MikroElektronika提供。

MICROCHIP

www.microchip.com/CEC1302

更多产品信息和各地销售办事处地址，请访问我公司网站。

Microchip Technology Inc. · 2355 W. Chandler Blvd. · Chandler, AZ 85224-6199

Microcontrollers • Digital Signal Controllers • Analog • Memory • Wireless

Microchip的名称和徽标组合及Microchip徽标均为Microchip Technology Incorporated在美国及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。
DS00002284A_CN