AN2591

ATECC608A安全引导入门用例

作者： *Kalyan C. Manukonda*
Microchip Technology Inc.

简介

Microchip ATECC608A器件属于CryptoAuthentication™系列高安全性加密器件，它将世界一流的基于硬件的密钥存储与硬件加密加速器相结合，以实现各种身份验证和加密协议。ATECC608A提供了一种机制来支持联网单片机（MCU）中的安全引导操作，这有助于识别主机中央处理单元（Central Processing Unit，CPU）上是否安装了欺诈代码。

CryptoAuthLib是一套适用于ATSHA204A、ATEC108A、ATECC508A和ATECC608A CryptoAuthentication器件的软件支持库（采用C语言编写）。这套软件支持库可移植、可扩展、功能强大且易于使用，适用于ATSHA和ATECC系列器件。

SAM Boot Assistant（SAM-BA®应用程序）允许使用USB或UART主机进行系统内编程（In-system Programming，ISP），而无需任何外部编程接口。

本应用笔记将使用SAM-BA应用程序来演示ATECC608A安全引导功能的一个实现示例。在本演示中，SAMD21器件将作为目标器件，其中包含SAM-BA监视器作为自举程序。在执行用户应用程序之前，自举程序会事先使用CryptoAuthLib对其执行验证。

包含内容

示例应用程序包含：

- SAM-BA监视器应用程序
- 用户应用程序示例
- 用于为用户应用程序生成公钥和签名的Python脚本
- 针对SAM-BA软件更新的小程序和二进制文件

硬件和软件要求

为了执行ATECC608A安全引导功能演示，必须满足以下硬件（图5）和软件要求。

硬件准备工作：

- SAMD21 Xplained Pro评估板
- CryptoAuth XPRO-B评估工具包或任一CryptoAuth-XPRO插座工具包（AT88CKSCKTUDFN-XPRO或AT88CKSCKTSOIC-XPRO），连接至EXT1
- OLED1 Xplained Pro，连接至EXT3
- 一根Micro-B转Type-B USB接口电缆

软件准备工作：

- Atmel Studio 7
- Atmel软件框架（ASF）3.34
- CryptoAuthLib
- SAM-BA 2.17

注： 上面列出的所有软件均可从Microchip网站下载。

参考资料

- ATECC608A产品详细信息
- CryptoAuthLib
- 安全IC概述
- SAM-BA系统内编程器
- SAM-BA概述和定制流程
- 在SAM器件上使用SAM-BA for Linux
- Atmel Studio 7
- SAM-BA User's Guide，SAM-BA软件安装完成后在安装目录下提供。

ATECC608A应用程序

ATECC608A器件具有灵活的命令集，可在许多应用中使用，其中包括：

- 网络/IoT节点端点安全管理、节点身份验证以及会话密钥的创建和管理。支持包括TLS 1.2（及更早版本）和TLS 1.3等多种协议的完整临时会话密钥生成流程。
- 安全引导，通过验证代码摘要并在收到“成功”信号时使能通信密钥支持MCU主机的安全引导。提供可增强性能的各种配置。
- 短小报文加密。
- 通过硬件高级加密标准（Advanced Encryption Standard，AES）引擎加密和/或解密短小报文或数据，如个人可识别信息（Personally Identifiable Information，PII）。ATECC608A器件直接支持AES-ECB模式，在主机的帮助下还可支持其他AES模式。此外，ATECC608A还具有支持AES-GCM的GFM计算功能。
- 软件下载的密钥生成支持——支持为已下载映像生成本地保护密钥。既支持将一个映像广播到多个其他系统（每个系统都具有相同的解密密钥），也支持点对点下载每个系统的独特映像。
- 生态系统控制和防伪，验证系统或元件是否可靠以及是否来自原始设备制造商。

此外，ATECC608A器件经过适当配置后可与ATECC508A器件兼容。

安全引导功能

如前文所述，ATECC608A提供了一种机制来支持联网MCU中的安全引导操作。上电时，主机MCU内的引导代码将代码摘要和相应的签名发送到ATECC608A器件。然后，ATECC608A使用内部存储的公钥来验证摘要。

如果引导时要验证的代码相对较短，则可以将代码字节发送到ATECC608A，然后使用安全哈希算法（Secure Hash Algorithm，SHA）计算引擎来计算代码摘要。

ATECC608A安全引导功能提供速度优化和线路保护两个选项。

速度优化

ATECC608A安全引导功能的速度优化选项可将签名和/或摘要存储在ATECC608A的受保护边界内，以此缩短执行时间。通过使用常规安全引导命令时切换模式，可更新签名和/或摘要，并验证签名并将签名/摘要存储在指定槽中。存储签名会限制需要发送到ATECC608A的IO块大小，因此可缩短引导时间。

如果存储摘要，则ATECC608A器件仅会对输入数组中的主机代码摘要与指定槽中存储的摘要进行比较。这样可以消除ECC验证的计算延迟，从而缩短引导时间。

线路保护

在某些应用中，可能会有攻击者切断ATECC608A器件与主机MCU之间的线路，然后用欺诈性的“成功”信号替换验证操作的结果，这种情况下需要为系统提供线路保护。如果安全引导命令的模式参数指示存在这种情况，则可以通过将代码摘要与nonce的摘要和IO保护密钥进行逻辑异或运算来对输入代码摘要进行加密。

配置和命令

ATECC608A的配置区域用于控制器件安全引导功能的工作模式。通常，安全引导命令使用这些配置位来确保执行正确的序列。

安全引导功能可配置为以下3种工作模式：

1. 完全安全引导：将摘要和签名均传输到ATECC608A器件。
2. 存储安全引导（FullSig）：存储签名并使用ECC验证函数验证摘要。
3. 存储安全引导（Fulldig）：存储摘要并在不进行ECC验证的情况下比较摘要。

安全引导命令可实现3种工作模式：

1. Full：将摘要和签名均发送到ATECC608A。然后使用签名和公钥验证摘要。
2. FullStore：将摘要发送到ATECC608A器件。然后使用签名验证摘要或将摘要存储在器件中。
3. FullCopy：该命令与Full命令基本相同，只是需要在验证成功后才将摘要/签名复制到器件。

SAM-BA监视器

SAM-BA监视器提供了一种简单的方法来编程片上闪存。SAM-BA监视器支持USB和UART通信。SAM-BA监视器将持续检测UART和/或USB接口的起始条件。

USB接口的起始条件是枚举完成。当检测到启动条件时，SAM-BA监视器会进入无限循环，等待SAM-BA命令。

UART接口上的起始条件以“#”（井号）字符指示。SAM-BA监视器接收到该字符后即开始等待SAM-BA命令。

软件实现

示例应用程序旨在协助使用ATECC608A器件演示安全引导功能。执行该应用程序时，将使用加密器件上的代码摘要和/或签名对用户应用程序进行身份验证。此外，该应用程序还可用于升级当前的用户应用程序。

设计注意事项

以下是该实现的设计注意事项：

- 在闪存中为SAM-BA监视器应用程序预留32 kB的存储空间（0x00000000至0x00008000）。这部分存储空间用于存储基于ASF的应用程序和驱动程序，以便顺利集成到其他系列器件。其中还包括完整的CryptoAuthLib，可启用库中的所有功能，以便进一步评估。
- 使用SAMD21器件内的BOOTPROT和SECURITY位来保护自举应用程序，即禁止外部对闪存进行读写访问以及为自举程序区域提供写保护。
- 仅允许通过UART接口与主机上的SAM-BA GUI进行交互。USB-CDC接口默认处于禁止状态。
- SAM-BA监视器应用程序并未在出厂时编程。要使用该应用程序，需按照**“使用SAM-BA监视器应用程序”一节**提供的步骤进行操作。

图1显示了针对示例应用程序的存储器分区情况。

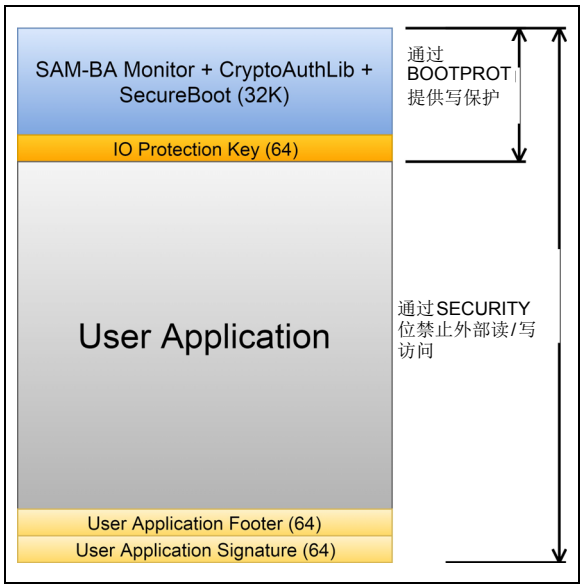

图1： *存储器映射*

安全自举程序流程

图2给出了使用SAM-BA监视器实现安全引导功能的概要流程图。

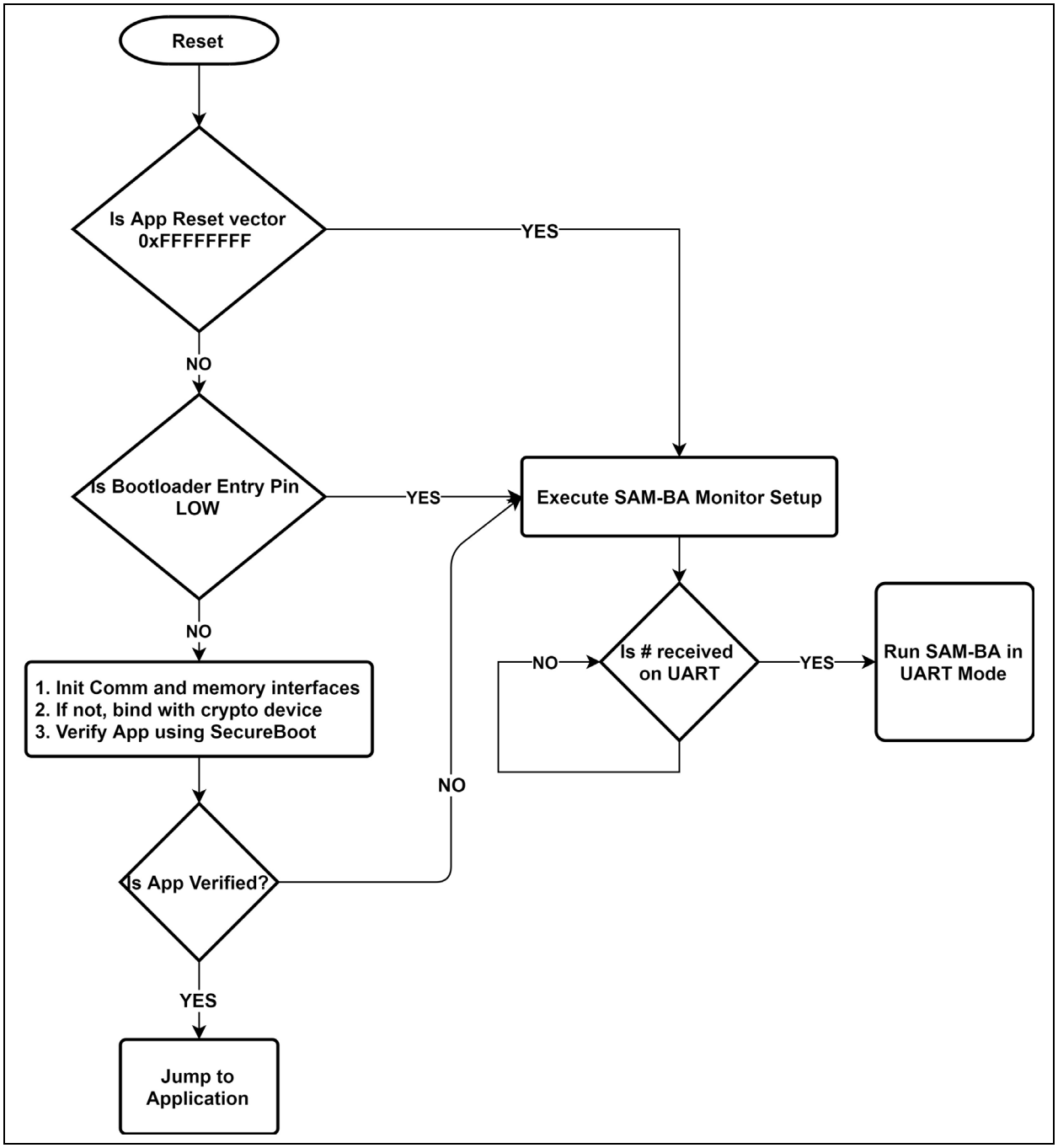

图2： *安全自举程序流程*

配置

可通过应用表1中描述的条件来定制示例应用程序。

表1： 配置条件

条件	说明
CRYPTO_DEVICE_ENABLE_SECURE_BOOT	该宏提供了一个用于使能或禁止安全引导功能的选项。
CRYPTO_DEVICE_LOAD_CONFIG_ENABLED	该宏提供了一个用于使能或禁止加密器件配置的选项。使用该宏的前提是目标板上连接有解锁状态的加密器件。 使能该条件时，目标板将预定义的配置数据和公钥加载到加密器件。加密器件的配置和数据区域随后将锁定。
USER_APPLICATION_START_PAGE	该宏提供了一个用于调整用户应用程序起始地址的选项。更改该地址时需要修改用户应用程序；SAM-BA小程序也会适当调整以反映新地址。
IO_PROTECTION_PAGE_ADDRESS	该宏提供了一个用于调整目标板上的IO保护密钥的选项。

使用SAM-BA监视器应用程序

示例应用程序通过Atmel Studio软件下载到SAMD21 MCU中。示例应用程序的自举程序大小和用户应用程序起始地址与ASF中的原始应用程序有所不同。为了能够将SAM-BA GUI与该版本的SAM-BA监视器搭配使用，需要使用示例应用程序包中提供的文件。

SAM-BA GUI设置

为了能够将SAM-BA GUI与SAM-BA监视器应用程序搭配使用，需要：

1. 将SAM-BA安装目录`[安装目录]\applets`下的文件与`Package\SAMBA_Files\applets`下的文件合并。
2. 将SAM-BA安装目录`[安装目录]\tcl_lib`下的文件与`Package\SAMBA_Files\tcl_lib`下的文件合并。

激活SAM-BA监视器

可以通过以下任何一种条件请求激活SAM-BA监视器（自举程序）：

1. **外部条件：**为了激活该条件，用户需要将自举程序进入引脚拉为低电平，同时将器件从复位状态释放。一般情况下使用可用作SAM-BA监视器触发信号的按钮（SW0）。器件上电或复位时，必须按住该按钮。
2. **内部条件：**在擦除器件后或应用程序复位向量（应用程序的起始地址 + 4）为空（`0xFFFFFFFF`）时，可以请求激活该条件。

运行SAM-BA

本部分介绍在运行Microsoft® Windows®的PC上使用SAM-BA应用程序的基本步骤。有关更多信息，请参见SAM-BA User's Guide（随SAM-BA软件安装提供）。

连接SAM-BA GUI

为了将SAM-BA监视器与UART主机搭配使用，需要通过调试USB端口将目标板连接到PC。

在Windows PC上执行SAM-BA应用程序时，将出现如图3所示的对话框。

单击**Connect**（连接）按钮，与器件建立连接。

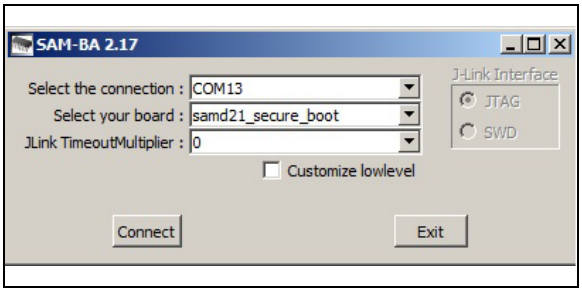

***图3：** 连接SAM-BA监视器对话框*

闪存编程

成功连接器件后，将出现如图4所示的画面。

为了升级现有应用程序，SAM-BA需要先擦除现有的应用程序文件，然后再下载最新的文件。

使用Flash（闪存）选项卡（图4中的标记1）加载闪存的内容。将程序下载到闪存时，起始地址（标记2）必须与SAM-BA监视器和小程序中配置的值相匹配（在示例应用程序中，该值为0x08000），否则将中止传输过程。

通过从下拉菜单（标记3）中选择“erase application area”（擦除应用程序区域）脚本并单击**Execute**（执行）（标记4）来擦除应用程序。

完成擦除后，选择要下载到器件闪存的文件，然后将地址（标记2）的值更改为0x08000。最后单击Send File（发送文件）按钮将固件映像下载到MCU。

脚本

表2列出了可供SAM-BA主机使用的预定义脚本。

表2：　　预定义脚本

脚本名称	说明
Erase Application Area	擦除所有应用程序代码（不会擦除SAM-BA监视器区域）。
Invalidate Application（使应用程序失效）	擦除应用程序的第一页。
Read Fuses（读取熔丝）	返回熔丝设置的值。有关详细信息，请参见ATECC608A Summary Data Sheet。
Read Lock Fuses（读取锁定熔丝）	读取当前锁定设置。
Read Device ID（读取器件ID）	读取器件标识寄存器。

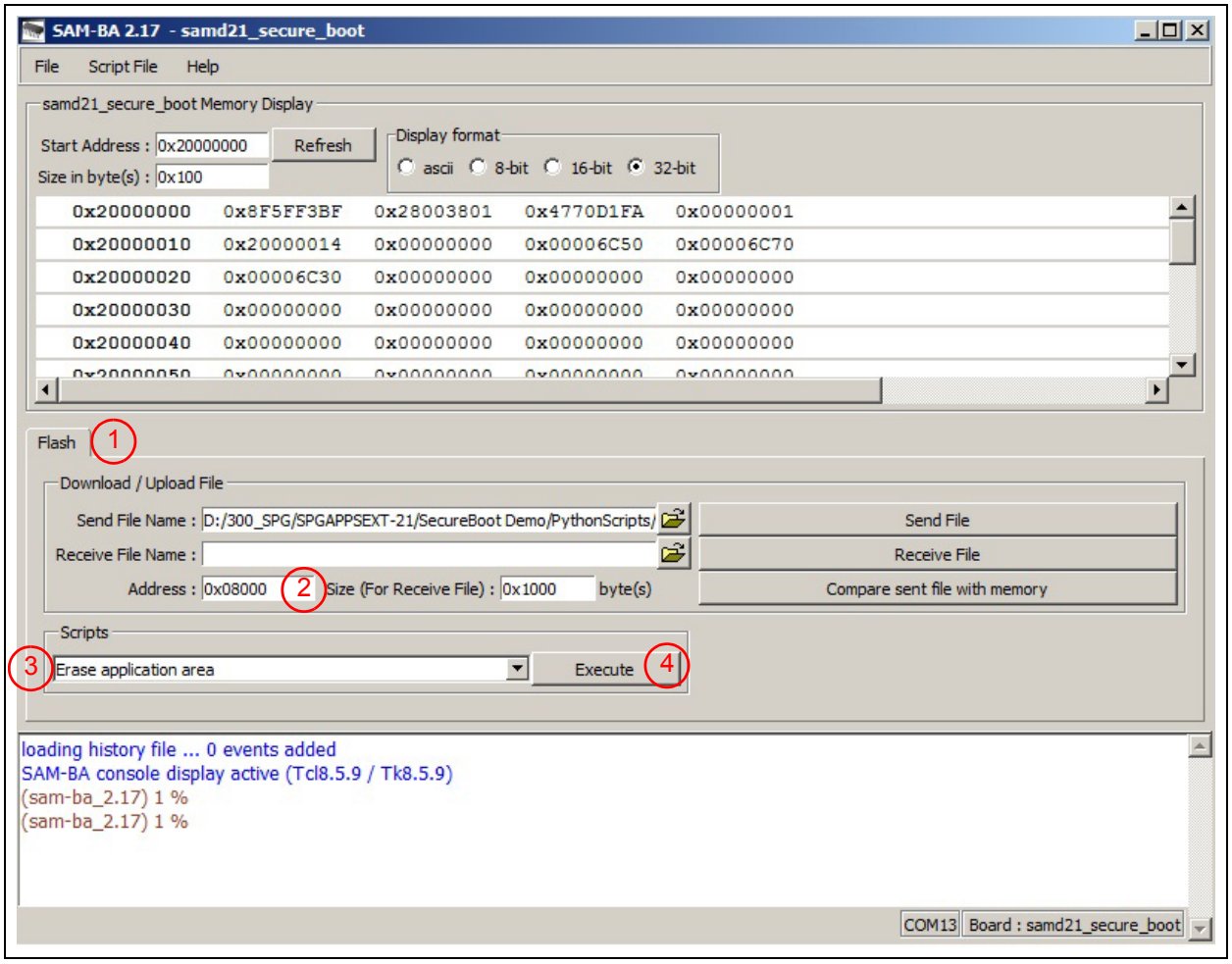

图4：　　SAM-BA® 窗口

运行示例应用程序

本部分介绍执行示例应用程序的基本步骤，具体分为以下几类：

1. 编译并下载SAM-BA监视器应用程序。
2. 编译并下载用户应用程序。
3. 使用目标板预配置ATECC608A器件。
4. 将目标板绑定到ATECC608A器件。
5. 验证安全引导功能。

编译并下载SAM-BA监视器应用程序

SAMD21系列器件的ROM中不包含SAM-BA监视器。在将SAM-BA GUI与SAMD21器件搭配使用之前，需要先编译并下载SAM-BA监视器应用程序。可以使用SWD调试器来实现此操作。

1. 运行Atmel Studio。从顶部菜单栏中选择**Tools**（工具）选项卡，然后单击Device Programming（器件编程）菜单选项。
2. 在Device Programming窗口中，选择工具（例如EDBG）并单击**Apply**（应用）。
3. 待EDBG工具运行后，单击**Fuses**（熔丝）选项卡。
4. 将NVMCTRL_BOOTPROT字段设为默认值0x07。
5. 单击**Memories**（存储器）选项卡，然后单击**Erase now**（立即擦除）按钮以擦除芯片。
6. 在Flash字段中，填写自举程序映像的路径，然后单击**Program**（编程）按钮。

编译并下载用户应用程序

示例应用程序包中提供了一个用户应用程序示例。该程序是一个针对SAM-BA监视器自举程序定制的ASF示例。

以下是基于原始ASF程序的定制流程：

1. 将用户应用程序的起始地址重定位到自举程序之后（例如，从32K地址开始）
   - 本示例项目配置为仅使用24K的用户应用程序空间。
2. 创建应用程序页脚结构。自举程序验证起始地址和大小参数是否符合自身的预期。

```
__attribute__((section(".footer_data")))
const memory_parameters
user_application_footer =
{
USER_APPLICATION_START_ADDRESS,
(USER_APPLICATION_END_ADDRESS -
USER_APPLICATION_START_ADDRESS),
0x00010001,
{0},
};
```

3. 将应用程序页脚重定位到映像的最后一页，具体可通过链接描述文件来实现。请参见随示例用户应用程序提供的samd21j18a_flash.ld文件。
4. 编译项目以生成如下文件：FREERTOS_OLED1_XPRO_EXAMPLE1.bin
5. 通过附加签名来保护生成的bin文件。示例应用程序包中包含必要的Python脚本和key.pem文件，方便用户使用key.pem文件中的私钥生成签名。按照以下步骤将签名附加到bin文件：

a) 使用密钥文件和用户应用程序调用sboot_sign_firmware.exe。
   - 进入命令提示符并使用以下命令：
     sboot_sign_firmware.exe -kkey.pem -bFREERTOS_OLED1_XPRO_EXAMPLE1.bin
   - 未向脚本传递密钥文件时，sboot_sign_firmware.exe将生成一个新的密钥对。这个新的密钥对将位于generated_key.pem文件中。

   注： 当用户使用新的密钥对时，应使用预配置服务或目标板将关联的公钥加载到加密器件。

b) FREERTOS_OLED1_XPRO_EXAMPLE1.bin现在将包含附加在文件末端位置的签名。

6. 使用SAM-BA GUI下载附加的签名FREERTOS_OLED1_XPRO_EXAMPLE1.bin（如**“使用SAM-BA监视器应用程序”一节**所述）。

使用目标板配置ATECC608A器件

ATECC608A器件的配置非常重要，对于保护用户应用程序必不可少。

作为本演示的一部分，可以选择使用自举程序来配置器件。自举程序中提供了一个用于使能该功能的宏（CRYPTO_DEVICE_LOAD_CONFIG_ENABLED）。默认情况下，该宏处于禁止状态。使能该宏后，会将一个固定的公钥以及其他配置加载到加密器件中。

1. 关闭目标板，然后将CryptoAuth XPRO-B板插入SAMD21 Xplained Pro评估板。
   - CryptoAuth XPRO-B板上的ATECC608A器件应处于解锁状态。
2. 接通目标板。
3. 使能宏时，目标板会在识别到解锁状态的加密器件后启动配置过程。
   - 如果加密器件处于锁定状态，则SAMD21器件将跳过配置过程。
4. 此时，ATECC608A应已完成配置且可供使用。

注： 考虑到用户可能会想要使用其他密钥或配置，Microchip还提供了多项配置服务来确保通过一种标准化的安全配置过程为器件配置正确的数据。

将目标板绑定到ATECC608A器件

这种绑定保护旨在防止攻击者切断ATECC608A器件与主机MCU之间的线路。此外，还有助于防止ATECC608A器件从目标板上移除并安装到另一块目标板上使用。即使攻击者设法从MCU中提取出IO保护密钥，也可以确保仅有一块目标板会受到影响。

此步骤无需用户干预。一旦目标板检测到加密器件并且主机MCU或加密器件上均未设置IO保护密钥，会立即启动该过程。

一旦目标板与加密器件完成绑定，目标板便会启动BOOTPROT熔丝设置，从而禁止对目标板自举程序部分的所有后续写操作。

在该过程的最后阶段，SAMD21和加密器件均会完成绑定并各自拥有惟一的IO保护密钥。

注： 一旦加密器件与主机MCU完成绑定，便无法在擦除主机MCU的IO保护密钥后重新绑定。

验证安全引导功能

此时，目标板与加密器件已绑定，且已加载自举程序和用户应用程序。

当目标板与加密器件一同接通后，将验证用户应用程序并随即开始执行。

在执行用户应用程序的过程中，FREERTOS_OLED1_XPRO_EXAMPLE ASF项目的所有功能均可供评估。

FREERTOS_OLED1_XPRO_EXAMPLE概述

FREERTOS_OLED1_XPRO_EXAMPLE用户应用程序旨在演示SAMD器件上FreeRTOS实时操作系统的基本使用，其中包括任务、队列和互斥（信号量）。

该应用程序设计为在SAMD Xplained Pro评估板上运行，评估板的EXT端口上连接了一个OLED1 Xplained Pro翼板。

该应用程序启动后会显示一个伪随机图形，此图形会在OLED上连同底部的菜单栏一起持续更新。菜单栏显示用户选择的画面。用户可通过按下OLED1 Xplained Pro翼板上的相应按钮来选择以下两项：

- 按钮1——图形：伪随机图形。
- 按钮2——终端：从终端（例如，EDBG虚拟COM端口）接收的文本。

要在终端窗口中添加文本，用户必须使用一根USB电缆将SAMD MCU的EDBG端口与PC相连。PC的USB端口将充当EDBG虚拟COM端口。终端仿真器软件必须设置为9600波特率、8个数据位、1个停止位、无奇偶校验。示例应用程序将回显收到的字符。

此外，OLED1 Xplained Pro翼板上的各个LED会在对应的任务循环期间点亮，以便直观地呈现任务切换情况：

- LED1表示正在更新图形和处理传入的终端字符。
- LED2表示正在将文本打印到终端窗口。
- LED3表示正在检查用户选择、处理显示缓冲区和菜单画面。

注： 请注意，当一个任务正在等待另一个任务释放资源时，可能会出现多个LED同时点亮的情况。在本用户应用程序中，资源是显示和终端文本缓冲区的互斥。

移植到其他自举程序

按照以下步骤，可轻松地将标准自举程序转换为类似的安全自举程序：

1. 将 CryptoAuthLib 集成到现有的自举程序中，包括app\secure_boot。
2. 将crypto_device_app.c和.h文件集成到项目中。
   - 复制crypto_device_app.c和.h文件并将其包含在项目中。
   - 在跳转到用户应用程序之前，调用crypto_device_verify_app。
   - 仅在显示ATCA_SUCCESS消息时跳转到用户应用程序。
3. 通过重新访问可配置宏来设置配置。

a) secure_boot.h

```
#define SECURE_BOOT_CONFIGURATION            SECURE_BOOT_CONFIG_FULL_DIG
#define SECURE_BOOT_DIGEST_ENCRYPT_ENABLED   true
#define SECURE_BOOT_UPGRADE_SUPPORT          true
```

b) secure_boot_memory.h

```
#define USER_APPLICATION_START_PAGE          (APP_START_ADDRESS / NVMCTRL_PAGE_SIZE)
#define IO_PROTECTION_PAGE_ADDRESS           ((USER_APPLICATION_START_PAGE - 1) * NVMCTRL_PAGE_
                                             SIZE)
#define USER_APPLICATION_START_ADDRESS       (USER_APPLICATION_START_PAGE * NVMCTRL_PAGE_SIZE)
#define USER_APPLICATION_END_ADDRESS         (USER_APPLICATION_START_ADDRESS + (24*1024))
#define USER_APPLICATION_HEADER_SIZE         (2 * NVMCTRL_PAGE_SIZE)
#define USER_APPLICATION_HEADER_ADDRESS      (USER_APPLICATION_END_ADDRESS - USER_APPLICATION_
                                             HEADER_SIZE)
```

c) crypto_device_app.h

```
#define CRYPTO_DEVICE_ENABLE_SECURE_BOOT     true
#define CRYPTO_DEVICE_LOAD_CONFIG_ENABLED    false
#define IO_PROTECTION_KEY_SLOT               4
#define SECURE_BOOT_PUBLIC_KEY_SLOT          11
#define SECURE_BOOT_SIGN_DIGEST_SLOT         12
```

4. 更新存储器接口：
   - Secure_boot_memory.c和io_protection_key.c文件包含针对NVM/闪存的访问函数。应根据使用的器件复查这些访问函数。
5. 存储器访问限制：
   - 在本示例应用程序中，使用 BOOTPROT 熔丝和SECURITY 位来避免对闪存进行不必要的访问。用户需根据使用的器件来实现类似的限制。
6. 用户应用程序更新：
   - 需将用户应用程序和页脚数据调整到自举程序中设定的新位置，以便自举程序能够验证其真实性，然后跳转到相应的位置执行用户应用程序。有关更多详细信息，请参见**“编译并下载用户应用程序”一节**。

7. 最后，用户需要复查示例应用程序包中提供的 Python 脚本，以便确保该脚本与存储器映射相匹配，并适当地生成密钥以及在正确的位置附加签名。

使用不同的器件和自举程序架构时，上述步骤也会略有差异，因此用户需根据具体应用考虑做出适当的调整。

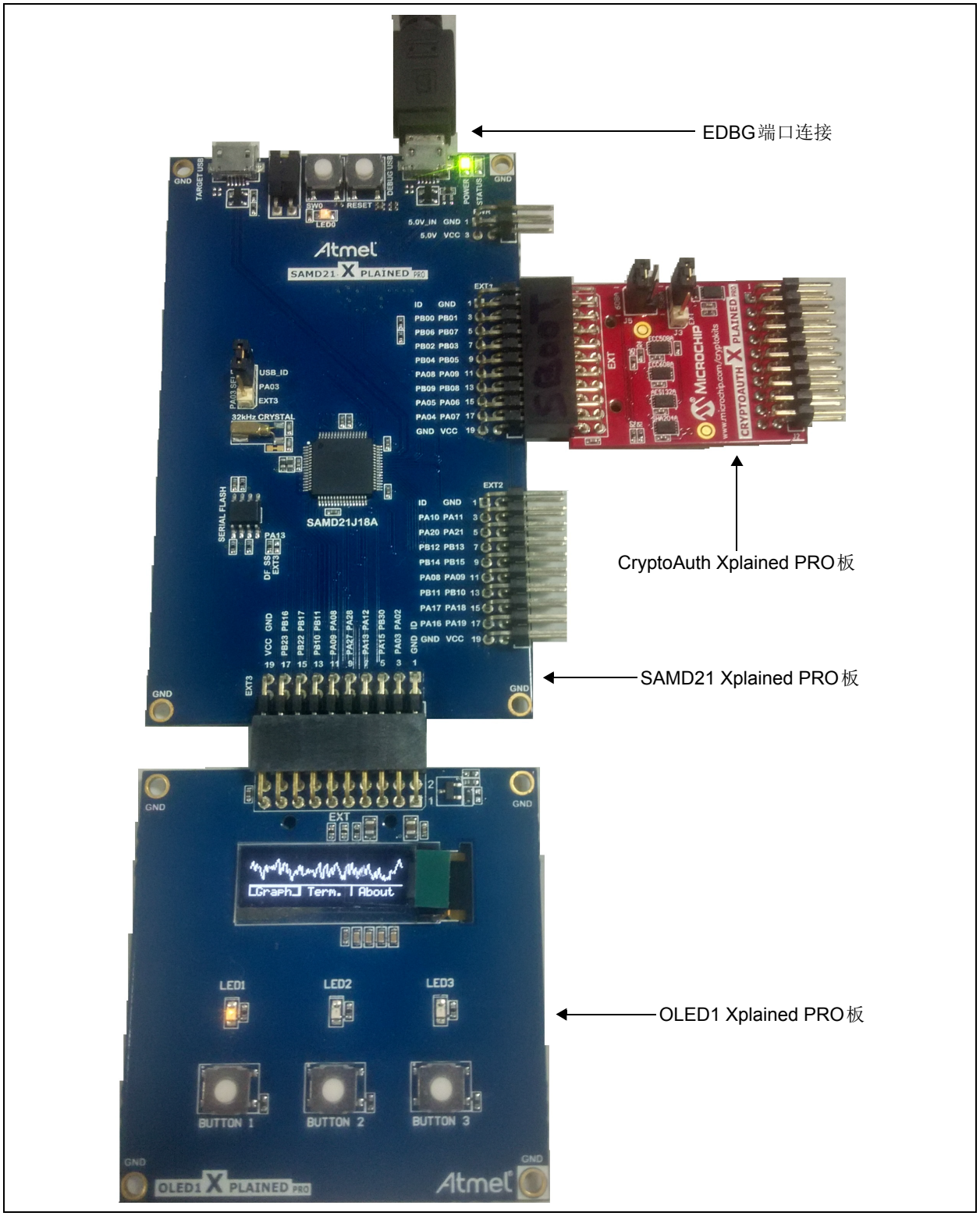

图5： *应用示例设置的俯视图*

请注意以下有关 Microchip 器件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指标。
- Microchip 确信：在正常使用的情况下， Microchip 系列产品是当今市场上同类产品中最安全的产品之一。
- 目前，仍存在着恶意、甚至是非法破坏代码保护功能的行为。就我们所知，所有这些行为都不是以 Microchip 数据手册中规定的操作规范来使用 Microchip 产品的。这样做的人极可能侵犯了知识产权。
- Microchip 愿与那些注重代码完整性的客户合作。
- 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。任何试图破坏 Microchip 代码保护功能的行为均可视为违反了《数字器件千年版权法案 （Digital Millennium Copyright Act）》。如果这种行为导致他人在未经授权的情况下，能访问您的软件或其他受版权保护的成果，您有权依据该法案提起诉讼，从而制止这种行为。

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。

本出版物中所述的器件应用信息及其他类似内容仅为您提供便利，它们可能由更新之信息所替代。确保应用符合技术规范，是您自身应负的责任。**Microchip 对这些信息不作任何明示或暗示、书面或口头、法定或其他形式的声明或担保，包括但不限于针对其使用情况、质量、性能、适销性或特定用途的适用性的声明或担保。** Microchip 对因这些信息及使用这些信息而引起的后果不承担任何责任。如果将 Microchip 器件用于生命维持和 / 或生命安全应用，一切风险由买方自负。买方同意在由此引发任何一切伤害、索赔、诉讼或费用时，会维护和保障 Microchip 免于承担法律责任，并加以赔偿。除非另外声明，在 Microchip 知识产权保护下，不得暗中或以其他方式转让任何许可证。

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

商标

ISBN：978-1-5224-4909-6

全球销售及服务网点

美洲

公司总部 Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 1-480-792-7200
Fax: 1-480-792-7277
技术支持：
http://www.microchip.com/support
网址：www.microchip.com

亚特兰大 Atlanta
Duluth, GA
Tel: 1-678-957-9614
Fax: 1-678-957-1455

奥斯汀 Austin, TX
Tel: 1-512-257-3370

波士顿 Boston
Westborough, MA
Tel: 1-774-760-0087
Fax: 1-774-760-0088

芝加哥 Chicago
Itasca, IL
Tel: 1-630-285-0071
Fax: 1-630-285-0075

达拉斯 Dallas
Addison, TX
Tel: 1-972-818-7423
Fax: 1-972-818-2924

底特律 Detroit
Novi, MI
Tel: 1-248-848-4000

休斯敦 Houston, TX
Tel: 1-281-894-5983

印第安纳波利斯 Indianapolis
Noblesville, IN
Tel: 1-317-773-8323
Fax: 1-317-773-5453
Tel: 1-317-536-2380

洛杉矶 Los Angeles
Mission Viejo, CA
Tel: 1-949-462-9523
Fax: 1-949-462-9608
Tel: 1-951-273-7800

罗利 Raleigh, NC
Tel: 1-919-844-7510

纽约 New York, NY
Tel: 1-631-435-6000

圣何塞 San Jose, CA
Tel: 1-408-735-9110
Tel: 1-408-436-4270

加拿大多伦多 Toronto
Tel: 1-905-695-1980
Fax: 1-905-695-2078

亚太地区

中国 - 北京
Tel: 86-10-8569-7000

中国 - 成都
Tel: 86-28-8665-5511

中国 - 重庆
Tel: 86-23-8980-9588

中国 - 东莞
Tel: 86-769-8702-9880

中国 - 广州
Tel: 86-20-8755-8029

中国 - 杭州
Tel: 86-571-8792-8115

中国 - 南京
Tel: 86-25-8473-2460

中国 - 青岛
Tel: 86-532-8502-7355

中国 - 上海
Tel: 86-21-3326-8000

中国 - 沈阳
Tel: 86-24-2334-2829

中国 - 深圳
Tel: 86-755-8864-2200

中国 - 苏州
Tel: 86-186-6233-1526

中国 - 武汉
Tel: 86-27-5980-5300

中国 - 西安
Tel: 86-29-8833-7252

中国 - 厦门
Tel: 86-592-238-8138

中国 - 香港特别行政区
Tel: 852-2943-5100

中国 - 珠海
Tel: 86-756-321-0040

台湾地区 - 高雄
Tel: 886-7-213-7830

台湾地区 - 台北
Tel: 886-2-2508-8600

台湾地区 - 新竹
Tel: 886-3-577-8366

亚太地区

澳大利亚 Australia - Sydney
Tel: 61-2-9868-6733

印度 India - Bangalore
Tel: 91-80-3090-4444

印度 India - New Delhi
Tel: 91-11-4160-8631

印度 India - Pune
Tel: 91-20-4121-0141

日本 Japan - Osaka
Tel: 81-6-6152-7160

日本 Japan - Tokyo
Tel: 81-3-6880-3770

韩国 Korea - Daegu
Tel: 82-53-744-4301

韩国 Korea - Seoul
Tel: 82-2-554-7200

马来西亚 Malaysia - Kuala Lumpur
Tel: 60-3-7651-7906

马来西亚 Malaysia - Penang
Tel: 60-4-227-8870

菲律宾 Philippines - Manila
Tel: 63-2-634-9065

新加坡 Singapore
Tel: 65-6334-8870

泰国 Thailand - Bangkok
Tel: 66-2-694-1351

越南 Vietnam - Ho Chi Minh
Tel: 84-28-5448-2100

欧洲

奥地利 Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

丹麦 Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

芬兰 Finland - Espoo
Tel: 358-9-4520-820

法国 France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

德国 Germany - Garching
Tel: 49-8931-9700

德国 Germany - Haan
Tel: 49-2129-3766400

德国 Germany - Heilbronn
Tel: 49-7131-72400

德国 Germany - Karlsruhe
Tel: 49-721-625370

德国 Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

德国 Germany - Rosenheim
Tel: 49-8031-354-560

以色列 Israel - Ra'anana
Tel: 972-9-744-7705

意大利 Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

意大利 Italy - Padova
Tel: 39-049-7625286

荷兰 Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

挪威 Norway - Trondheim
Tel: 47-7288-4388

波兰 Poland - Warsaw
Tel: 48-22-3325737

罗马尼亚 Romania - Bucharest
Tel: 40-21-407-87-50

西班牙 Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

瑞典 Sweden - Gothenberg
Tel: 46-31-704-60-40

瑞典 Sweden - Stockholm
Tel: 46-8-5090-4654

英国 UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820