# 使用 PIC32CM LSx MCU 防止克隆

AN5548

## 简介

克隆是指未经原始制造商的适当授权而对产品、器件或元件进行复制或再生产。这可能涉及复制产品的设计、功能或标识，通常是为了仿制假冒伪劣产品或破解版产品以达到各种目的，例如销售假冒伪劣产品、危害信息安全或创造不公平的竞争优势。

市场上出售的每一款正品都会有惟一标识产品品牌的密钥和凭证。惟一标识产品品牌的密钥或凭证至关重要，需要加以保护以防止产品被克隆。它们可以保证硬件和软件都是正版，并且不会在假冒伪劣硬件上运行正版固件。

本文档解释了保护产品免遭克隆的必要性以及如何借助 PIC32CM LS60 单片机防止克隆。

### 缩写

本文档中使用了以下缩写：

- **AS**：应用程序安全（Application Secure）
- **ANS**：应用程序非安全（Application Non-Secure）
- **ANSC**：应用程序非安全可调用（Application Non-Secure Callable）
- **CMSE**：Cortex®-M 安全扩展（Cortex-M Security Extensions）
- **DFP**：器件系列包（Device Family Pack）
- **MCC**：MPLAB®代码配置器（MPLAB Code Configurator）
- **API**：应用程序编程接口（Application Programming Interface）
- **SG**：安全网关（Secure Gateway）
- **BXNS**：转移并交换到非安全状态（Branch with exchange to Non-Secure state）
- **BLXNS**：通过链接转移并交换到非安全状态（Branch with link and exchange to Non-Secure state）
- **RN**：随机数（Random Number）
- **MAC**：报文身份验证代码（Message Authentication Code）
- **Ack**：应答数据（Acknowledgement data）
- **PKI**：公钥基础架构（Public Key Infrastructure）
- **Nack**：无应答数据（No Acknowledgement of data）
- **IoT**：物联网（Internet of Things）
- **EEPROM**：电可擦除的可编程只读存储器（Electrically Erasable Programmable Read-Only Memory）
- **DICE**：设备标识符组合引擎（Device Identifier Composition Engine）
- **PKI**：公钥基础架构（Public Key Infrastructure）
- **ECDH**：椭圆曲线 Diffie Hellman（Elliptic Curve Diffie Hellman）
- **ECDSA**：椭圆曲线数字签名算法（Elliptic Curve Digital Signature Algorithm）

# 目录

# 1. 保护的必要性

保护产品免遭克隆很有必要，原因分为以下几点：

**维护品牌声誉：**克隆可能导致生产和分销印有原始制造商品牌名称的假冒伪劣产品。如果消费者收到不合格产品或因假冒伪劣商品而遭受不良后果，则可能会损害品牌声誉。

**守护消费者安全：**假冒伪劣产品或克隆产品可能不符合与正品相同的安全和质量标准。

**避免收入损失：**克隆会导致破解版产品或假冒伪劣产品入市销售，进而剥夺原始制造商的合法收入来源。

**规避安全风险：**在汽车、航空航天和电子等领域，如果克隆产品危及关键系统或基础设施，则可能带来安全风险。例如，汽车系统中克隆的电子元件可能会导致故障或漏洞，进而危及车内乘客或损害车辆安全。

**维护市场诚信：**克隆会导致破解版产品或假冒伪劣产品充斥市场，进而扭曲市场动态，破坏公平竞争和市场诚信。保护产品免遭克隆有助于为合法企业维持公平的竞争环境，并促进基于创新、质量和价值的良性竞争。

# 2. 使用 PIC32CM LSx MCU 防止克隆

以下章节详细介绍了 PIC32CM LSx MCU 有助于防止克隆的功能。

## 2.1 PIC32CM Lx 系列单片机（MCU）

PIC32CM Lx 系列单片机兼具稳健的安全性和超低功耗，同时配备增强型触摸和智能模拟功能，运行频率为 48 MHz，存储器配置最高 512 KB 闪存和 64 KB SRAM。该系列 MCU 包含三个型号：PIC32CM LS60（48 引脚）、PIC32CM LS00（64 引脚）和 PIC32CM LE00（100 引脚）。

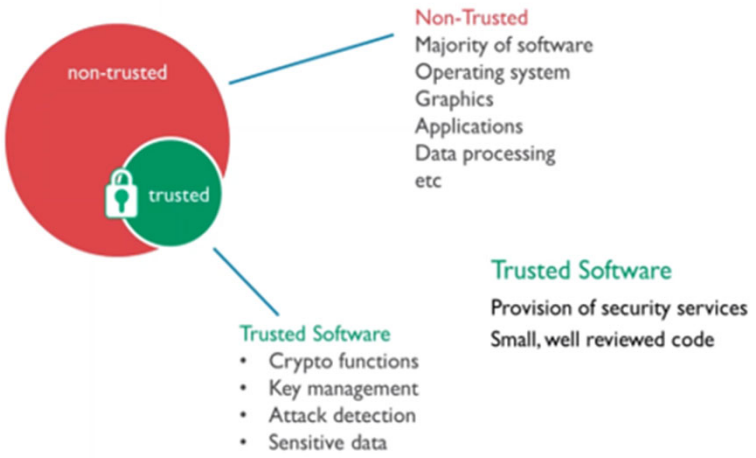
PIC32CM LE00 为通用型号。PIC32CM LS00 提供安全引导和 Arm® TrustZone®技术等安全功能。PIC32CM LS60 将 Arm TrustZone 技术与我们的可信平台 ECC608 安全元件集成在单一封装中，并受可信平台密钥配置服务和可信平台设计套件 v2 支持。PIC32CM LSx MCU 的以下功能有助于防止克隆。有关 PIC32CM Lx 系列 MCU 的更多信息，请参见 PIC32CM Lx MCU。

以下章节介绍了 PIC32CM LSx MCU 有助于防止克隆的功能。

### 2.1.1 Cortex M23 Arm TrustZone

PIC32CM LS60 MCU 搭载大量 Arm TrustZone 技术。这使得安全程序与非安全程序可在同一芯片上运行。TrustZone 可创建隔离的安全区域，仅允许获得授权的软件访问特定的存储器、外设和数据，从而确保系统完整性且不影响性能。

**图 2-1.** TrustZone 技术应用




### 2.1.2 ATECC608B 安全元件

ATECC608B 可保护敏感信息，具体通过加密协议和稳健的硬件安全功能来实现。

**加密协议：**

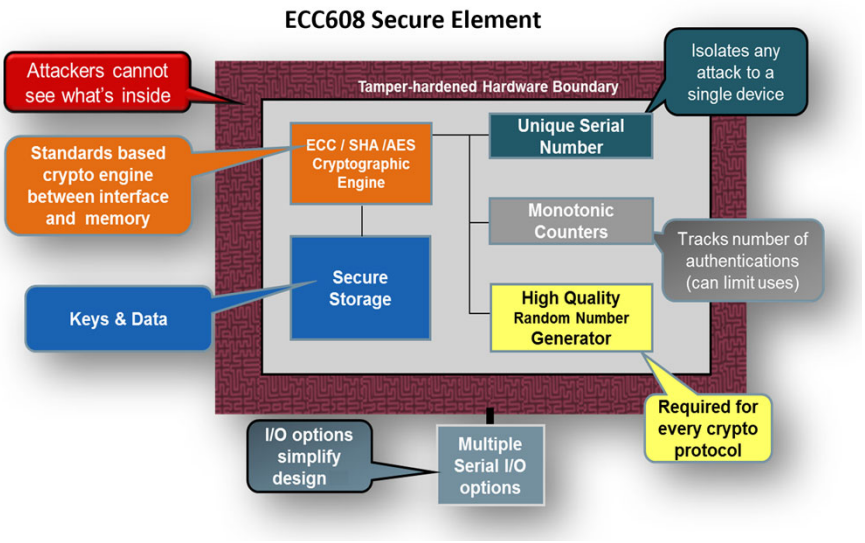
- **椭圆曲线 Diffie-Hellman（ECDH）：**简化用于加密和解密的安全密钥交换。
- **椭圆曲线数字签名算法（ECDSA）：**通过数字签名确保数据的完整性和真实性。

**硬件安全功能：**

- **安全加密引擎：**实现行业标准加密算法（ECC、SHA 和 AES）来保护器件与存储器之间的数据传输。
- **安全密钥和数据存储：**安全地存储加密密钥和机密数据，以阻止未经授权的用户访问。
- **惟一序列号：**实现个体标识并增强安全性。

- **单调计数器：**跟踪身份验证尝试的次数，有助于检测异常和潜在的安全漏洞。
- **高质量随机数发生器：**该发生器可生成不可预测的数字，这对于安全通信至关重要。
- **篡改硬化的硬件边界：**器件的这种物理结构可阻止攻击者篡改其内部组件和访问敏感信息。

**图 2-2.** ATECC608B 安全元件功能



# 3. 用例：打印机和墨盒

**场景：**

大型企业的日常运营中经常会使用到打印机，需要打印的内容包括文档和演示文稿等。此外，为了保证打印质量和信息安全，这类企业还需要寻求值得信赖的供应商采购专用墨盒。

**问题：**

这类企业担心打印机中使用的墨盒可能是假冒伪劣产品。克隆产品会影响打印质量、缩短墨盒使用寿命并带来敏感数据泄露等安全风险。

本文档的后续章节将参考该用例来讨论如何防止克隆。

# 4. 两种保护方法

## 4.1 使用 TrustZone

在打印机和墨盒用例中，可采用 TrustZone 技术解决打印机墨盒克隆问题。

- **可信（安全）执行环境（Trusted Execution Environment，TEE）：**TrustZone 在打印机的硬件内创建一个安全区域，与常规操作系统和应用程序隔离。该 TEE 负责处理墨盒身份验证和打印作业处理等关键任务，保护这些任务免遭篡改。
- **存储器分区：**TrustZone 可将打印机的存储器划分为安全区域和非安全区域。用于墨盒身份验证的敏感数据和代码位于安全存储器中，即使主系统受到威胁，也可以阻止未经授权的访问。
- **利用加密技术进行反克隆：**每个正品墨盒在制造过程中都会获得惟一的加密密钥或标识符。当墨盒插入打印机时，打印机的固件会与安全 TEE 进行交互，以使用该密钥验证墨盒是否为正品。

务必在安全环境内执行这些加密操作，以确保身份验证过程本身不会遭到篡改。如果墨盒是正品，则开始打印。否则，打印机将拒绝打印并向用户显示警告消息。

在 PIC32CM LSx 单片机（MCU）的相关章节中，TrustZone 创建了一个安全环境来运行安全程序和非安全程序。这通过将存储器和外设划分为彼此隔离的安全区域与非安全区域来实现。这种隔离可保护安全代码免遭非安全程序未经授权的访问。

**安全区域与非安全区域：**

- **安全区域：**仅限安全软件（机密信息密钥和安全引导）访问。
- **非安全区域：**器件上运行的所有软件（典型应用程序）均可访问。
- **非安全可调用（Non-Secure Callable，NSC）区域：**一种特殊的安全存储区，允许使用经过授权的任务在受控条件下从非安全状态切换到安全状态。

为了确保提供全面的保护，安全代码必须遵循特定的准则并利用特殊的安全指令，以在安全状态与非安全状态之间切换的过程中维护安全性。Arm Cortex-M 安全扩展（CMSE）为开发人员提供了在安全软件环境内管理这些安全指令的工具。

在 TrustZone 中，安全代码执行与非安全代码执行之间的切换受到严格控制。非安全代码只能调用满足特定标准的安全函数：

- **安全网关（SG）：**安全函数的第一条指令必须是 SG 指令，指示安全入口点。
- **非安全可调用（NSC）存储区：**安全函数必须位于指定的 NSC 存储区中，非安全代码可使用经过授权的调用对其进行访问。

这种隔离可将大多数安全代码隔离在安全存储区内。非安全代码只能访问 NSC 存储区中含有 SG 指令的经授权安全函数。任何违反上述安全规则的尝试（例如，直接访问安全区域或者代码与当前安全状态不匹配）都将触发硬故障异常，进而停止执行程序。

### 4.1.1 示例应用程序

该应用程序基于超时切换 LED 并在串行控制台上打印 LED 切换速率，而非安全应用程序请求安全应用程序读取 LED 切换速率并打印在串行终端上。此外，安全模式应用程序还通过 I/O1 Xplained Pro 扩展工具包上的温度传感器每 500 毫秒读取一次当前室温。之后，该应用程序将温度读数写入 EEPROM，并在收到非安全模式应用程序的请求时进行读取。每次从非安全模式应用程序收到温度显示请求时，都会切换绿色 LED（LED0）。每当用户按下 PIC32CM LS60 Curiosity Pro 评估工具包上的开关 SW0 时，温度值读数的周期都会依次变为 1s、2s 和 4s，最后再回到 500 ms。当非安全模式应用程序通过非安全可调用（NSC）函数请求保护应用程序时，温度读数会传输到非安全模式应用程序。

非安全模式应用程序请求安全模式应用程序提供温度值，并在从安全模式应用程序收到这些值后将其打印在串行控制台上。此外，当非安全模式应用程序收到用户的请求（即，按下串行控制台上的按键）时，它

还将请求安全模式应用程序获取 EEPROM 中存储的最后五个温度值。非安全应用程序在控制台上打印存储的最后五个温度值。每次从 EEPROM 读取温度值时，都会切换红色 LED（LED1）。

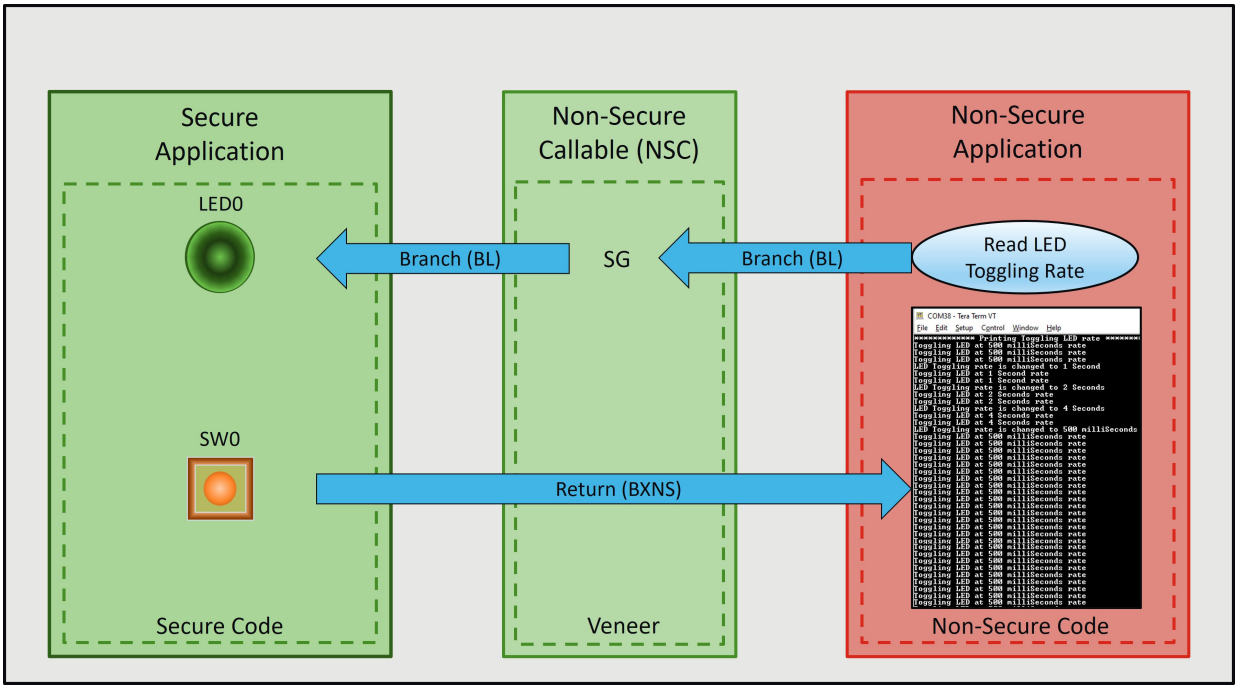
#### 4.1.1.1 设计

安全应用程序以 500 ms 的速率连续切换 LED0，后续每次按下开关（SW0）时，切换速率都会依次变为 1s、2s、4s，最后再回到 500 ms。

借助 BL 到 SG 的转移，非安全应用程序可使用 NSC 请求安全应用程序提供其数据。

借助 BXNS 转移，安全应用程序可返回到非安全应用程序以在串行控制台上打印数据。

**图 4-1.** 应用程序状态切换

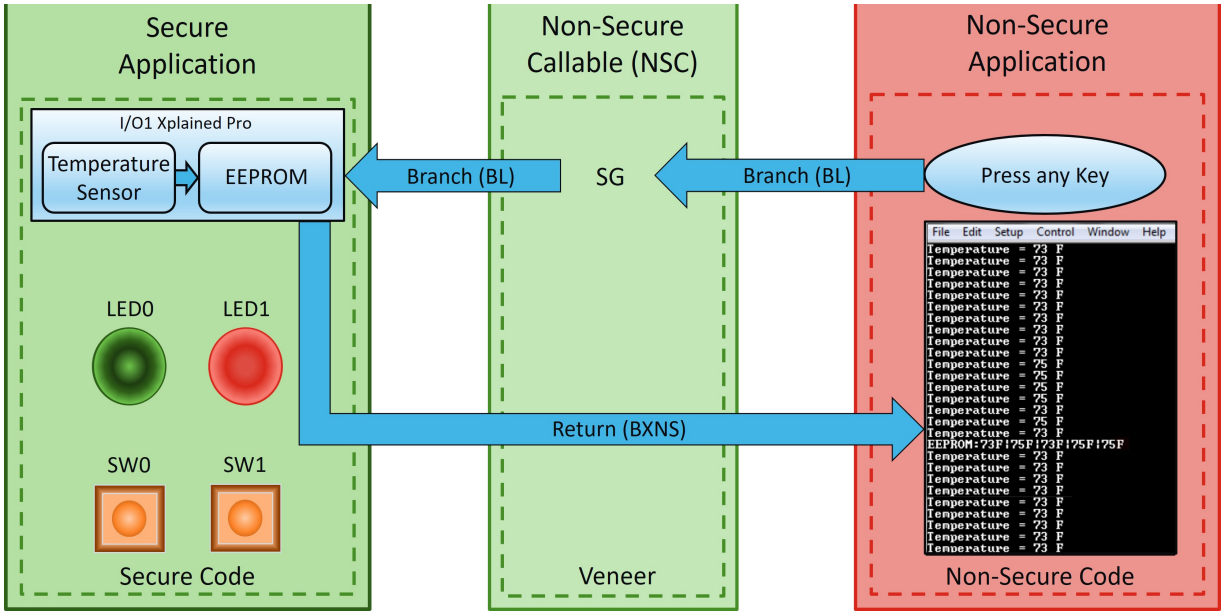



在该应用程序的扩展功能中，安全应用程序从 I/O1 Xplained Pro 扩展套件上的温度传感器读取当前室温并写入 EEPROM。

借助 BL 转移，非安全应用程序可使用 NSC 请求安全应用程序提供温度值，并将其打印在串行控制台上。

安全应用程序随后返回到非安全应用程序以获取 EEPROM 数据，并将其打印在串行控制台上。

**图 4-2.** 扩展应用程序状态切换

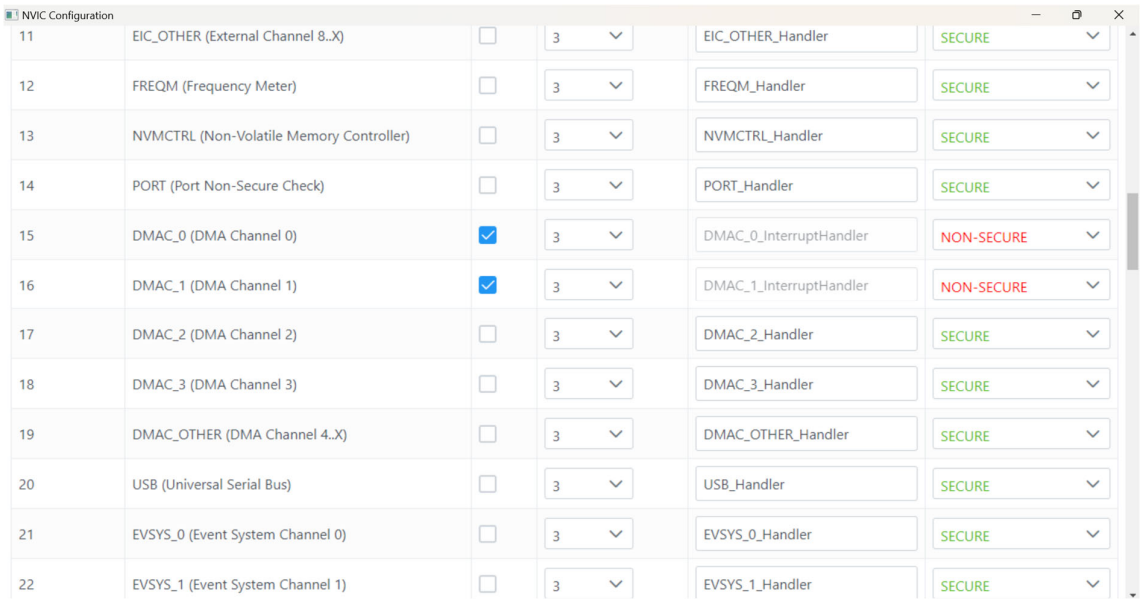



在示例实现中，`secureAppEntry( )`是从非安全应用程序调用的安全 API。在安全区域中执行`secureAppEntry( )`后，将返回到非安全应用程序。当非安全程序使用 NSC 调用安全 API 时，将使用 BXNS 指令返回到非安全状态来将该 API 执行完毕。

#### 4.1.1.2 配置

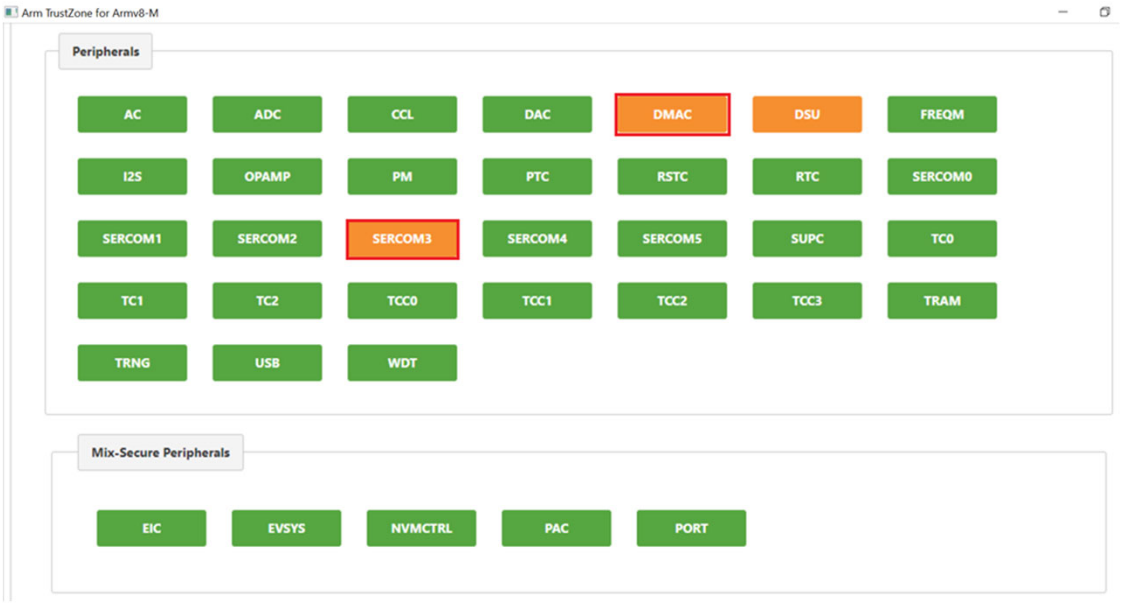
1. **嵌套向量中断控制器（Nested Vector Interrupt Controller，NVIC）：**
   NVIC 针对安全性进行了扩展，允许使用安全异常和非安全异常。根据 NVIC 中配置的优先级设置，安全代码可以中断非安全代码的执行，非安全代码也可以中断安全代码的执行。内核级 NVIC 寄存器会进行复制。这样便有两个向量表定义，一个用于安全，另一个用于非安全。
   当系统启动时，所有中断默认映射到安全区域（安全向量表）。安全区域中可访问的特定 CMSIS 函数将每个中断向量分配给非安全处理程序（在非安全向量表中声明）。

**图 4-3.** MPLAB®代码配置器——NVIC 设置




2. **SysTick 模块：**可配置为安全或非安全。
3. PIC32CM LS00/LS60 系列器件内置 5 个混合安全外设，因此安全与非安全应用程序混合安全外设之间可共享以下几个内部资源：PORT、EIC、EVSYS 和 NVMCTRL。
   - **外设访问控制器（Peripheral Access Controller，PAC）：**管理外设的安全属性（安全或非安全）。
   - **非易失性存储器控制器（NVMCTRL）：**处理安全和非安全闪存区域编程。
   - **I/O 控制器（PORT）：**支持将每个 I/O 单独分配给安全或非安全应用程序。
   - **外部中断控制器（External Interrupt Controller，EIC）：**支持将每个外部中断单独分配给安全或非安全应用程序。
   - **事件系统（EVSYS）：**支持将每个事件通道单独分配给安全或非安全应用程序。
   - **引脚配置：**可根据用户的要求将引脚配置为安全或非安全。
4. **外设访问控制器：**
   可使用外设访问控制器（PAC）将每个外设配置为安全或非安全。将外设分配给安全区域时，仅授予对其寄存器的安全访问权限，并且只能在安全区域管理中断处理。
   1. 启动 MCC 并打开 TrustZone 配置窗口。
   2. 在 **Plugins**（插件）项目列表中，选择应用程序的安全区域和非安全区域的 **Peripheral Configuration**（外设配置）。
   3. 选中 **SERCOM3** 和 **DMAC** 框作为非安全外设。选中后，框的颜色将从绿色变为橙色。

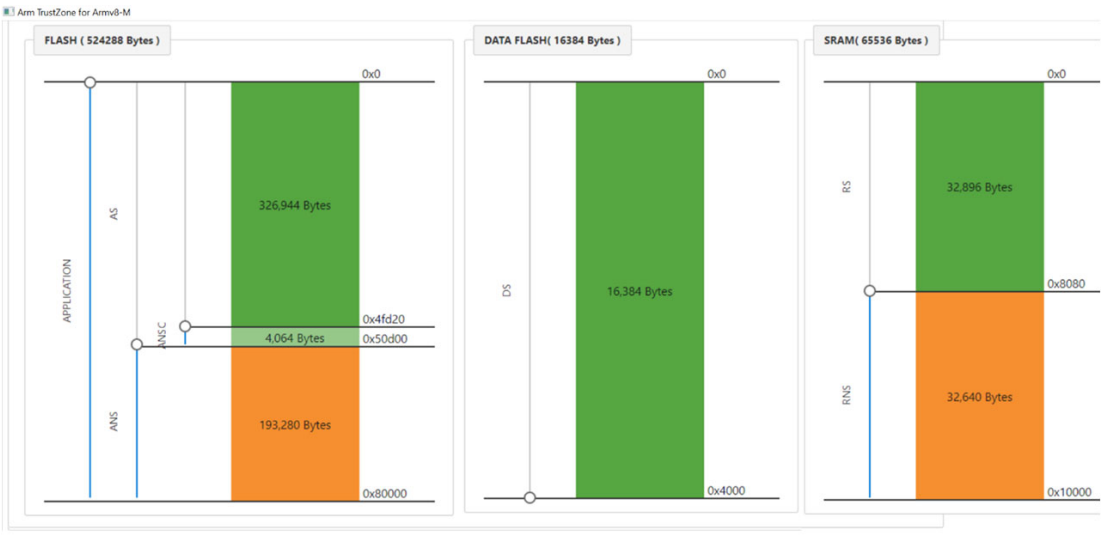
**图 4-4.** MPLAB®代码配置器——Arm® TrustZone® for Armv8-M（Armv8-M 的 Arm TrustZone）外设配置




**注：**SERCOM3 和 DMA 外设配置为非安全，它们通过 NSC（非安全可调用）API 从安全应用程序获取 LED 切换速率和温度读数，以便将 LED 切换速率打印在 PC 上运行的串行控制台上。

5. 可根据应用程序的要求将存储器配置为安全或非安全。
   a. 启动 MCC 并打开 TrustZone 配置窗口。
   b. 在 **Plugins** 项目列表中，选择应用程序的安全区域和非安全区域的 **Memory Configuration**（存储器配置）。

**图 4-5.** MCC——Armv8 的 TrustZone——存储器配置




可根据需要使用以下标记来配置存储器。闪存区域（512 KB）可划分为以下区域：

**AS：**放置安全应用程序的区域。

**ANS：**放置非安全应用程序的区域。

**ANSC**：放置非安全可调用函数（用于在安全应用程序与非安全应用程序之间建立通信的函数）的区域。

## 流程图

**图 4-6.** 安全应用程序流程图 1

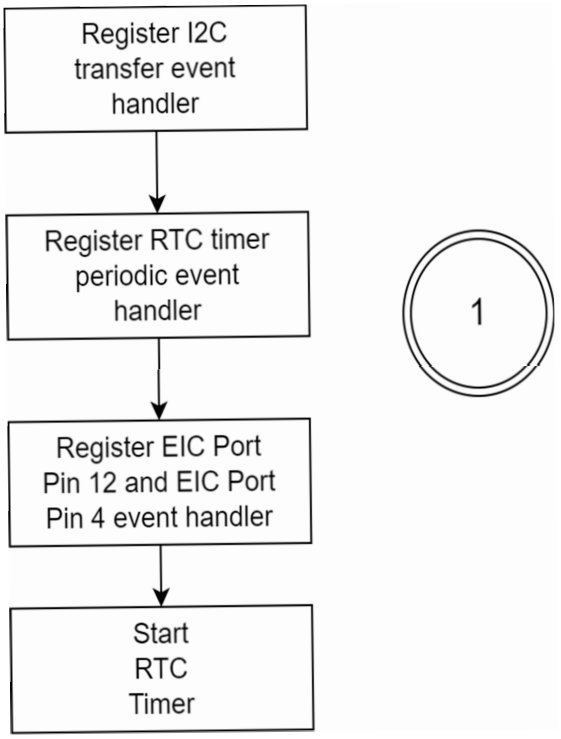


**图 4-7.** 安全应用程序流程图 2

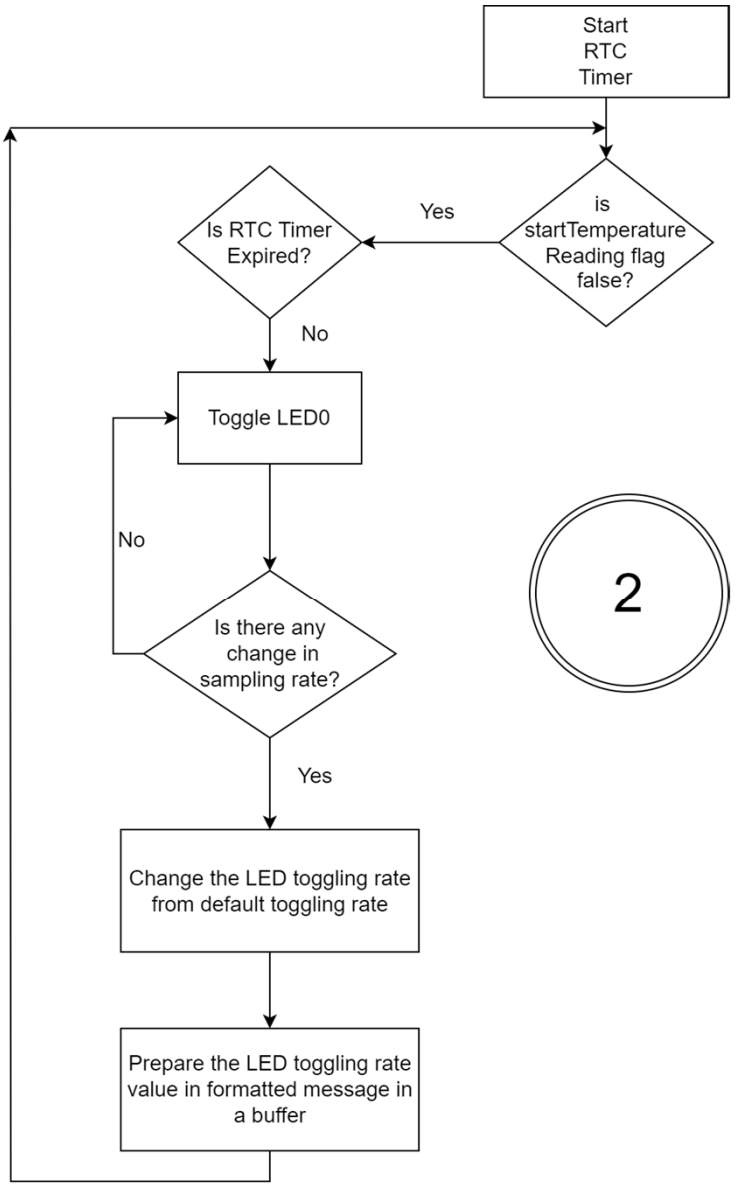


**图 4-8.** 安全应用程序流程图 3

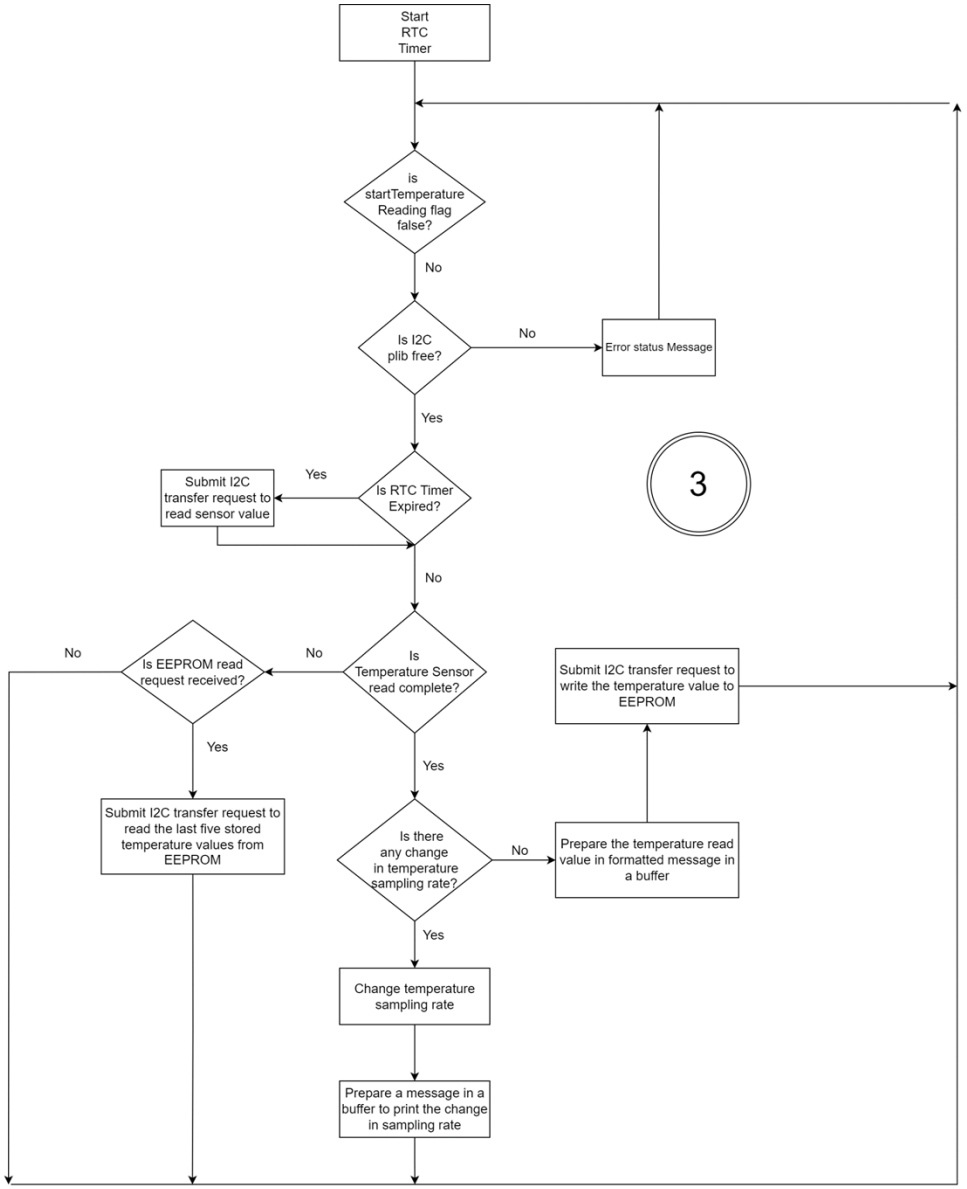


**图 4-9.** 安全应用程序流程图 4

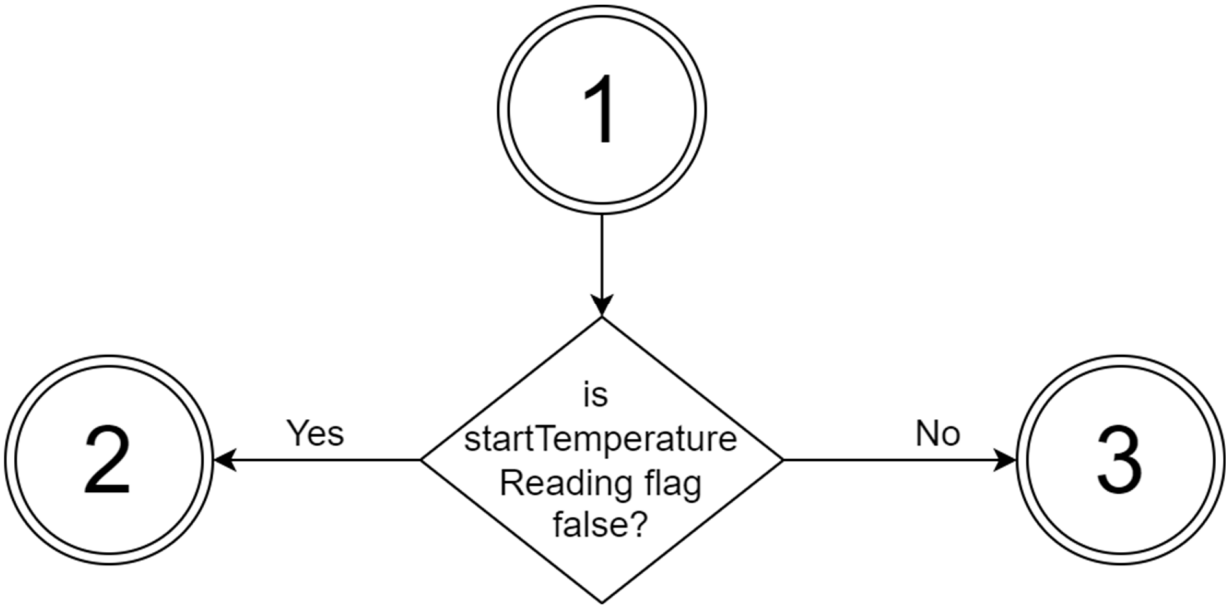
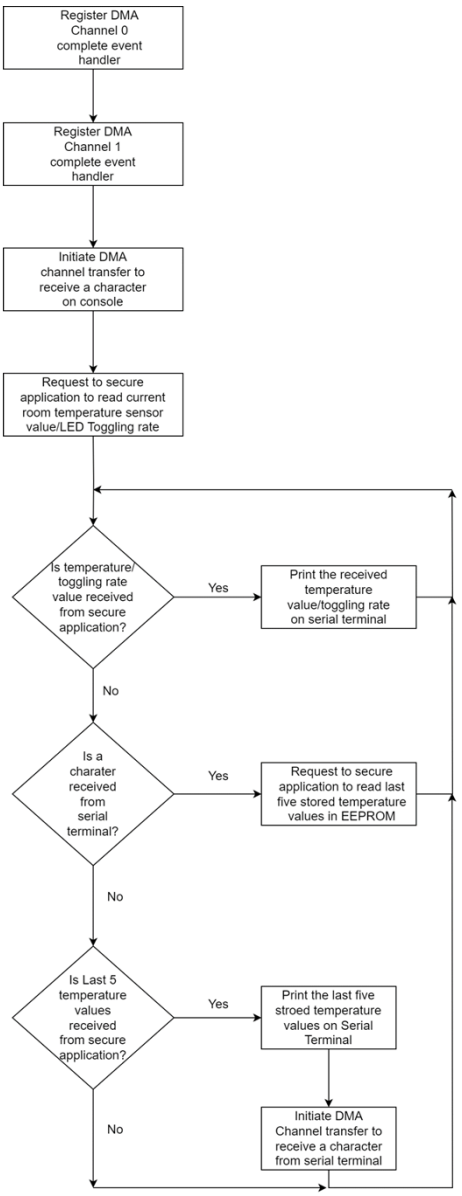


**图 4-10.** 非安全应用程序流程图




## 实现

MCC 为安全和非安全项目组件提供了预先编写的代码模板。在安全项目的 TrustZone 文件夹中，`nonsecure_entry.c` 文件包含非安全可调用（NSC）函数的实现。这些函数充当“桥梁”，允许非安全项目访问存储在安全项目中的数据。Cortex-M 安全扩展（CMSE）属性用于在安全项目代码中标识这些 NSC 函数。在安全项目的 `main.c` 文件中，一个名为 `secureApp()` 的函数持续管理 LED 切换和温度传感器读数。MCC 可能将该函数调用置于循环内以实现持续执行。非安全应用程序依赖名为 `SecureApp_Entry()` 的 NSC 函数。该函数用于访问安全数据，具体通过在自身内部调用安全项目中的 `secureApp()` 函数来实现。最后，非安全应用程序利用 DMA 通道和 SERCOM3 外设在连接到 PC 的串行控制台上打印获取的数据。

**图 4-11.** NSC 函数原型与实现

```
void __attribute__((cmse_nonsecure_entry)) secureAppEntry(void)
{
    secureApp();
}
```

### 以打印机和墨盒为例进行说明

打印机和墨盒用例可使用 TrustZone 技术来保护其固件和关键操作。打印机将身份验证令牌和固件代码等敏感信息存储在安全存储区中。该安全区域完全隔离，常规打印应用程序或连接到打印机的任何不受信任的外设都无法访问。任何未经授权的函数试图访问安全区域内的敏感操作（如 LED 切换或温度读取）都会触发安全异常（类似于硬故障异常），从而阻止未经授权的访问。

想象一下打印机墨盒中包含类似于固件代码的身份验证数据。插入墨盒后，只有墨盒包含特殊的非安全可调用（NSC）函数时才能与打印机的固件进行交互。这些 NSC 函数充当安全网关，其中第一条指令是全局安全（Secure Global，SG）指令，允许非安全墨盒与安全打印机固件之间进行受控的通信。缺少 NSC 函数的墨盒无法与安全区域进行交互，任何绕过 NSC 网关的尝试都将失败，从而阻止未经授权的访问。

TrustZone 技术主要有两个优点：将敏感数据隔离在安全存储器中并要求通过 NSC 函数进行身份验证。首先，该技术充当一种反克隆措施，防止未经授权复制打印机的固件或绕过安全措施。其次，通过控制对安全操作的访问确保公司数据的安全。只有包含有效 NSC 函数的经授权墨盒才能与打印机进行交互，从而保护打印作业或网络配置等关键信息免遭未经授权的访问。

从本质上讲，以安全打印机为例对 TrustZone 进行说明展示了安全存储器分区和通过 NSC 函数进行受控通信如何增强器件的安全性。

## 4.2 使用 ATECC608B 安全元件

在打印机和墨盒用例中，PIC32CM LS60 MCU 上的安全元件 ATECC608B 可在身份验证过程中添加一层额外的安全保护，有助于防止器件遭到克隆。ATECC608B 是一种专用的硬件组件，可在安全环境中存储敏感数据并执行加密操作。

#### 身份验证方法

以下方法利用加密技术建立安全通信并验证设备标识，最终防止未经授权的克隆企图。

**对称身份验证：**对称身份验证使用质询和响应过程。在对称身份验证中，PIC32CM LS60 MCU 主机质询远程设备以确保设备可靠并且可以信任设备。受到质询的设备将使用预期结果响应。该方法要求主机和远程设备共享相同的密钥。此外，远程设备可以发送惟一序列号，因此响应与其他远程设备不同。

**非对称身份验证：**在非对称身份验证中，验证者通过验证签名来核实远程设备的真实性。非对称身份验证以利用两个密钥为基础。

- 其中一个密钥需要保密。该密钥称为私钥。
- 第二个密钥在数学上与私钥相关，称为公钥。

公钥是公开共享的。密钥所有者将使用公钥来验证签名。主机向远程设备发送随机质询。远程设备以签名响应。但是，主机只需要来自远程设备的公钥（而非保密密钥）来验证用于响应质询的签名。如果签名验证匹配，则远程设备已成功响应质询，并且主机可以信任远程设备。

正品打印机墨盒内的 ATECC608B 安全元件有助于使用质询-响应协议实现对称安全身份验证。

**用于安全标识的惟一密钥**——每个正品墨盒均内置 ATECC608B 安全元件。在制造过程中，每个墨盒内置的该安全元件中都会安全地编入一个惟一的加密密钥。

#### 质询响应协议实际应用

开机或插入墨盒——当打印机开机或插入新墨盒时，打印机会启动与墨盒的 ATECC608B 的通信过程。

发出质询——打印机向墨盒发送质询。该质询通常为随机数。

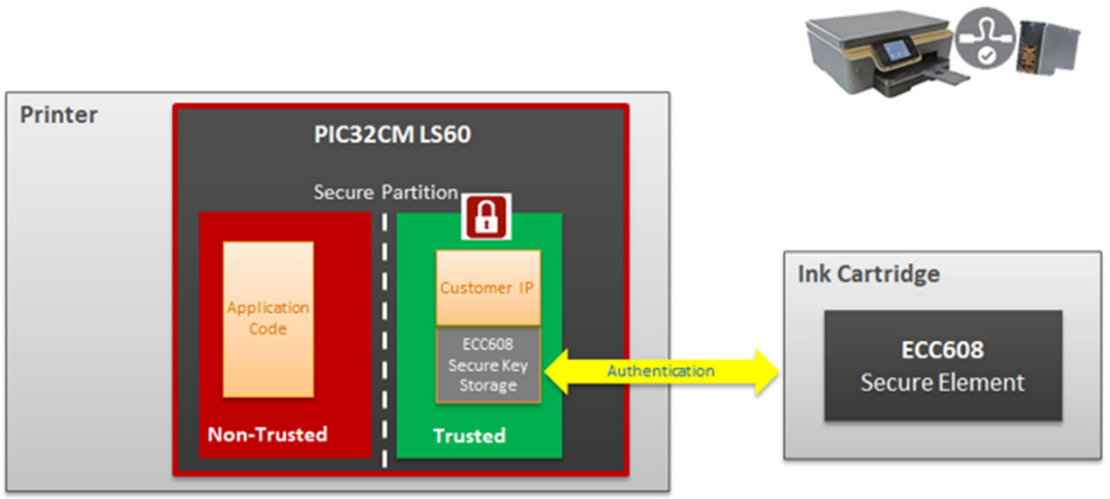
**来自墨盒的安全响应**——墨盒的 ATECC608B 接收质询。ATECC608B 使用其惟一密钥来安全地解密质询，然后对质询执行加密操作（计算报文身份验证代码（MAC））并将该响应（MAC）发送回打印机。

**验证和决策**——打印机接收来自墨盒的响应（MAC）。打印机使用预定义的算法和原始质询来验证收到的 MAC。

成功——如果计算出的 MAC 值与接收到的 MAC 值匹配，则说明墨盒为正品，打印机可以开始打印。

失败——如果两个 MAC 值不匹配，则打印机将墨盒标识为假冒伪劣产品。打印机可能会拒绝打印或显示警告消息，具体取决于打印机的设置。

**图 4-12.** PIC32CM LS60 上的打印机墨盒身份验证用例




### 4.2.1 ATECC608B 示例程序

**安全 IoT 网关应用概述：**

该应用演示了 PIC32CM LS60 单片机（MCU）上的反克隆功能。最初，主机应用程序启动与其连接的客户端的对称身份验证过程。此外，主机还连接到 AWS IoT 云。PIC32CM LS60 MCU 主机将与 PIC32CM LS60 客户端 MCU 成功建立连接，因为 ATECC608B 安全元件将确保成功完成身份验证过程。主机随后将接收传感器数据并将其显示在 MIKROE OLED C Click board™上，同时还会将该数据发布到 AWS 云。但是，由于 PIC32CM LE00 客户端没有内置 ATECC608B，因此将无法完成身份验证过程。如果身份验证失败，数据将不会在主机端显示，也不会发布到云端。

#### 4.2.1.1 身份验证序列

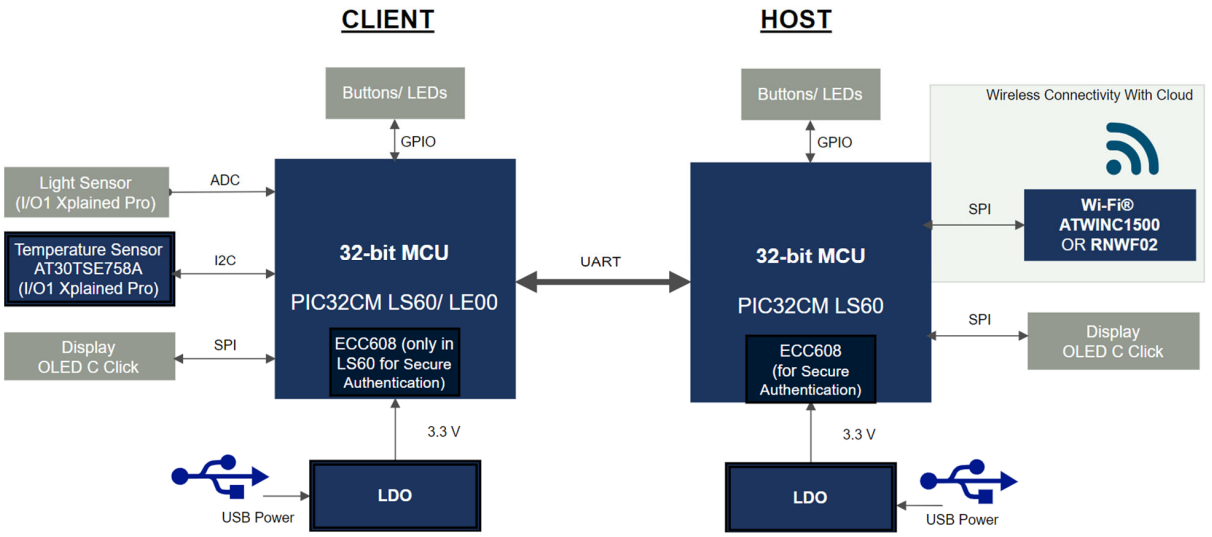
验证从 PIC32CM LS60 MCU 主机请求远程设备（客户端）的序列号开始。主机发送一个随机数，此随机数预期远程设备使用共享机密信息密钥进行哈希运算。该过程称为*质询*，因为它质询远程设备来提供正确的答案。

远程设备使用共享密钥和惟一序列号对随机数进行哈希运算，然后发回最终生成的哈希输出，称为报文身份验证代码（MAC）。主机通过重复相同的操作来检查返回的 MAC。它使用随机数和远程设备的惟一序列号对共享密钥进行哈希运算。主机比较两个结果。如果结果匹配，则表示远程设备已成功响应质询，主机可以信任外部设备。如果远程设备也是 PIC32CM LS60 MCU，就属于这种情况。

如果远程设备是 PIC32CM LE00（未内置 ATECC608B），则身份验证将失败。

此外，主机还连接到 AWS IoT 云。当按下主机上的 SW0 按钮时，会立即将内置 ATECC608B 生成的随机数通过 USART 引脚发送到客户端，然后等待结果。一旦客户端通过身份验证，主机便可接收传感器数据并将其显示在 MIKROE OLED C Click 板上。此外，该数据也会定期发布到 AWS IoT Core。每次将数据发布到云端时，都会切换主机上的 LED0。

**图 4-13.** 身份验证框图




## AWS 帐户设置

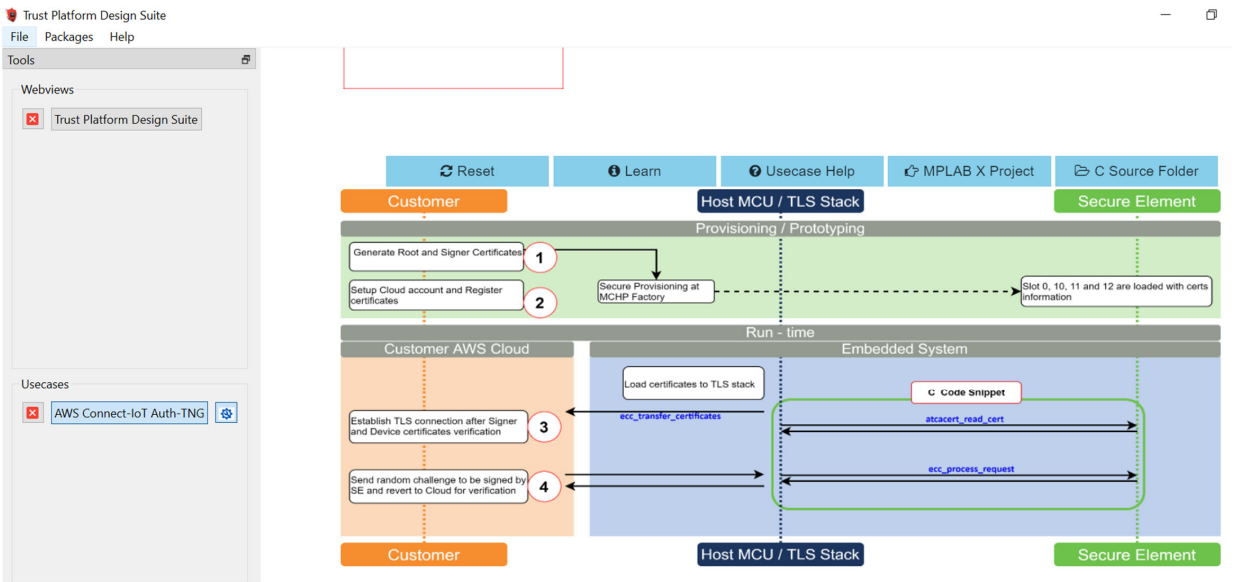
为了运行该应用，需要一个 Amazon Web Services（AWS）帐户。有关创建 AWS 帐户的更多信息和步骤，请参见 readme.md。

## AWS 云 IoT 配置

借助 Microchip 可信平台设计套件（Trust Platform Design Suite，TPDS）工具，可以使用 AWS 云平台来配置器件（ECC608B 安全元件）。

在 TPDS 中，按照 readme.md 中的 *AWS 云 IoT 配置指南*部分提及的步骤启动 AWS IoT 身份验证用例并执行配置。

**图 4-14.** 可信平台设计套件——AWS IoT 身份验证用例事务图



### 4.2.1.2 配置

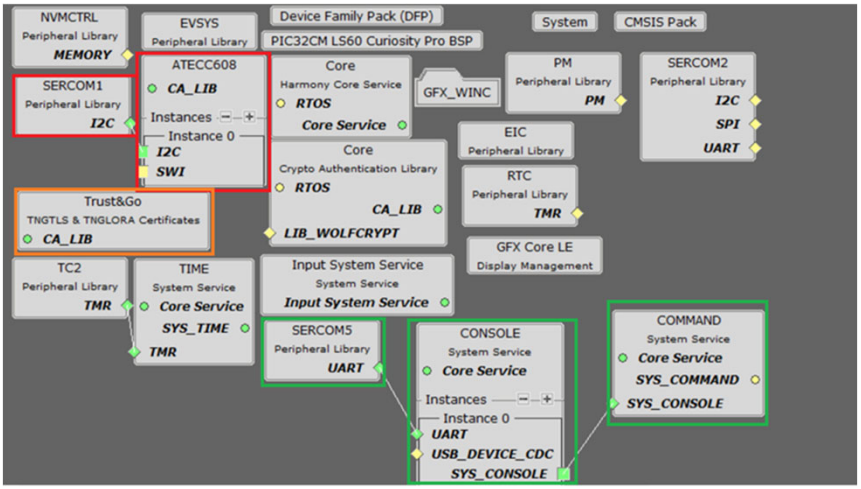
#### 主机

在下图所示的项目图窗口中，用红框标示的模块为 ATECC608B 安全元件配置，CA_LIB 表示 CryptoAuth 库。SERCOM1 配置为 $I^2C$，用于将数据写入 ATECC608B 元件的槽。

用绿框标示的 SYS_CONSOLE 配置有助于简化通信，建立 Wi-Fi 连接。SYS_CONSOLE 用于实现控制台打印，它允许用户输入命令通过 CLI 建立 Wi-Fi 连接，并将 SERCOM 5 配置为 UART 来实现该通信。

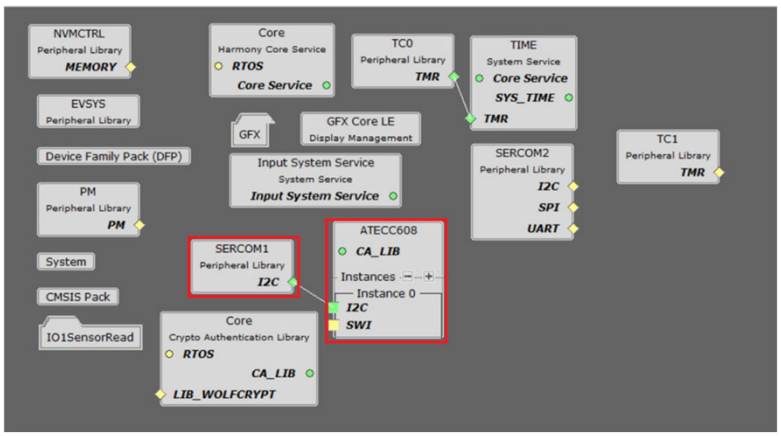
用橙框标示的模块用于 TrustZone 配置，可启用 TrustFLEX 证书。

**图 4-15.** 主机 MCU 的项目图



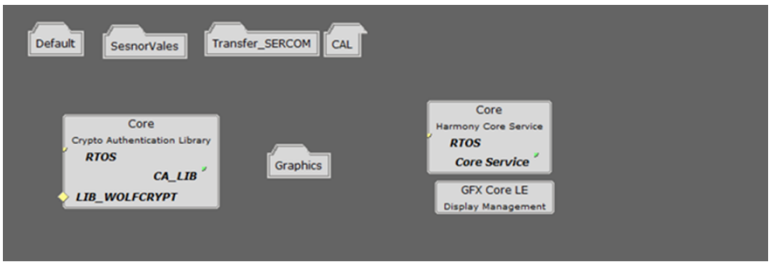

#### 客户端

**图 4-16.** 真实客户端的项目图配置




真实客户端的配置与主机配置类似，但它没有将 Trust&Go 模块添加到项目图中，因为它不需要连接到云或与云之间验证证书。

**图 4-17.** 不良客户端的项目图配置




不良客户端没有 ATECC608B 安全元件，因此项目图中不存在 ATECC608B 模块。由于没有 ATECC608 安全元件，因此无法响应主机发送的质询，导致身份验证失败。

## 流程图——主机

**图 4-18.** 主机初始化流程图

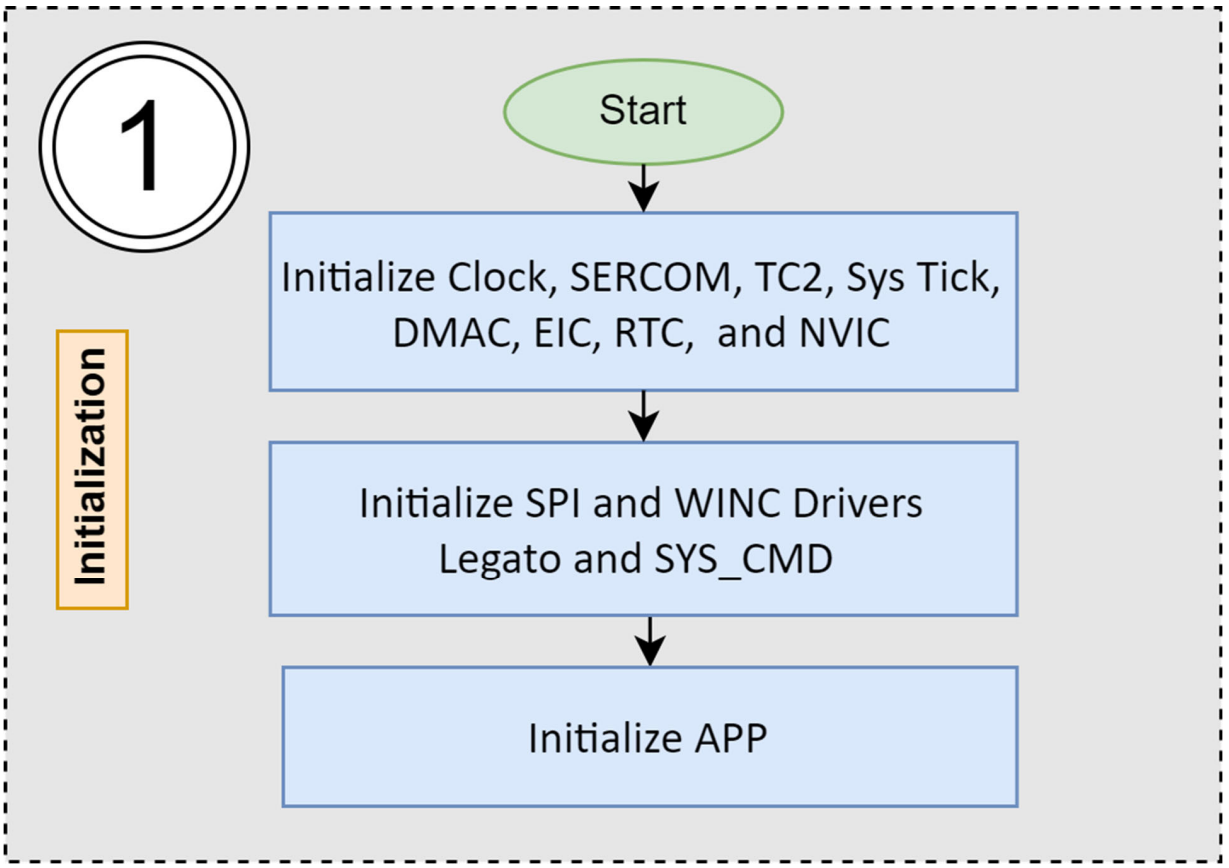


**图 4-19.** 主机云连接流程图

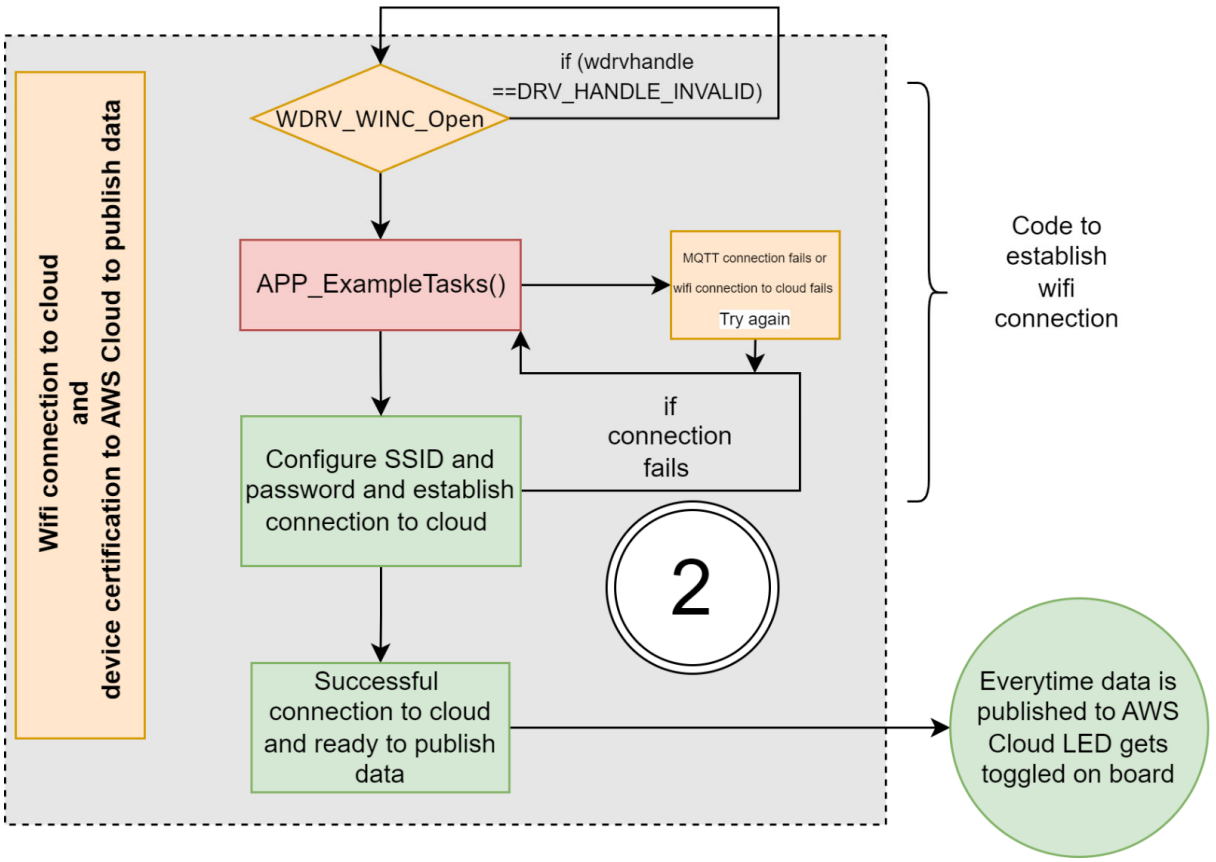
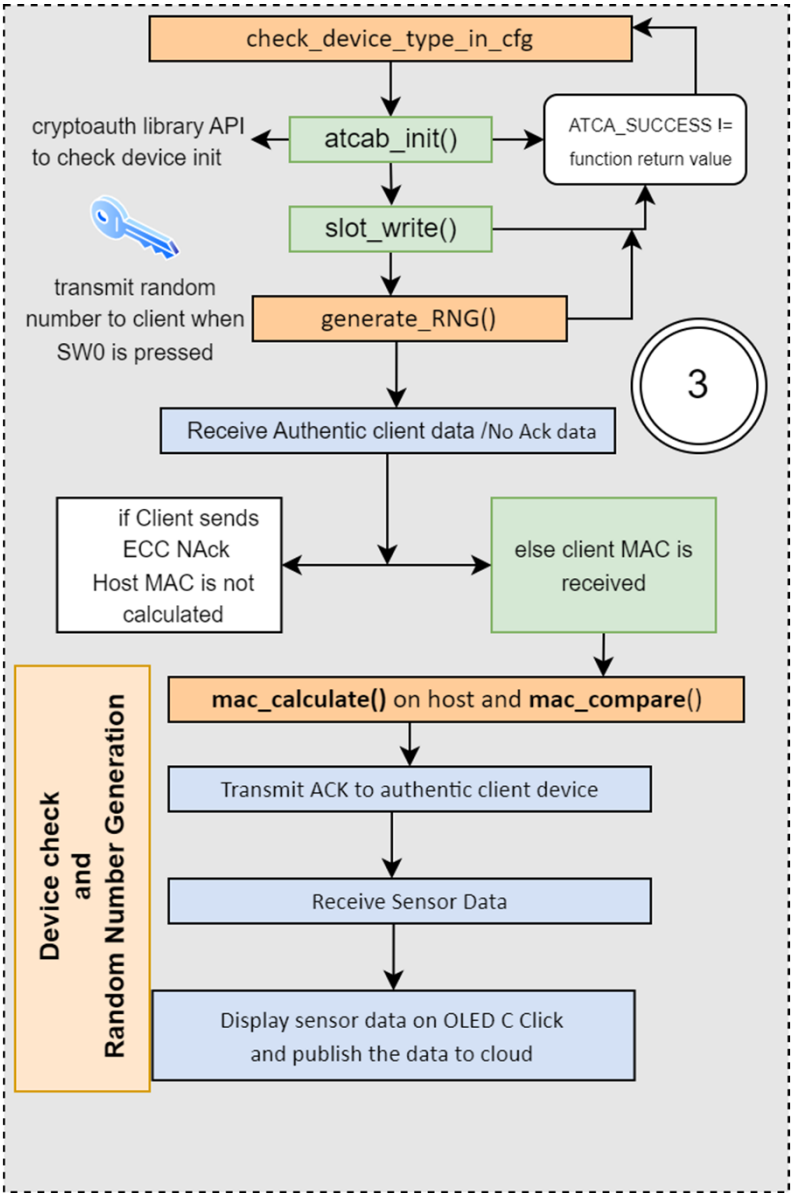


**图 4-20.** 主机身份验证初始化流程图




**slot_write()** 用于检查是否正确写入槽 5 中的机密信息密钥和槽 6 中的 I/O 保护密钥。ATECC608B 安全元件中的槽是存储密钥的数据区域。

**注：** 在对称身份验证的情况下，槽 5 专门用于存储主机与客户端之间共享的机密信息密钥。

槽 6 中的 I/O 保护密钥用于确保主机与客户端之间安全进行数据传输。

## 流程图——客户端

**图 4-21.** 客户端系统初始化应用程序流程图

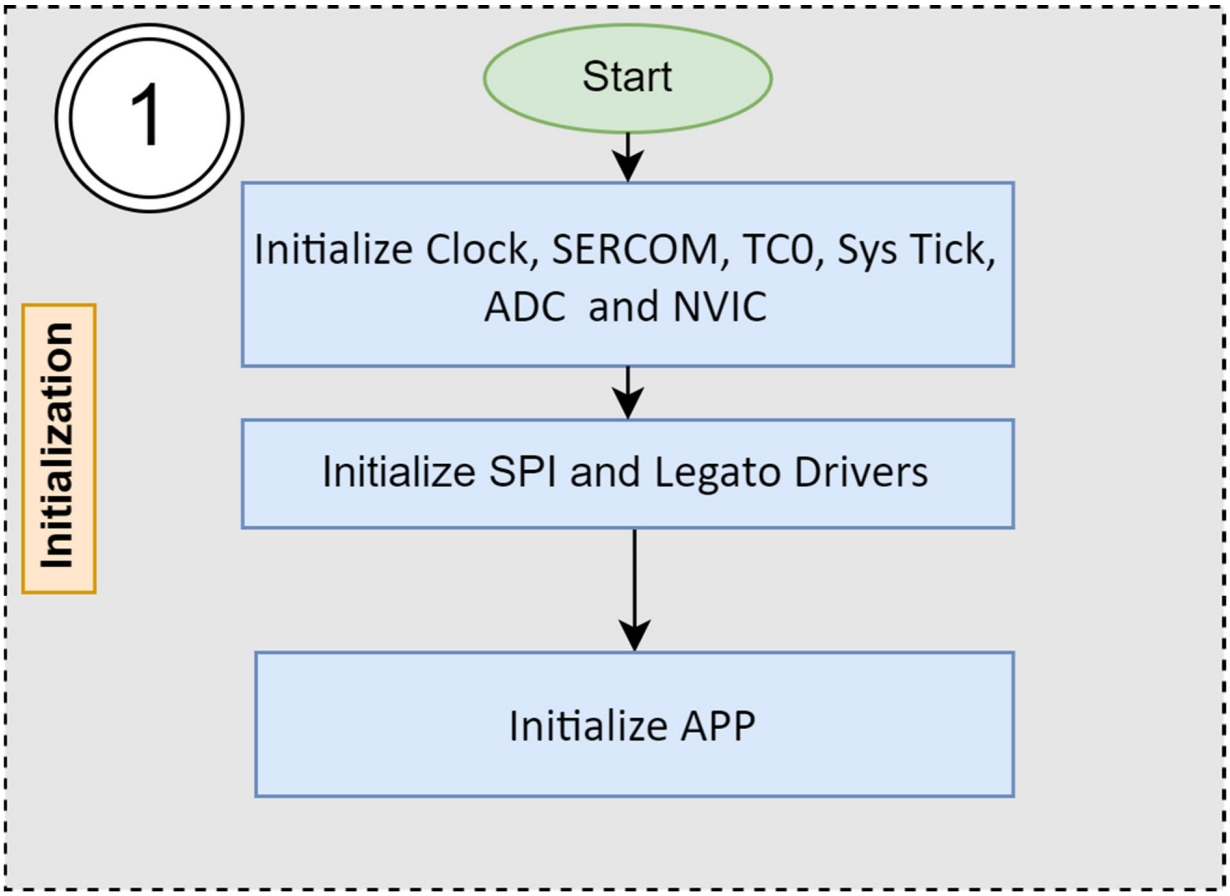



**图 4-22.** 客户端应用程序流程图

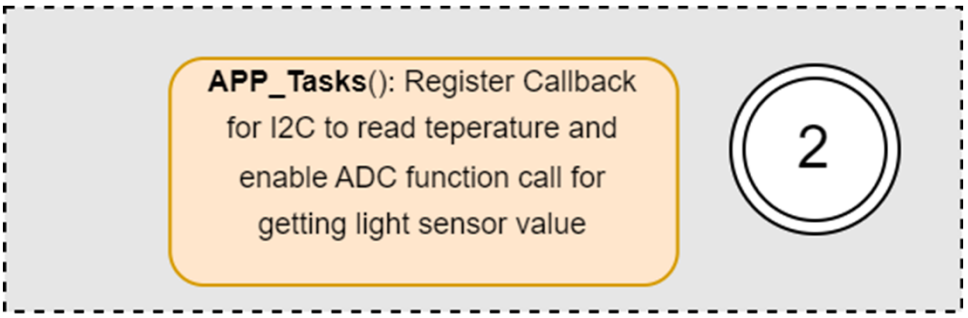


**图 4-23.** 客户端应用程序总体流程图

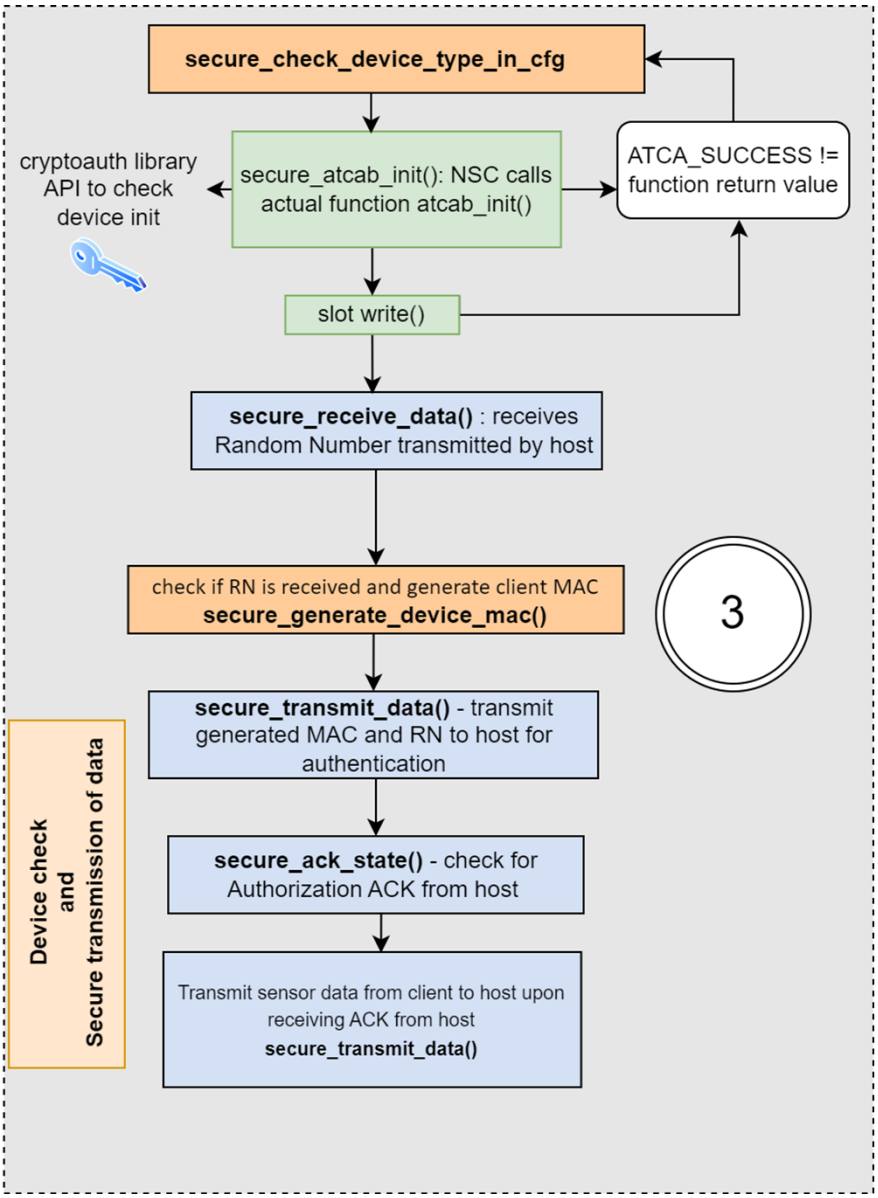
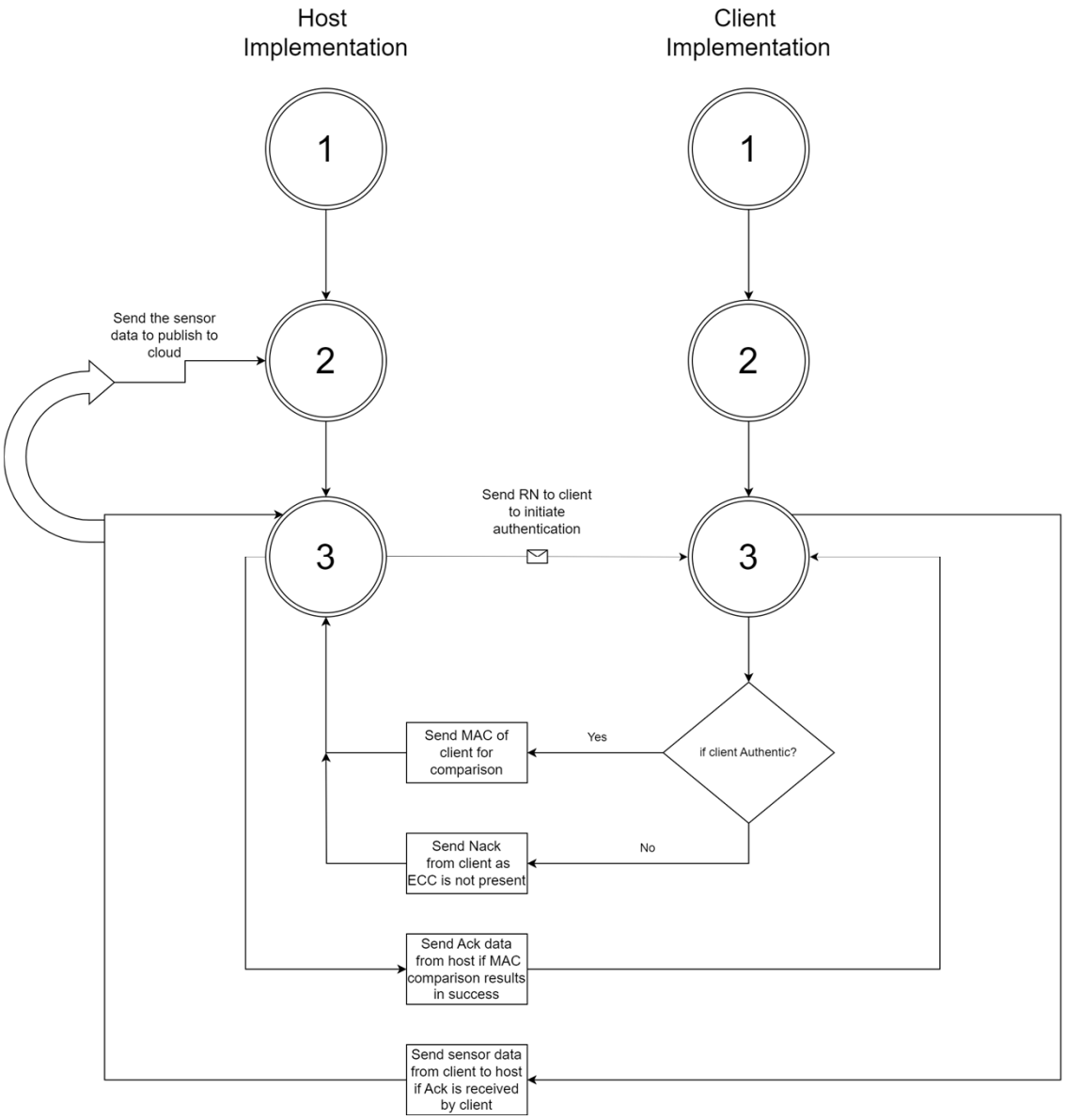


**图 4-24.** 身份验证过程




## 实现

该应用程序使用 CryptoAuth 库 API 实现主机和客户端之间的对称身份验证。`ATCA_STATUS atcab_init(ATCAIfaceCfg* cfg)` 用于创建供基本 API 使用的全局 ATCA 设备对象。

成功时返回 ATCA_SUCCESS，失败时返回错误代码。`check_device_type_in_cfg()` 借此来获取设备详细信息并初始化设备上的加密操作。

`ATCA_STATUS atcab_info(uint8_t_revision )` 使用 Info 命令获取设备版本（DevRev）。

`ATCA_STATUS atcab_read_serial_number (uint8_t_serial_number)` 在应用程序中用于返回设备的 9 字节序列号。

`ATCADeviceType get_device_type_id(uint8_t_revision_byte)` 用于检查芯片上内置的安全器件的类型，例如 ATECC608B 或 ATECC508A。

**主机项目的 API 和函数：**

`uint8_t slot_write(uint8_t slot_num)`：将数据写入 ATECC608B 安全元件的数据区域槽。

`uint8_t generate_RNG()`：在主机端生成一个随机数并发送给客户端。

`uint8_t calculate_host_mac(void)`：计算主机的 MAC。

`ATCA_STATUS mac_compare(void)`：将从客户端收到的 MAC 与主机端生成的 MAC 进行比较。

**客户端项目的 API 和函数：**

`secure_generate_device_mac()`：生成客户端的设备 MAC。

`secure_pass_sensor_data()`：如果客户端是真实的，则将传感器数据发送到主机。

`secure_transmit_data()`：将生成的 MAC 和 RNG（32 字节）发送到主机以进行身份验证。

`secure_receive_data()`：接收随机数以进行 MAC 计算。

`secure_receive_state()`：检查是否收到随机数。

## 以打印机和墨盒为例进行说明

打印机和墨盒公司面临的一项重大挑战是假冒伪劣产品。我们探讨一下对称身份验证如何保护这些设备并确保使用的墨盒是正品。

在本例中，打印机充当主机 MCU（PIC32CM LS60 Curiosity Pro），正品墨盒是客户端（LS60）。插入新墨盒时，打印机启动身份验证。打印机向墨盒发送一个随机数质询。

墨盒的安全元件 ATECC608B 验证其真实性。该安全元件通过使用共享机密信息密钥和墨盒的惟一序列号对随机数进行哈希运算，以计算出报文身份验证代码（MAC）。打印机的 ATECC608B 执行相同的计算，以生成自己的 MAC。

之后，打印机将从墨盒收到的 MAC 与其自己计算出的 MAC 进行比较。如果两个 MAC 匹配，则认为该墨盒是正品（由该公司生产，在本例中为 LS60），打印机随后开始打印。如果两个 MAC 不匹配，则身份验证失败，表明墨盒是假冒伪劣产品，打印机拒绝打印。

# 5. 结论

通过利用 ATECC608B 的安全存储和加密功能，可以高度安全的方式实现对称身份验证协议，从而有效防止器件遭到克隆并确保通信的完整性。

TrustZone 技术在防止器件遭到克隆方面发挥着至关重要的作用，该技术通过建立安全的执行环境使各种过程（例如，保护需要高安全性的敏感数据）不受普通区域的干扰，从而确保安全通信并增强器件对篡改和攻击的抵抗力。*普通区域*不经过安全网关就无法直接访问安全区域。这提供了一层额外的安全保护，有效防止器件遭到克隆。

# 6. 参考资料

有关 Microchip 产品和服务的更多信息，请访问 Microchip 网站或联系当地的销售代表。

- PIC32CM LS60 Curiosity Pro 评估工具包
- PIC32CM LE00 Curiosity Pro 评估工具包
  有关本应用笔记中提及的应用程序演示，可单击以下链接进行下载：
- PIC32CM LS60 Curiosity Pro 评估工具包上的 TrustZone 应用程序
- PIC32CM LS60 Curiosity Pro 评估工具包上的安全 IoT 网关应用程序
  有关应用的更多信息，请参见：
  - PIC32CM LS60 Curiosity Pro 评估工具包上的安全 IoT 网关
  - PIC32CM LS60 Curiosity Pro 评估工具包上的 TrustZone 入门
- PIC32CM LS60/LS00 安全参考指南
- 有关各种应用的更多信息，请参见 GitHub 上的 reference_apps 资源库
- 有关 32 位单片机资料和解决方案的更多信息，请参见：
  32 位单片机相关资料和解决方案参考指南

# 7. 版本历史

**版本 A——2024 年 9 月**

本文档的初始版本。

# Microchip 信息

## Microchip 网站

Microchip 网站（www.microchip.com）为客户提供在线支持。客户可通过该网站方便地获取文件和信息。我们的网站提供以下内容：

- **产品支持**——数据手册和勘误表、应用笔记和示例程序、设计资源、用户指南以及硬件支持文档、最新的软件版本以及归档软件
- **一般技术支持**——常见问题解答（FAQ）、技术支持请求、在线讨论组以及 Microchip 设计伙伴计划成员名单
- **Microchip 业务**——产品选型和订购指南、最新 Microchip 新闻稿、研讨会和活动安排表、Microchip 销售办事处、代理商以及工厂代表列表

## 产品变更通知服务

Microchip 的产品变更通知服务有助于客户了解 Microchip 产品的最新信息。注册客户可在他们感兴趣的某个产品系列或开发工具发生变更、更新、发布新版本或勘误表时，收到电子邮件通知。

欲注册，请访问 www.microchip.com/pcn，然后按照注册说明进行操作。

## 客户支持

Microchip 产品的用户可通过以下渠道获得帮助：

- 代理商或代表
- 当地销售办事处
- 应用工程师（ESE）
- 技术支持

客户应联系其代理商、代表或 ESE 寻求支持。当地销售办事处也可为客户提供帮助。本文档后附有销售办事处的联系方式。

也可通过 www.microchip.com/support 获得网上技术支持。

## Microchip 器件代码保护功能

请注意以下有关 Microchip 产品代码保护功能的要点：

- Microchip 的产品均达到 Microchip 数据手册中所述的技术规范。
- Microchip 确信：在正常使用且符合工作规范的情况下，Microchip 系列产品非常安全。
- Microchip 注重并积极保护其知识产权。严禁任何试图破坏 Microchip 产品代码保护功能的行为，这种行为可能会违反《数字千年版权法案》（Digital Millennium Copyright Act）。
- Microchip 或任何其他半导体厂商均无法保证其代码的安全性。代码保护并不意味着我们保证产品是“牢不可破”的。代码保护功能处于持续发展中。Microchip 承诺将不断改进产品的代码保护功能。

## 法律声明

提供本文档的中文版本仅为了便于理解。请勿忽视文档中包含的英文部分，因为其中提供了有关 Microchip 产品性能和使用情况的有用信息。Microchip Technology Inc.及其分公司和相关公司、各级主管与员工及事务代理机构对译文中可能存在的任何差错不承担任何责任。建议参考 Microchip Technology Inc.的英文原版文档。

本出版物及其提供的信息仅适用于 Microchip 产品，包括设计、测试以及将 Microchip 产品集成到您的应用中。以其他任何方式使用这些信息都将被视为违反条款。本出版物中的器件应用信息仅为您提供便利，将来可能会发生更新。如需额外的支持，请联系当地的 Microchip 销售办事处，或访问 www.microchip.com/en-us/support/design-help/client-support-services。

## 商标



ISBN： 979-8-3371-0101-9

## 质量管理体系

有关 Microchip 质量管理体系的信息，请访问 www.microchip.com/quality。

# 全球销售及服务网点


**美洲**

**公司总部**
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
电话：480-792-7200
传真：480-792-7277
技术支持：
www.microchip.com/support
网址：
www.microchip.com

**亚特兰大**
德卢斯，佐治亚州
电话：678-957-9614
传真：678-957-1455

**奥斯汀，德克萨斯州**
电话：512-257-3370

**波士顿**
韦斯特伯鲁，马萨诸塞州
电话：774-760-0087
传真：774-760-0088

**芝加哥**
艾塔斯卡，伊利诺伊州
电话：630-285-0071
传真：630-285-0075

**达拉斯**
阿迪森，德克萨斯州
电话：972-818-7423
传真：972-818-2924

**底特律**
诺维，密歇根州
电话：248-848-4000

**休斯顿，德克萨斯州**
电话：281-894-5983

**印第安纳波利斯**
诺布尔斯维尔，印第安纳州
电话：317-773-8323
传真：317-773-5453
电话：317-536-2380

**洛杉矶**
米慎维荷，加利福尼亚州
电话：949-462-9523
传真：949-462-9608
电话：951-273-7800

**罗利，北卡罗来纳州**
电话：919-844-7510

**纽约，纽约州**
电话：631-435-6000

**圣何塞，加利福尼亚州**
电话：408-735-9110
电话：408-436-4270

**加拿大 - 多伦多**
电话：905-695-1980
传真：905-695-2078

**亚太地区**

**澳大利亚 - 悉尼**
电话：61-2-9868-6733

**中国 - 北京**
电话：86-10-8569-7000

**中国 - 成都**
电话：86-28-8665-5511

**中国 - 重庆**
电话：86-23-8980-9588

**中国 - 东莞**
电话：86-769-8702-9880

**中国 - 广州**
电话：86-20-8755-8029

**中国 - 杭州**
电话：86-571-8792-8115

**中国 - 香港特别行政区**
电话：852-2943-5100

**中国 - 南京**
电话：86-25-8473-2460

**中国 - 青岛**
电话：86-532-8502-7355

**中国 - 上海**
电话：86-21-3326-8000

**中国 - 沈阳**
电话：86-24-2334-2829

**中国 - 深圳**
电话：86-755-8864-2200

**中国 - 苏州**
电话：86-186-6233-1526

**中国 - 武汉**
电话：86-27-5980-5300

**中国 - 西安**
电话：86-29-8833-7252

**中国 - 厦门**
电话：86-592-2388138

**中国 - 珠海**
电话：86-756-3210040

**亚太地区**

**印度 - 班加罗尔**
电话：91-80-3090-4444

**印度 - 新德里**
电话：91-11-4160-8631

**印度 - 浦那**
电话：91-20-4121-0141

**日本 - 大阪**
电话：81-6-6152-7160

**日本 - 东京**
电话：81-3-6880-3770

**韩国 - 大邱**
电话：82-53-744-4301

**韩国 - 首尔**
电话：82-2-554-7200

**马来西亚 - 吉隆坡**
电话：60-3-7651-7906

**马来西亚 - 槟榔屿**
电话：60-4-227-8870

**菲律宾 - 马尼拉**
电话：63-2-634-9065

**新加坡**
电话：65-6334-8870

**台湾地区 - 新竹**
电话：886-3-577-8366

**台湾地区 - 高雄**
电话：886-7-213-7830

**台湾地区 - 台北**
电话：886-2-2508-8600

**泰国 - 曼谷**
电话：66-2-694-1351

**越南 - 胡志明市**
电话：84-28-5448-2100

**欧洲**

**奥地利 - 韦尔斯**
电话：43-7242-2244-39
传真：43-7242-2244-393

**丹麦 - 哥本哈根**
电话：45-4485-5910
传真：45-4485-2829

**芬兰 - 埃斯波**
电话：358-9-4520-820

**法国 - 巴黎**
电话：33-1-69-53-63-20
传真：33-1-69-30-90-79

**德国 - 加兴**
电话：49-8931-9700

**德国 - 哈恩**
电话：49-2129-3766400

**德国 - 海尔布隆**
电话：49-7131-72400

**德国 - 卡尔斯鲁厄**
电话：49-721-625370

**德国 - 慕尼黑**
电话：49-89-627-144-0
传真：49-89-627-144-44

**德国 - 罗森海姆**
电话：49-8031-354-560

**以色列 - 霍德夏沙隆**
电话：972-9-775-5100

**意大利 - 米兰**
电话：39-0331-742611
传真：39-0331-466781

**意大利 - 帕多瓦**
电话：39-049-7625286

**荷兰 - 德卢内市**
电话：31-416-690399
传真：31-416-690340

**挪威 - 特隆赫姆**
电话：47-72884388

**波兰 - 华沙**
电话：48-22-3325737

**罗马尼亚 - 布加勒斯特**
电话：40-21-407-87-50

**西班牙 - 马德里**
电话：34-91-708-08-90
传真：34-91-708-08-91

**瑞典 - 哥德堡**
电话：46-31-704-60-40

**瑞典 - 斯德哥尔摩**
电话：46-8-5090-4654

**英国 - 沃金厄姆**
电话：44-118-921-5800
传真：44-118-921-5820