Application Note

密钥写入器部署策略：生产环境中的安全器件预置

Diwakar Dhyani,Frangline Jose, Keerthy J

摘要

本应用手册提供了将 TDA4x/DRA8x 处理器从高安全性现场可保护 (HS-FS) 工作模式转换为高安全性强制安全 (HS-SE) 工作模式的综合指南。文中介绍了 TI 的一次性可编程 (OTP) 密钥写入器工具架构，以及适用于开发和生产环境的部署方法。还解释了使用德州仪器 (TI) 基础安全 (TIFS) API 进行现场更新的过程。工程师将学习如何选择合适的安全密钥预置策略，实施安全的器件编程工作流程，以及排查 OTP 密钥编程操作中遇到的常见问题。

内容

商标

1 简介

本文适用于为 TI 处理器实施安全密钥预置的生产工程师、安全架构师和制造团队。其中涵盖密钥写入器部署策略、架构组件和生产工作流程。密钥写入器用户将掌握多种实用知识：选择合适的部署方法、将器件从现场可保护（FS 或 HSFS）状态切换为强制安全 (HS-SE) 状态，以及解决常见的预置问题。读者将掌握必要的理论和实践知识，以便在实际生产环境中实施、优化密钥写入器操作并排查其故障。

1.1 为什么需要密钥写入器

TI 处理器出厂时处于 HS-FS（高安全性现场可保护）模式。在此状态下，由于信任根 (RoT) 密钥尚未编程到器件 OTP-eFuse 中，因此不会强制执行安全引导。借助密钥写入器工具，我们能够将这些信任根密钥和相关的安全字段编程到 eFuse 中，从而将器件从 HS-FS 工作模式切换到 HS-SE 模式。当器件处于 HS-SE 状态时，由硬件强制执行安全引导。

可以在 OTP-eFuse 阵列中编程以下字段，但并非所有字段都是切换到 HS-SE 器件所必需的：

必填字段

- SMPK HASH（二级制造商公钥哈希值）。
- SMEK（二级制造商加密密钥）。
- KEYCNT（密钥计数）。
- KEYREV（密钥版本）。

选填字段

- BMPK HASH（备用制造商公钥哈希）。
- BMEK（备用制造商加密密钥）。
- SWREV、MSV、JTAG（用于防回滚保护的软件版本，特定于型号的值，JTAG 禁用）。
- 扩展 OTP 字段。

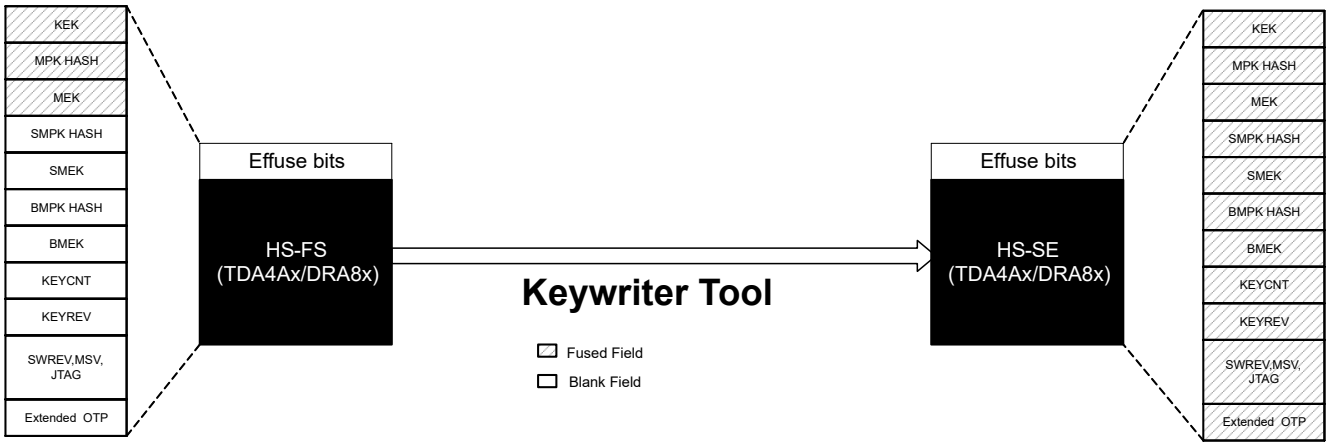

图 1-1. 器件生命周期：通过密钥写入器 eFuse 编程工作流程实现 HS-FS 到 HS-SE 的切换

1.2 什么是密钥写入器

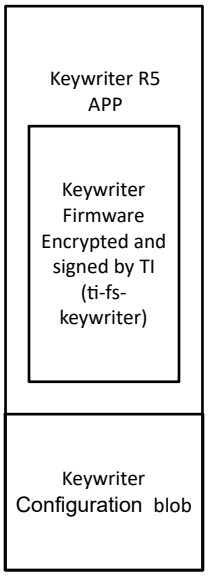

图 1-2. 密钥写入器系统架构，其中显示了 TIFS 固件、R5 应用程序和证书 blob 组件

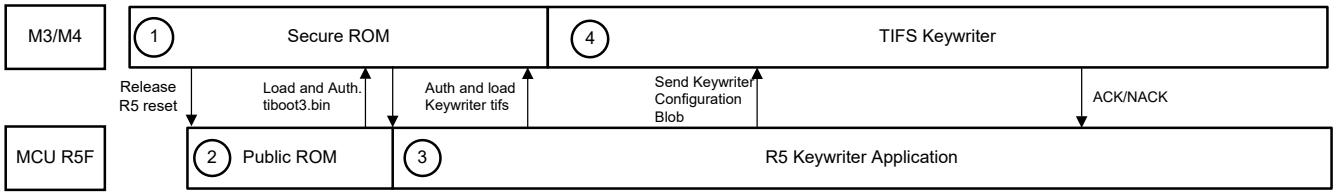

图 1-3. 密钥写入器引导流程

密钥写入器工具由三个主要组件组成：

- **密钥写入器固件**：这是在器件的安全子系统 (M3/M4_0) 上运行的安全 OTP 密钥写入器固件。它负责验证来自 x509 证书的 OTP 配置，并将数据编程到器件的 OTP-eFuse 中。
- **密钥写入器配置 blob**：一个证书，包含将编程到 OTP-eFuse 中的 eFuse 配置。
- **密钥写入器 R5 应用程序**：这是公共密钥写入器应用程序。它直接在器件的主引导内核上引导，无需任何其他引导加载程序。它负责将 OTP 配置发送到在安全子系统 (M3/M4) 上运行的安全密钥写入器组件，以将密钥编程到器件 OTP-eFuse 中。

2 密钥写入器证书 blob

2.1 证书生成概述

密钥写入器证书 blob 采用结合了数字签名和加密的分层安全方法。OTP 配置数据使用随机生成的 AES-256 会话密钥进行加密。然后使用 TI-FEK（TI 现场加密密钥）对该会话密钥进行加密，以确认只有具有相应私钥的真实 TI 固件才能对其解密。整个证书使用 SMPK（二级制造商私钥）进行签名以用于身份验证。证书还可以选择使用 BMPK（备用制造商私钥）进行双重签名，以支持密钥轮换场景。有关完整的密钥写入器 blob 生成流程，请参阅下图。

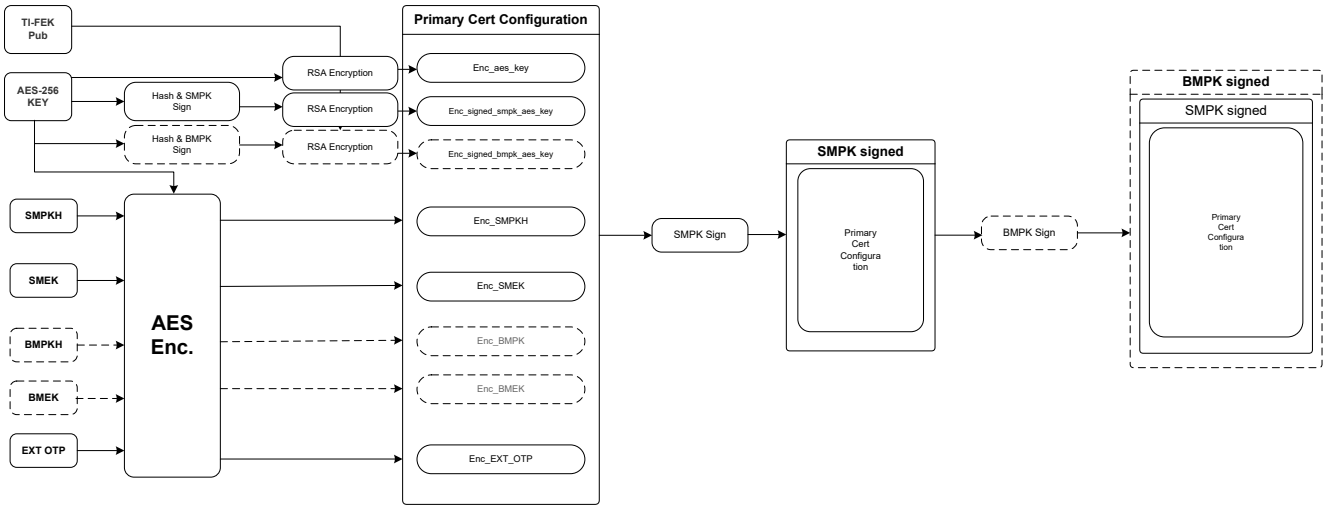

图 2-1. 证书 blob 生成流程：AES 加密、TI-FEK 密钥打包和双重签名身份验证

3 生产部署方法

有多种部署方法可用于满足不同的生产环境和要求。每种方法都提供了具体的实施步骤，使客户能够选择最适合其生产设置和需求的方法。这种灵活性确保客户可以选择任何合适的方法，而不受预定义用例的限制。

3.1 OSPI 引导方法

初始设置和密钥预置过程：

1. 将密钥写入器映像刷写到 OSPI 闪存存储器的主引导位置。
2. 将 HS-SE 签名的应用程序映像刷写到备用引导位置。
3. 为处理器 (MPU) 上电。引导 ROM 从 OSPI 闪存中的主位置读取密钥写入器映像。
4. 由于器件处于 HS-FS (高安全性现场可保护) 模式，密钥写入器应用程序将会运行并将安全密钥编程到器件上。

   切换到安全引导：

   对 OTP-eFuse 进行编程后，器件在下一个电源周期进入 HS-SE 模式。对客户密钥以及 KEYREV、KEYCNT 都进行了编程后，硬件会切换到 HS-SE 状态。此过程无法逆转回 HS-FS 状态。
5. 在下一次上电复位时，ROM 引导加载程序将强制执行安全引导。首先加载主引导位置的密钥写入器映像，但由于它不是用 OTP-eFuse 中新编程的客户信任根密钥签名的，因此身份验证失败。
6. ROM 引导加载程序的回退机制激活，从 OSPI 闪存的备用引导位置读取应用程序映像。它使用 eFuse 中存储的公钥哈希值成功对经 HS-SE 签名的应用程序映像进行了身份验证。
7. 器件使用客户密钥 (SMPKH) 签名的映像成功引导。
8. 在此阶段，最好擦除 OSPI 闪存中的主映像，并用与从 OSPI 闪存辅助分区加载的映像相同、使用客户密钥签名的应用程序映像副本对其重新编程。

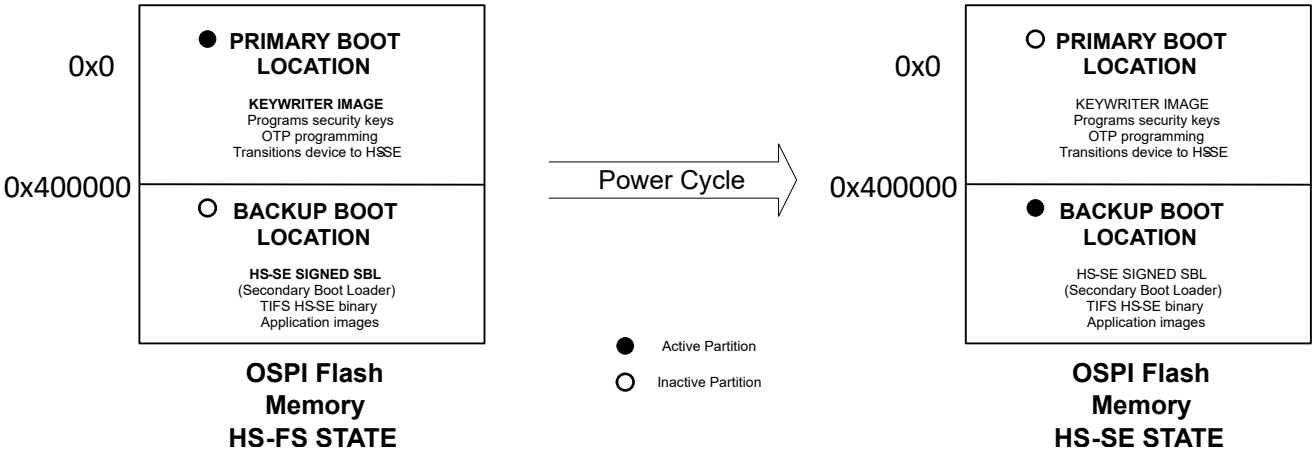

图 3-1. OSPI 引导方法

3.2 eMMC 引导方法

初始设置和密钥预置过程：

1. 将密钥写入器映像刷写到 eMMC 器件的 Boot 0 分区。
2. 将经 HS-SE 签名的应用程序映像刷写到 eMMC 器件的 Boot-1 分区。
3. 将引导模式引脚配置为 eMMC 引导模式，并为器件上电。
4. ROM 引导加载程序读取 PARTITION_CONFIG 寄存器（默认设置：Boot-0 处于活动状态），由于器件处于 HS-FS 状态，ROM 对密钥写入器进行身份验证并运行它。
5. 密钥写入器完成密钥预置后，密钥写入器应用程序更新 eMMC 的 EXT_CSD 寄存器中的 PARTITION_CONFIG 字段，将活动引导分区从 Boot-0 更改为 Boot-1。有关参考实现，请参阅常见问题解答。

切换到安全引导：

6. 对板卡进行断电重启，ROM 引导加载程序检查引导模式引脚（配置为 eMMC 引导模式），并读取 PARTITION_CONFIG 字段以确定哪个分区处于活动状态。
7. 由于上一步已将活动分区更改为 Boot-1，ROM 从 Boot-1 获取映像。
8. 器件使用 Boot-1 中经 HS-SE 签名的生产映像成功引导
9. 在此阶段，最好擦除 eMMC 闪存中的主映像，并用与从 eMMC 闪存辅助分区加载的映像相同、使用客户密钥签名的应用程序映像副本对其重新编程。

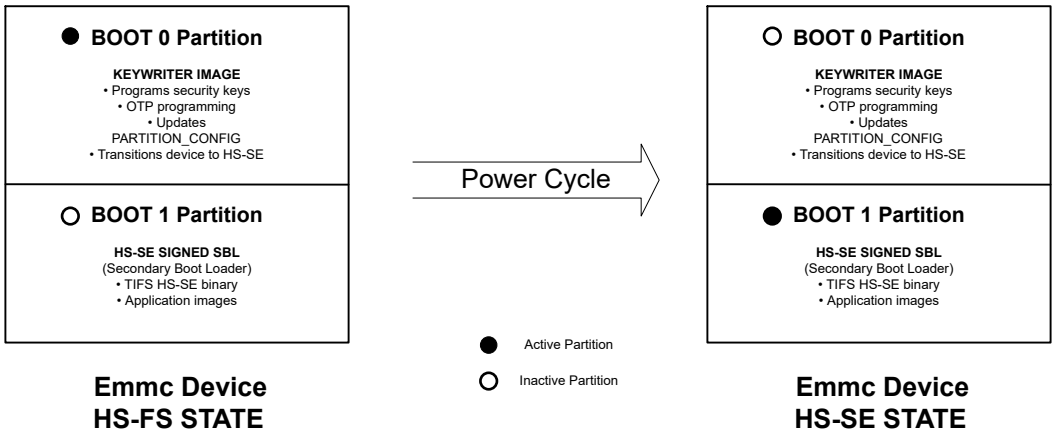

图 3-2. eMMC 引导模式

3.3 使用 DFU 备用方法进行 eMMC 引导

初始设置和密钥预置过程：

1. 将主引导介质设置为 EMMC，将备用介质设置为 DFU。
2. 为器件上电。由于我们尚未将任何映像刷写到 eMMC 中，引导 ROM 将无法从主引导介质读取映像，并回退到备用引导模式。
3. 引导 ROM 启动 DFU 引导。使用 DFU 接口加载密钥写入器映像。
4. 密钥写入器二进制文件将密钥编程到 OTP 中。

切换到安全引导：

5. 对板卡进行断电重启，通过 DFU 接口使用经 HS-SE 签名的映像引导至 U-Boot。按照 TDA4 刷写技术中“5 eMMC 刷写”一节的说明，使用 DFU 接口将经 HS-SE 签名的映像刷写到 eMMC 中。
6. 对板卡进行断电重启，因为 eMMC 是主引导介质且具有有效的已签名引导映像。ROM 将从 eMMC 读取、验证并引导应用程序映像。

备注

备用引导位置与备用引导模式不同。引导 ROM 支持备用 OSPI 偏移：如果在主偏移处找不到有效映像，它会自动跳转到同一 OSPI 闪存内的备用偏移处。而备用引导模式由硬件配置，会回退到完全不同的引导介质，具体取决于物理 BOOTMODE 引脚。

3.4 JTAG/开发引导方法

初始设置：

1. 通过设置相应的引导引脚 (BOOTMODE[4] = 0)，将器件配置为开发引导 (DEV BOOT) 模式。
2. 在 DEV BOOT 期间，器件等待来自 MCU R5 的固件加载消息。
3. 将 JTAG 仿真器（XDS110、XDS200 或 XDS560）连接到微处理器/MPU。

预置过程：

4. 连接到 MCU Cortex R5F 内核 0。将 R5F 内核复位到干净状态。
5. 将密钥写入器应用程序加载到 MCU R5 内核中。
6. 将密钥写入器证书 blob 加载到指定的内存位置（例如，对于 TDA4AL 为 0x41C7F004，密钥写入器证书从 keywr_end + 1 开始，该位置位于“.keywr_bin_end”段中，请查阅映射文件或链接器命令文件）。
7. 在 MCU R5 上开始执行密钥写入器程序。
8. 密钥写入器固件验证证书、解密密钥并编程 OTP-eFuse，将器件从 HS-FS 切换到 HS-SE。

此链接中的常见问题解答提供了有关此方法的更多详细信息。此常见问题解答还提供了一个可直接与 CCS 脚本 shell 一起使用的 Java 脚本。

3.5 RGMI 以太网引导模式

初始设置和密钥预置过程：

1. 将器件配置为 RGMI 引导模式。
2. 在主机 PC 上为微处理器设置静态 IP，并将链路配置为 100M 全双工。
3. 将 tftpd32 应用程序下载到主机 PC 上，并使用 tftpd32 应用程序设置 DHCP 服务器。
4. 使用以太网电缆将 PC 以太网端口连接到器件上的 CPSW 端口。

有关更多详细信息，请参阅常见问题解答。

备注

只有 TDA4VH 类器件支持以太网引导模式

4 现场更新

4.1 SWREV（软件版本）

OTP-eFuse 中的 SWREV 字段用于实现软件回滚保护，防止攻击者将主应用程序固件降级到具有已知漏洞的旧版本。当器件引导时，TIFS/引导 ROM 代码将引导映像证书中嵌入的软件版本值与编程到 OTP-eFuse 中的 SWREV 值进行比较。如果证书的软件版本低于 OTP SWREV 值，则引导过程被拒绝，从而确保验证并加载相等或更高的 SWREV 版本号。

可以更新 SWREV 的组件包括：

1. 软件版本 SBL。
2. 软件版本 SYSFW/TIFS。
3. 软件版本安全板卡配置。

更新步骤：

- HS-SE TIFS 提供了在运行时使用 TISCI_MSG_WRITE_SWREV 命令更新 SWREV 值的功能。
- eFuse 写入操作需要 VPP_MCU。

备注

TI 建议除非必要，否则不要更改 TIFS/SYSFW 的 SWREV。错误、不存在的 TIFS 软件版本可能会使器件变砖。

4.2 KEYREV（密钥版本）

OTP-eFuse 中的 KEYREV 字段控制安全引导操作使用哪些信任根密钥：

- KEYREV = 1：激活二级制造商密钥集 (SMPK/SMEK)
- KEYREV = 2：激活备用制造商密钥集 (BMPK/BMEK)

更新步骤：

- 在 HS-SE 器件上，可以使用 TISCI_MSG_WRITE_KEYREV 命令在运行时更新 KEYREV
- 更新 KEYREV 需要一个由两部分组成的双重签名证书：使用 SMPK 私钥签名的主证书和使用 BMPK 私钥签名的二级证书
- TISCI_MSG_WRITE_KEYREV 消息只能由安全板卡配置中 write_host 下提到的主机发送

作为参考，可参阅使用 TIFS API 更新密钥版本的常见问题解答。

5 常见调试步骤

本节介绍了在密钥预置过程中诊断和解决问题的系统性方法。按照这些步骤操作可以高效地排查故障。

5.1 空跑测试

- 在密钥写入器应用程序中删除/注释掉 VPP 使能逻辑，编译并运行密钥写入器工具
- 如果禁用了 VPP，eFuse 编程将失败。
- 请参阅 TIFS（唤醒 UART）跟踪数据，以解析验证信息以及密钥写入器 TIFS 返回的失败消息，因为实际 eFuse 烧录会失败。

以下代码显示了 J721S2 EVM 上 WKUP 和 MCU UART 的参考日志，用于生成证书 blob 的命令为：

```
./gen_keywr_cert.sh -t ti_fek_public.pem
-s keys/smpk.pem --smek keys/smek.key -s-rp --smek-rp
-b keys/bmpk.pem --bmek keys/bmek.key -b-rp --bmek-rp
--mek-opt 0x1 --mpk-opt 0x21
--keycnt 2 --keycnt-wp
--keyrev 1
```

表 5-1.

MCU UART（R5 应用程序）	WKUP UART（密钥写入器 TIFS）
OTP Keywriter Version: 02.00.00.00 (May 20 2026 - 16:02:05) OTP Keywriter ver: 10.1.4-v10.01.04a-1-gf7c27 (Fie Legacy Boot Mode Key programming sequence initiated Taking OTP certificate from 0x41c70004 Sciclient_otpProcessKeyCfg returns: -1 Debug response: 0x800 Key programming sequence completed	# Decrypting extensions.. # MPK Options: 0x21 MEK Options: 0x1 MPK Opt P1: 0x1 MPK Opt P2: 0x1 MEK Opt: 0x1 * SMPKH Part 1 BCH code: 61b45b59 * SMPKH Part 2 BCH code: 417d4cb4 * SMPK Hash (part-1,2): 1f6002b07cd9b0b7c47d9ca8d1aae57b8e8784a12f636b2b760d7d98a18f189701 60dfd0f23e2b0cb10ec7edc7c6edac3d9bdfefe0eddc3fff7fe9ad875195527d01 * SMEK BCH code: 21224fcc * SMEK Hash: 92785809a3dfefea57f6bbed642d730ba5d05e601222a72e815bf01ceb3a50f96ab85d282425f684436fabd4c7da624b791da411615035314103cc64e611f532 * BMPKH Part 1 BCH code: 81a4977b * BMPKH Part 2 BCH code: 613bf931 * BMPK Hash (part-1,2): b41865771ef3e13933568b1d1d50a72f5037a2a103c4535c713e10a61df1609c01 f6033117fbb56d5f190a17598e151141c6e413e2d853e56aae7997820639909b01 * BMEK BCH code: 21ec5cec * BMEK Hash: 21a5ae74b64b1c9fbd1f9201e60a319fe417edf06c2f9ba71fa3e1a967d171b684a4f85a83b8a4821abffe8e322b3697e299ffa94dec921bd4ac99f8ca59dd6c EXT OTP extension programming disabled MSV extension programming disabled * KEY CNT: 03030000 * KEY REV: 01010000 SWREV extension programming disabled FW CFG REV extension programming disabled * KEYWR VERSION: 0x20000 # # Programming Keys.. # * MSV: [u32] bch + msv: 0x8BAC0FFE MSV extension programming disabled [u32] bch + msv: 0x8BAC0FFE * SWREV: [u32] SWREV-SBL: 0x1 [u32] SWREV-SYSFW: 0x1 SWREV extension programming disabled [u32] SWREV-SBL: 0x1 [u32] SWREV-SYSFW: 0x1 * FW CFG REV: [u32] SWREV-FW-CFG-REV: 0x0 SWREV SEC BCFG extension programming disabled [u32] SWREV-FW-CFG-REV: 0x0 * EXT OTP: EXT OTP extension programming disabled * BMPKH, BMEK: Error in programming BMPKH part 1 debug_response: 0x800

5.2 软件包要求

确认正在使用最新的密钥写入器附加包，且该软件包可从安全资源获取。

5.3 eFuse 编程设置

在整个密钥预置过程中，VPP（编程电压）必须保持稳定。

5.4 验证编程结果

- 成功的 eFuse 编程会返回调试响应 0x0。在 MCU UART 上获取 R5 密钥写入器应用程序日志。以下参考日志显示密钥预置成功。

```
OTP Keywriter Version: 02.00.00.00 (Jul 19 2023 - 11:15:35)
OTP Keywriter ver: 9.0.7-v09.00.07 (Kool Koala)
OTP_VppEn
WKUP_GPIO0_54 output high
Key programming sequence initiated
Taking OTP certificate from 0x41c7f004
Debug response: 0x0
Key programming sequence completed
```

- 非零响应表示存在错误。有关具体错误代码的详细信息，请参阅 TISCI 文档。

5.5 引导失败故障排查

如果器件在 eFuse 编程后无法引导：

- 验证用于签名引导映像的密钥哈希值是否与编程到 OTP-eFuse 中的哈希值匹配。
- 从器件提取公钥哈希值，并与安全客户 MPK 哈希值（Sec Cust MPK Hash，即有效的信任根密钥哈希值）进行比较。

  要从器件提取公钥哈希值，请参阅常见问题解答。

5.6 无唤醒 UART 时的跟踪数据收集

- 如果器件上没有唤醒 UART，则使用跟踪缓冲区捕获 TIFS 跟踪数据。

6 总结

本应用手册全面概述了在生产环境中实现安全器件预置的密钥写入器部署策略。可以使用多种部署方法来适应不同的生产场景，包括从使用 OSPI 引导的汽车和工业应用程序到使用 eMMC 引导的大批量消费电子产品等。

工程师必须根据其具体的生产要求、数量和基础设施，选择合适的部署方法。正确理解证书生成、验证过程和常见调试步骤，有助于在实际环境中成功实施密钥写入器操作并排查其故障。

7 参考资料

1. 德州仪器 (TI)，*TISCI 密钥写入器用户指南*，用户指南。
2. 德州仪器 (TI)，*Jacinto7 高安全性器件开发*，应用手册。
3. 德州仪器 (TI)，*PDK 密钥写入器用户指南*，用户指南。

重要通知和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、与某特定用途的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他安全、安保法规或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的相关应用。严禁以其他方式对这些资源进行复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。对于因您对这些资源的使用而对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，您将全额赔偿，TI 对此概不负责。

TI 提供的产品受 TI 销售条款)、TI 通用质量指南 或 ti.com 上其他适用条款或 TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。 除非德州仪器 (TI) 明确将某产品指定为定制产品或客户特定产品，否则其产品均为按确定价格收入目录的标准通用器件。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

最后更新日期：2025 年 10 月