使用 TPDS 的 32 位 MCU 安全器件密钥配置

TB3374

简介

可信平台设计套件（Trust Platform Design Suite，TPDS）是一套全面的工具和服务，旨在辅助开发和部署安全可信的应用程序与系统。该套件包含一系列软件、硬件和服务，可将加密、身份验证和授权等安全功能集成到产品中。可信平台设计套件提供仿真环境、测试工具和认证流程，以确保应用程序满足所需的安全标准。该工具可简化安全系统的创建过程，降低实现安全可信功能的复杂度，同时满足与数据保护和隐私相关的监管和合规要求。

本文档说明了如何使用可信平台设计套件 v2（TPDS）在 32 位 MCU 安全器件上配置密钥。本密钥配置指南的目标是在安全元件内部编程、存储或写入密钥。作为示例，本文档参考了 PIC32CM LS60 单片机（MCU）。

目录

1. 使用可信平台设计套件在 PIC32CM LS60 Curiosity Pro 评估工具包上配置密钥

PIC32CM LS60 系列配备了安全、超低功耗的 PIC32CM LS60 Arm® Cortex®-M23 单片机。该 MCU 将 TrustFLEX ECC608 安全子系统和 Arm TrustZone®技术集成在单一封装中。此外，还具有增强型外设触摸控制器（Peripheral Touch Controller，PTC）以及智能模拟功能，例如运放、ADC、DAC 和模拟比较器。

注：在本文档的范围内，配置密钥时不会锁定安全元件中的插槽，以防止将来对这些插槽的访问被永久锁定。有关更多信息，请参见“ATECC608B Data Sheet”（*DS40002239*）。

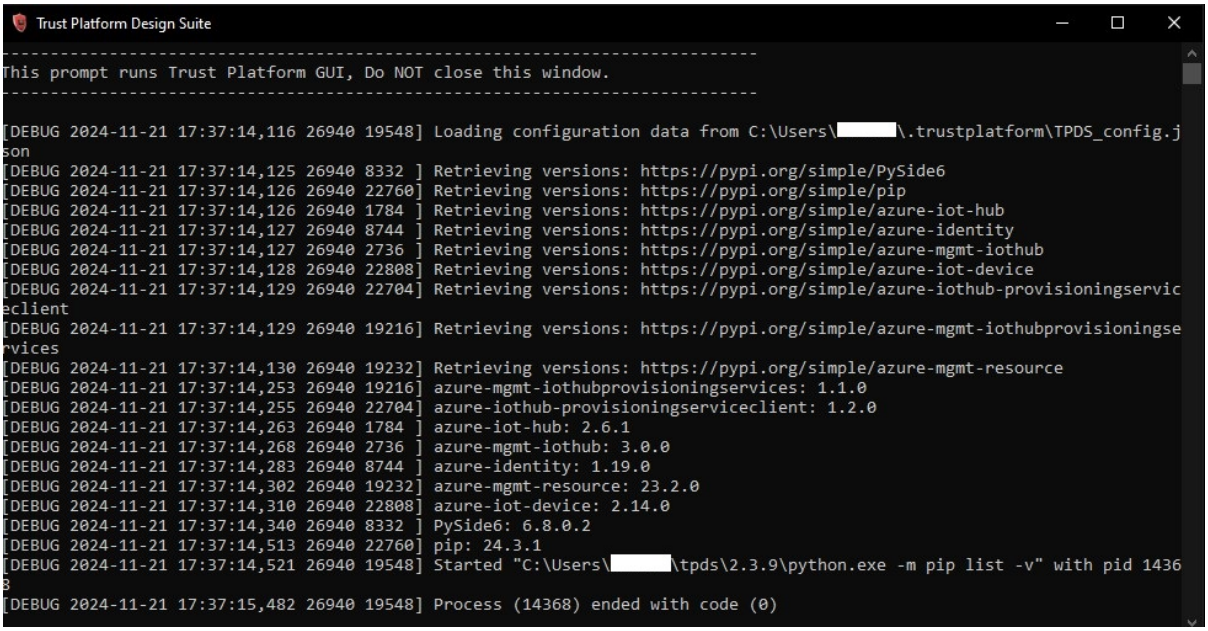
本演示使用以下软件和硬件工具：

- 可信平台设计套件 v2
- PIC32CM LS60 Curiosity Pro 评估工具包

要在 PIC32CM LS60 Curiosity Pro 评估工具包上配置密钥，请按照以下步骤操作：

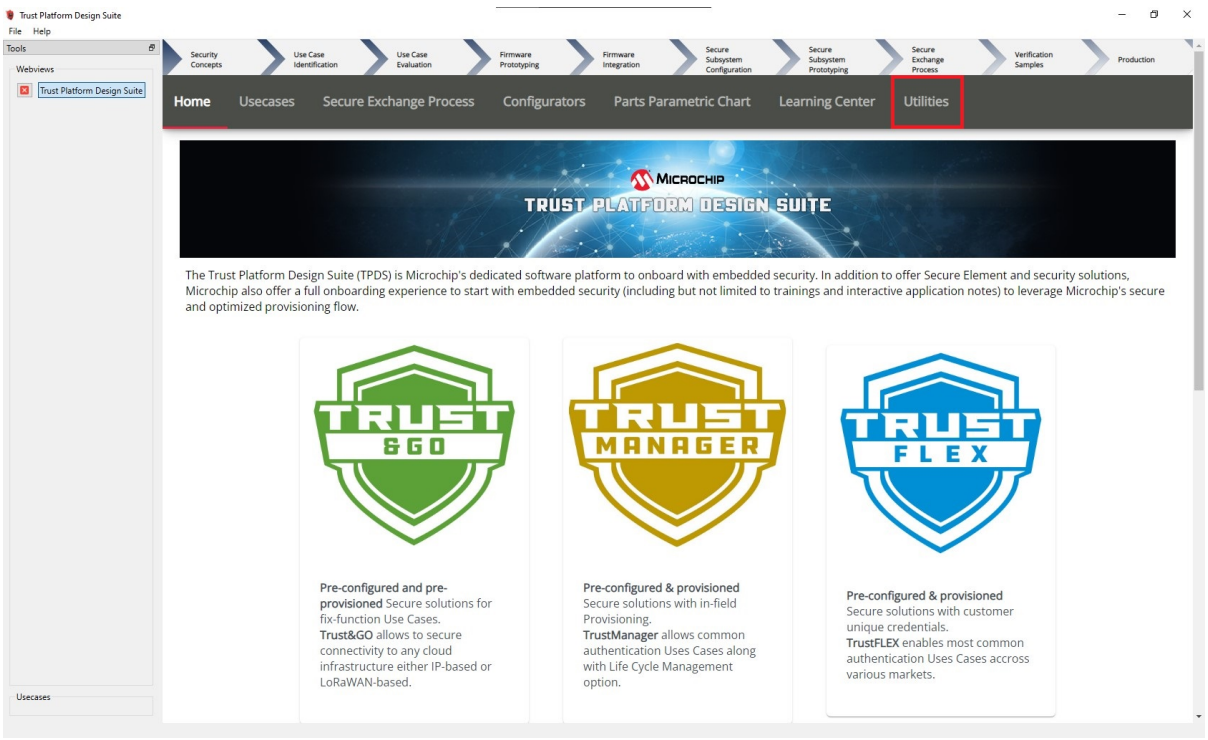
1. 从 **Start**（开始）菜单中，启动**可信平台设计套件**。

图 1-1. TPDS 启动控制台



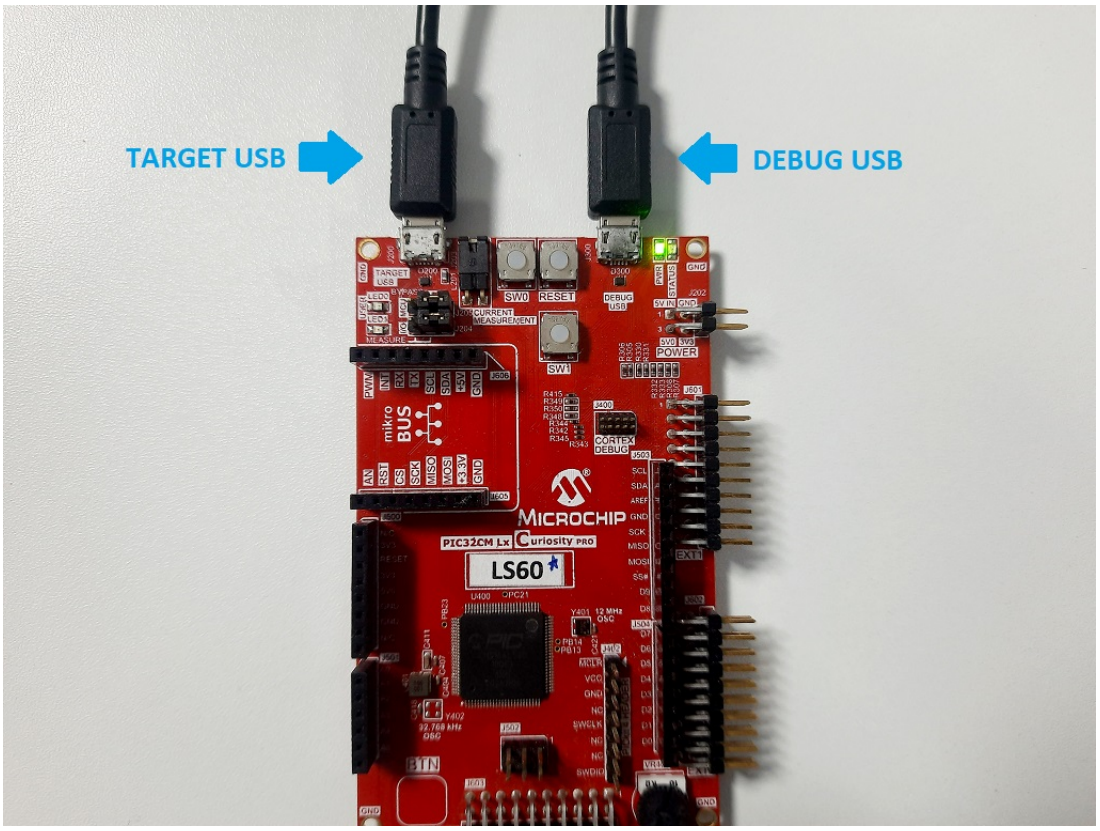
2. 打开 TPDS 后，单击 **Utilities**（实用工具）选项卡。

图 1-2. Preferences（首选项）配置



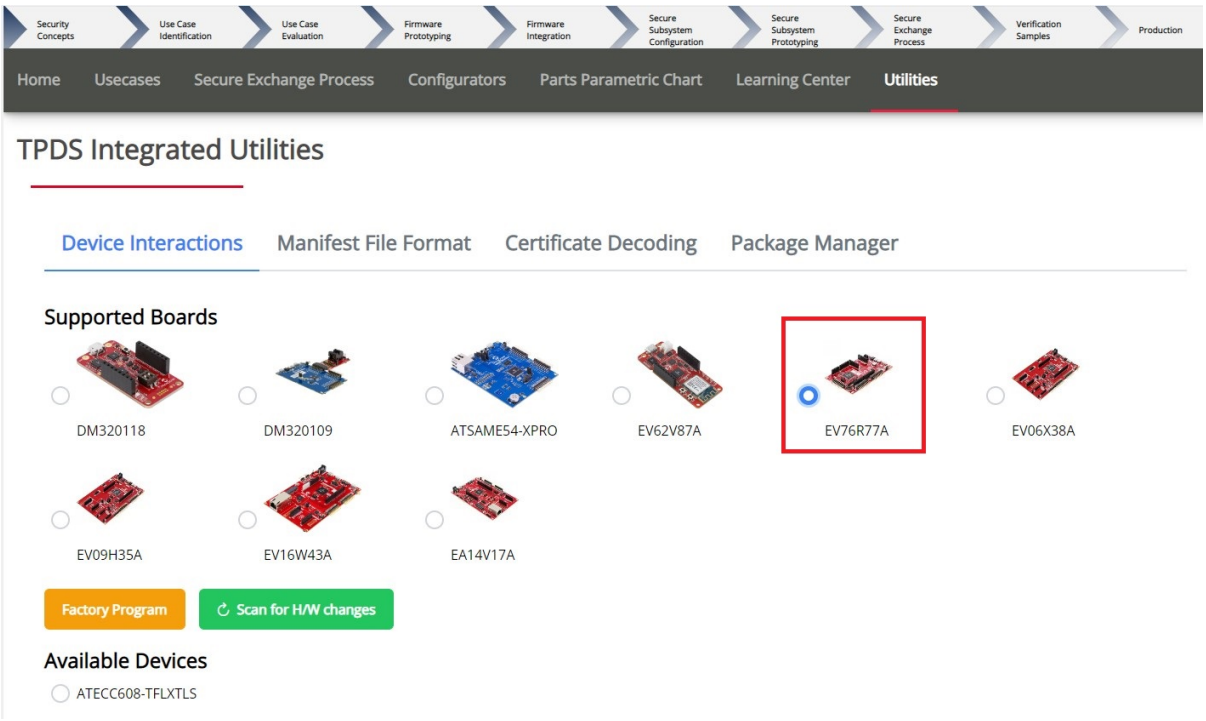
3. 连接两根 micro-USB 线缆：一根线缆从 PIC32CM LS60 Curiosity Pro 评估工具包上的 DEBUG USB 端口连接到 PC，另一根线缆从 PIC32CM LS60 Curiosity Pro 评估工具包上的 TARGET USB 端口连接到 PC。此配置允许通过 TPDS 进行密钥配置。

图 1-3. 硬件连接



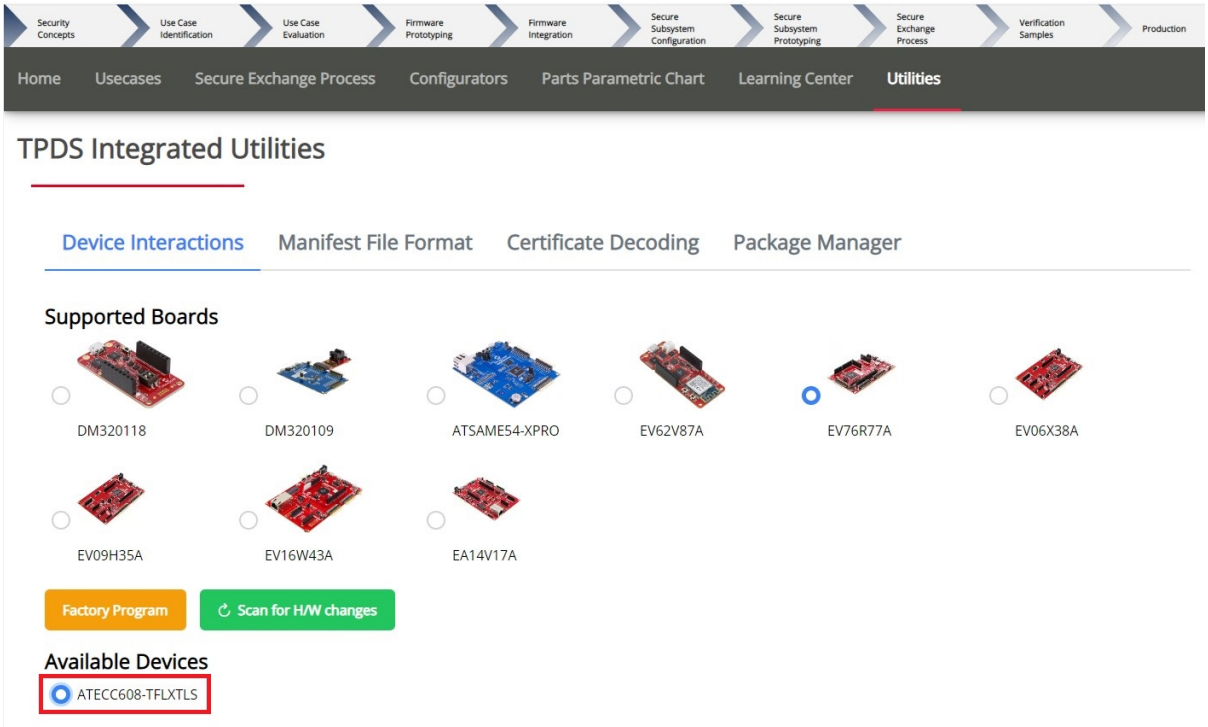
4. 在 TPDS Integrated Utilities（TPDS 集成实用工具）下，单击 **Device Interactions**（器件交互），然后在 Supported Boards（支持的开发板）下，选择 **EV76R77A**。
   注：EV76R77A 是 PIC32CM LS60 Curiosity Pro 评估工具包的部件编号。

图 1-4. 开发板选择



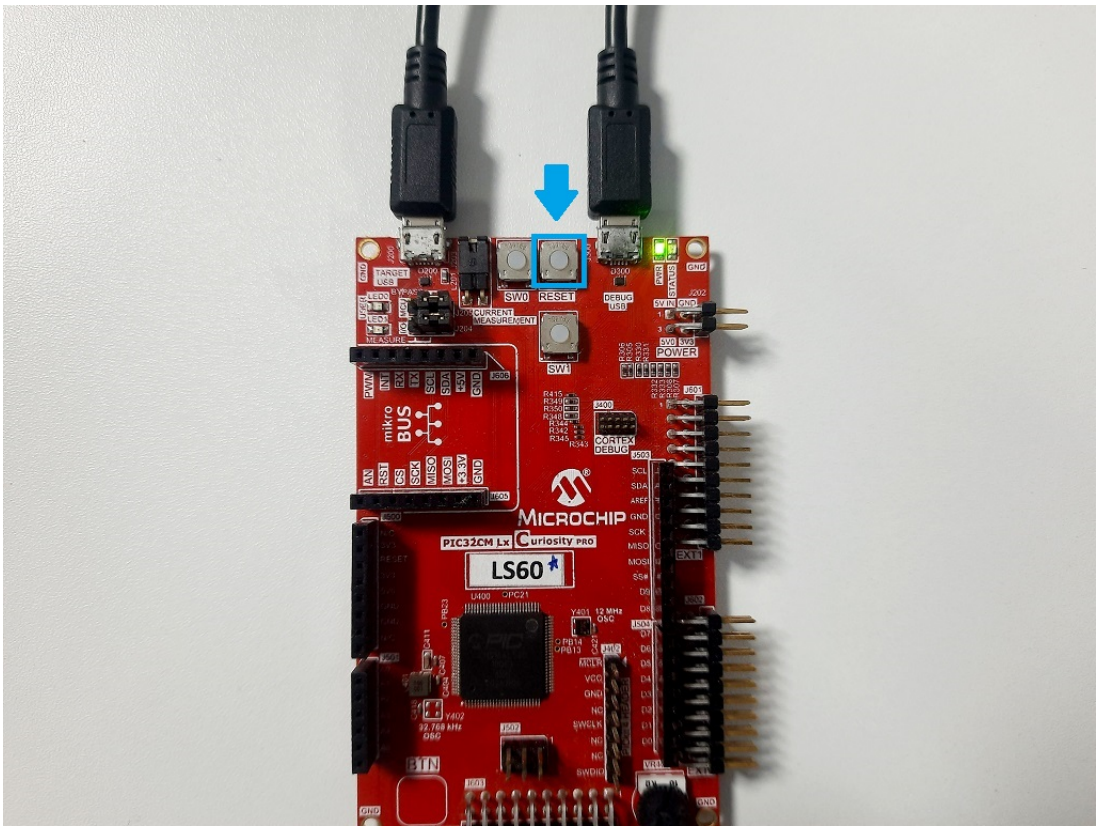
5. 从 **Available Devices**（可用器件）部分中，选择 **ATECC608-TFLXTLS**。

图 1-5. 选择 ATECC608-TFLXTLS



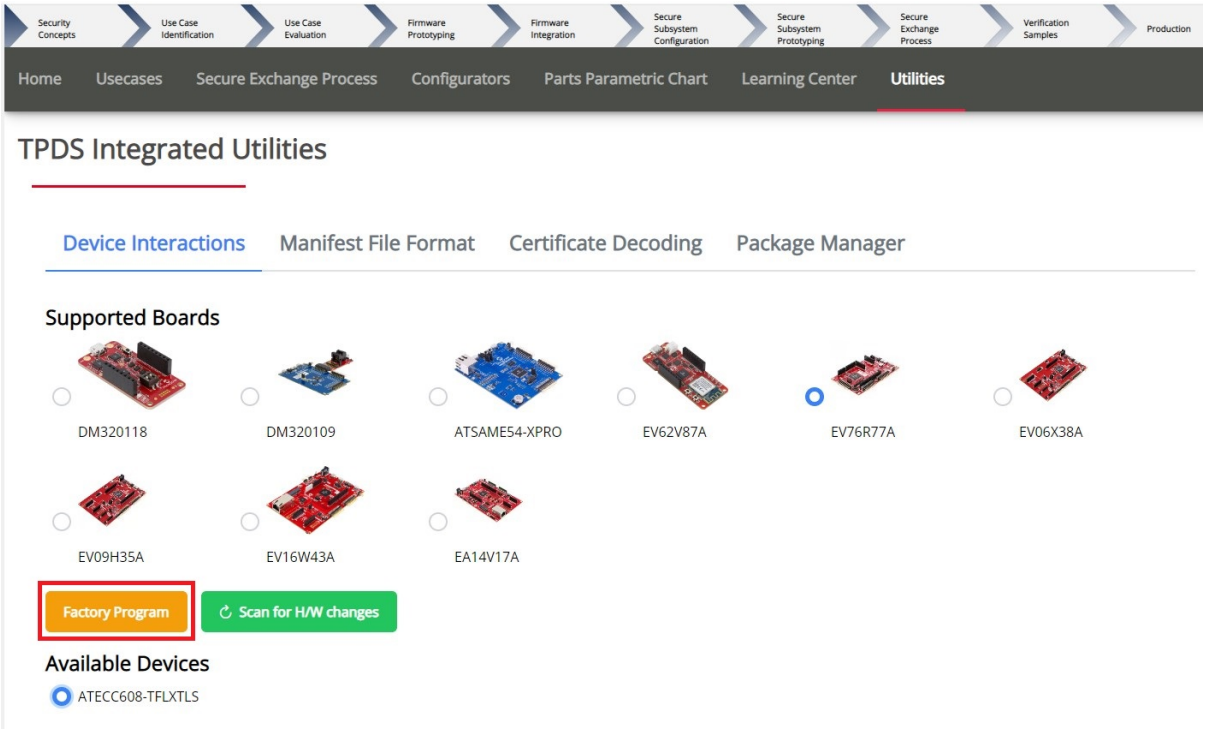
6. 按下 PIC32CM LS60 Curiosity Pro 评估工具包上的复位按钮以复位器件，如下所示。

图 1-6. 复位 PIC32CM LS60 Curiosity Pro 评估工具包



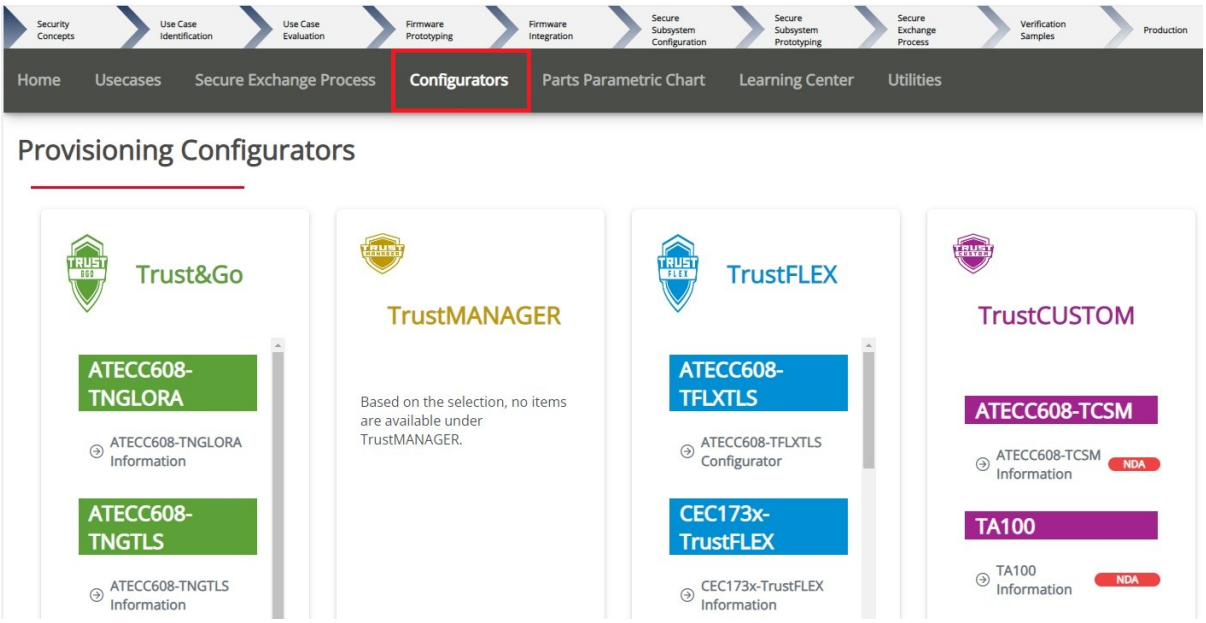
7. 单击 **Factory Program**（出厂程序）以在 PIC32CM LS60 Curiosity Pro 评估工具包上对密钥配置固件进行编程。

图 1-7. 密钥配置固件程序



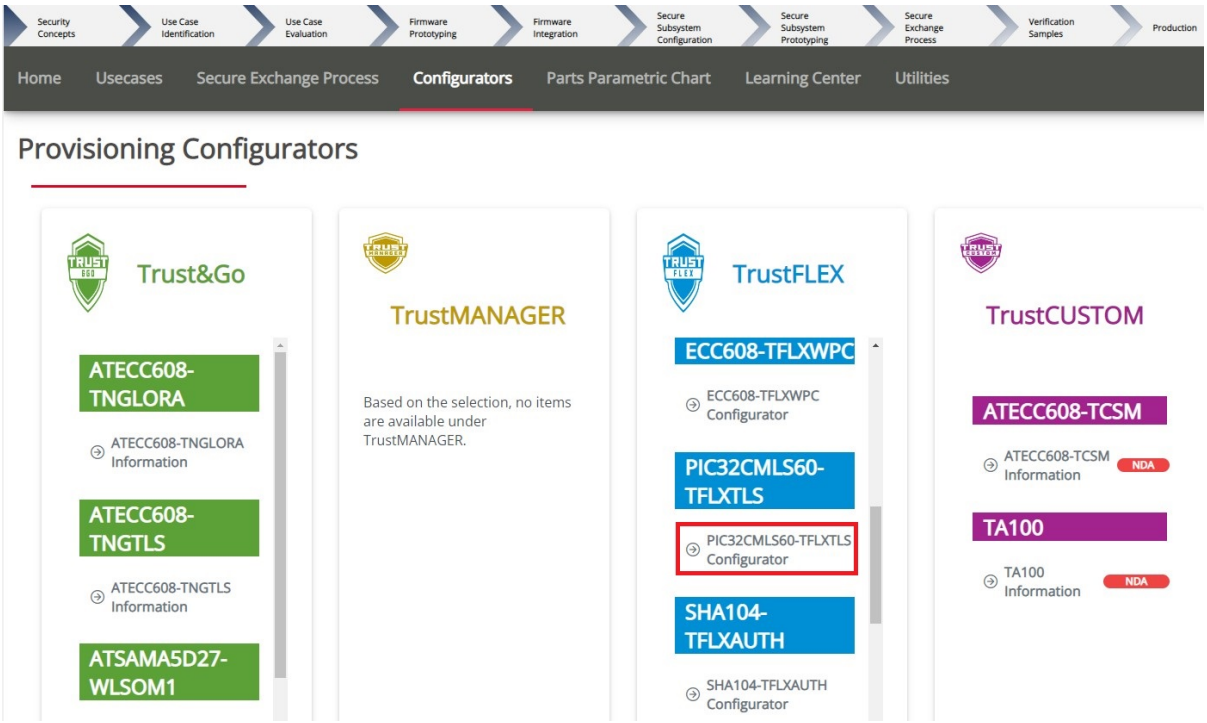
8. 编程成功完成后，单击 **Configurators**（配置器）选项卡。

图 1-8. 配置选择



9. 在 Provisioning Configurators（配置配置器）中的 TrustFLEX 部分下，单击 **PIC32CMLS60-TFLXTLS Configurator**（PIC32CMLS60-TFLXTLS 配置器）。

图 1-9. 选择 PIC32CMLS60-TFLXTLS 配置器



10. 在 PIC32CMLS60 TrustFLEX XML 生成器中选择 Slot 以配置密钥，如下所示。

图 1-10. Slot 5 选择

PIC32CMLS60 TrustFLEX XML Generator

PIC32CMLS60 Package:

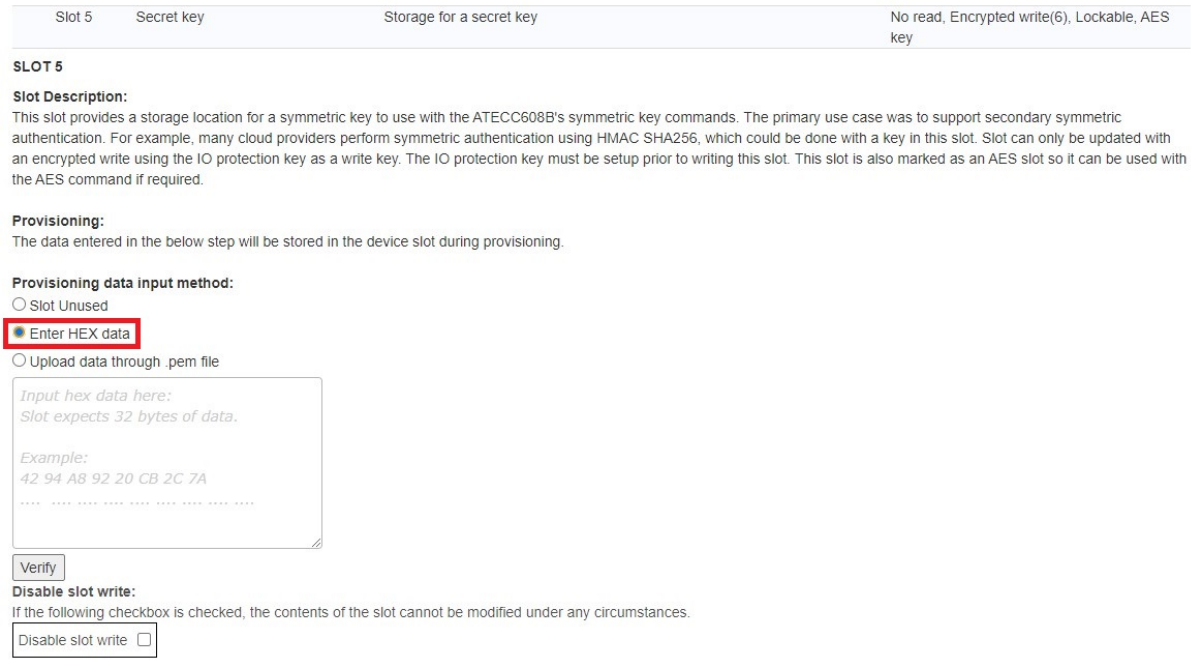
(•) I2C
( ) SWI

Click on table rows for more info.

Slot Number	Slot Use-case	Description	Slot Property
Slot 0	Primary private key	Primary authentication key	Permanent, Ext Sign, ECDH
Slot 1	Internal sign private key	Private key that can only be used to attest internal keys and state of the device. Can't be used to sign arbitrary messages.	Permanent, Int Sign
Slot 2	Secondary private key 1	Secondary private key for other uses	Updatable, Ext Sign, ECDH, Lockable
Slot 3	Secondary private key 2	Secondary private key for other uses	Updatable, Ext Sign, ECDH, Lockable
Slot 4	Secondary private key 3	Secondary private key for other uses	Updatable, Ext Sign, ECDH, Lockable
Slot 5	Secret key	Storage for a secret key	No read, Encrypted write(6), Lockable, AES key
Slot 6	IO protection key	Key used to protect the I2C bus communication (IO) of certain commands. Requires setup before use.	No read, Clear write, Lockable
Slot 7	Secure Boot digest	Storage location for Secure Boot digest. This is an internal function, so no reads or writes are enabled.	No read, No write
Slot 8	General data	General public data storage (416 bytes)	Clear read, Always write, Lockable
Slot 9	AES key	Intermediate key storage for ECDH and KDF output	No read, Always write, AES key
Slot 10	Device compressed certificate	Certificate primary public key in the Crypto Authentication compressed format	Clear read, No write
Slot 11	Signer public key	Public key for the CA (signer) that signed the device cert	Clear read, No write
Slot 12	Signer compressed certificate	Certificate for the CA (signer) certificate for the device certificate in the CryptoAuthentication compressed format	Clear read, No write

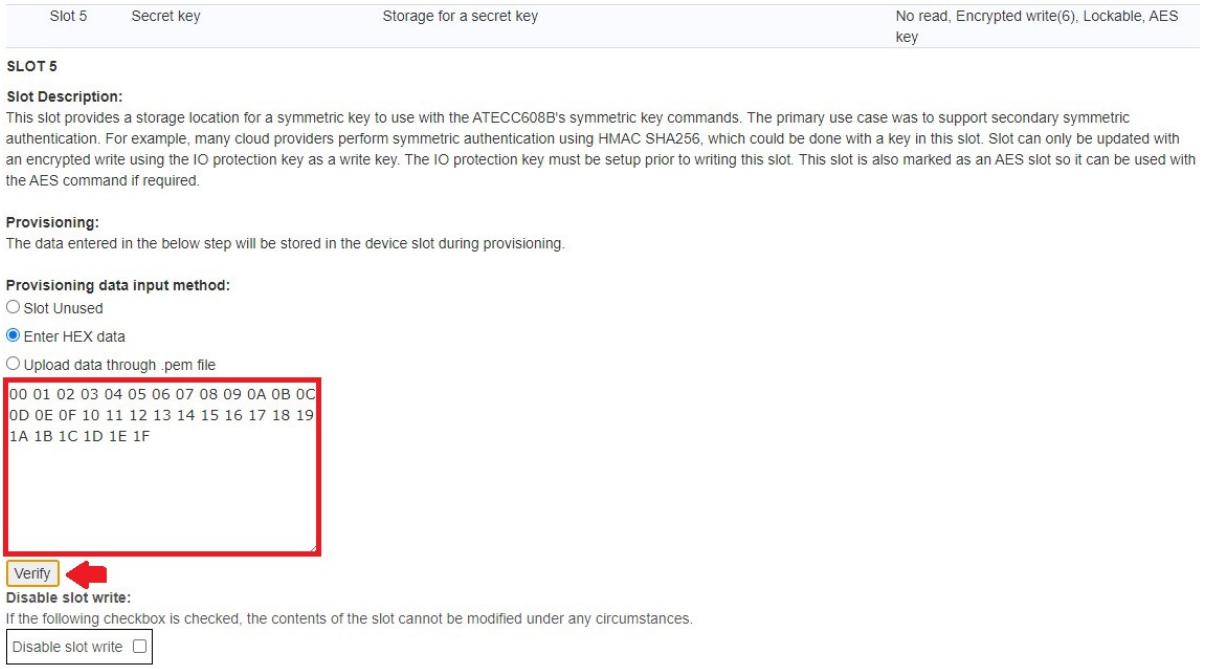
11. 在 Slot 5 部分中选择 **Enter HEX data**（输入 HEX 数据）。

图 1-11. Slot 5 中的 HEX 数据选项



12. 在输入部分以随机十六进制值的形式输入*密钥*，然后单击 **Verify**（验证）以验证数据长度。

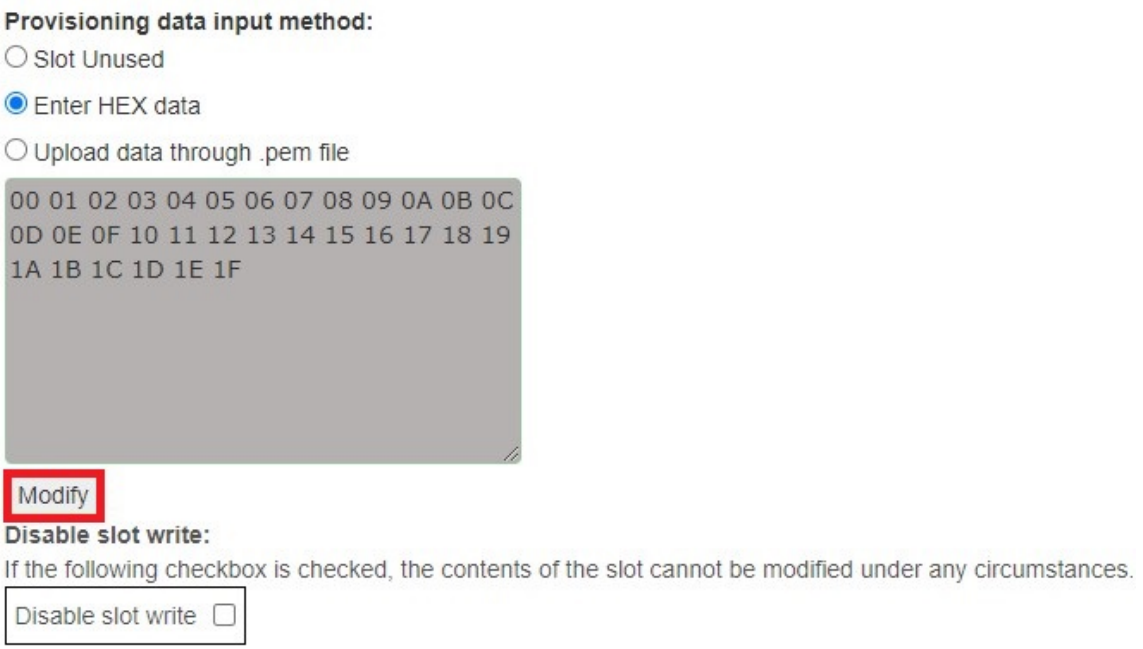
图 1-12. 输入密钥



注：

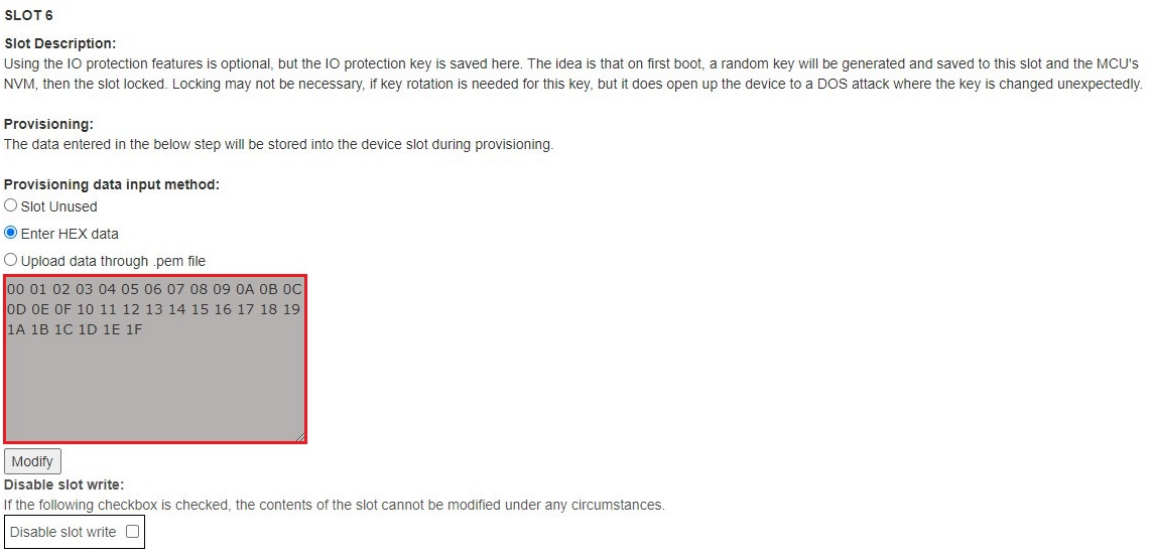
- 单击 **Modify**（修改）以更改 Slot 5 的内容。

图 1-13. Slot 5 内容修改



- 在这种情况下，密钥（Slot 5）依赖于 Slot 6 中的 I/O 保护密钥。这种依赖性至关重要，因为必须保护该密钥免受物理攻击。请确保按照步骤 10 到 12 中定义的流程，正确添加 I/O 保护密钥的取值。

图 1-14. 输入 I/O 保护密钥



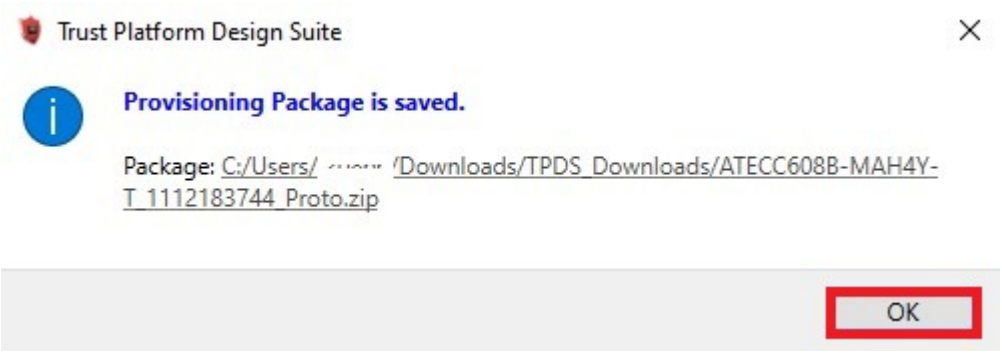
13. 向下滚动并单击 Prototyping（原型设计）部分中的 **Generate Provisioning Package**（生成配置包）。

图 1-15. 配置包生成

注：在原型设计包中，为配置包生成的 XML 中的所有用户数据均为未加密的明文。如需获得加密的配置包，请使用生产（Production）包。

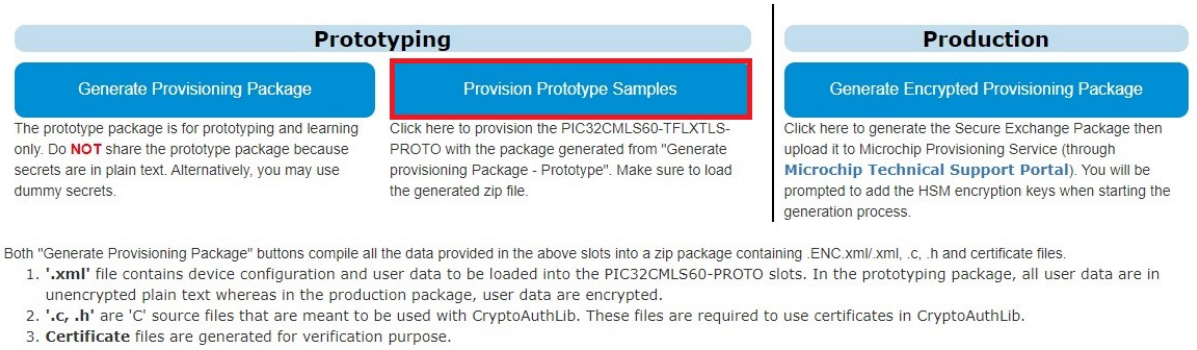
14. 配置包保存在以下位置：*Users/xxx/Downloads/TPDS_Downloads*。
15. 选择所需的 Provisioning Package（配置包），然后单击 **OK**（确定）。

图 1-16. 配置包位置



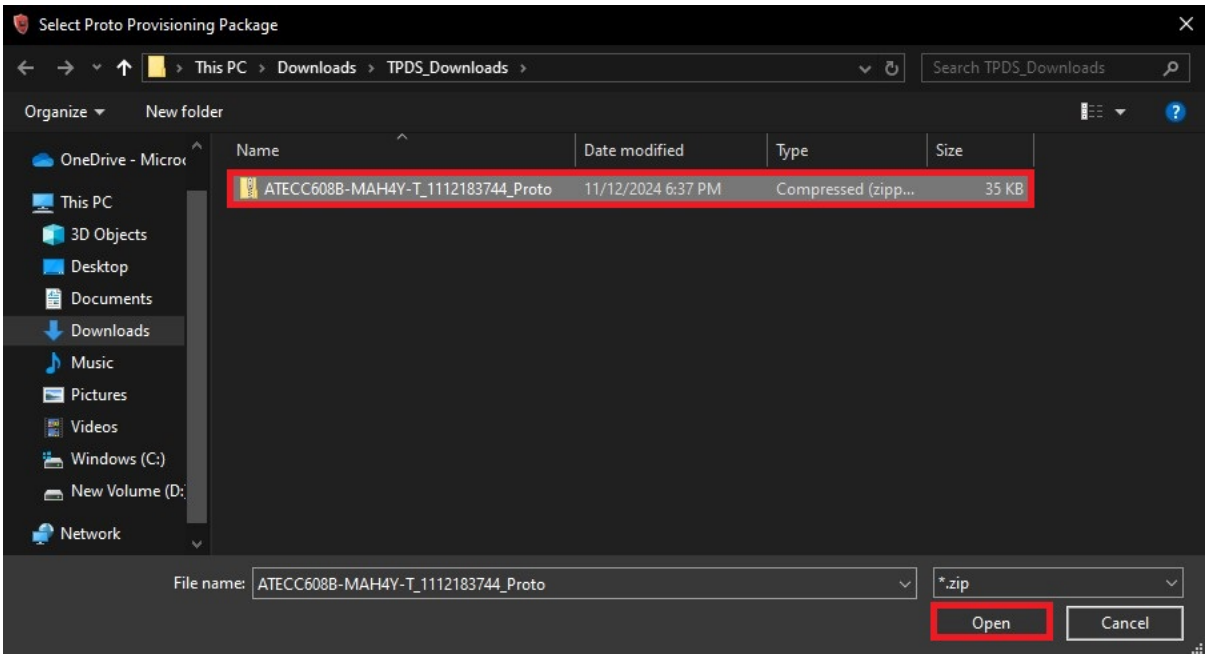
16. 单击 **Provision Prototype Samples**（配置原型样片）以在安全元件内部编程密钥。

图 1-17. 配置密钥



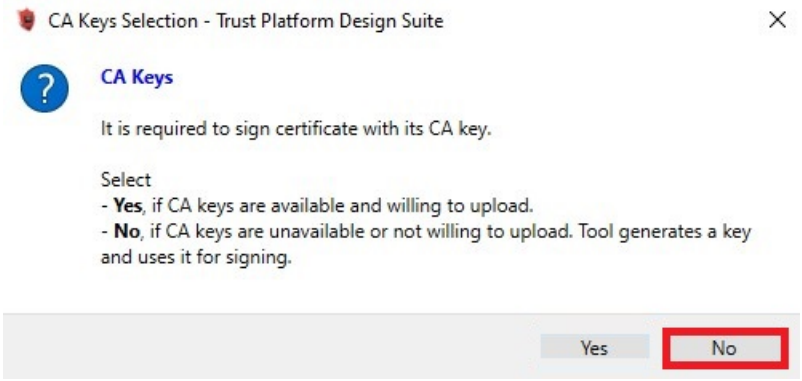
17. 转到配置包下载位置：*Users/xxx/Downloads/TPDS_Downloads*，选择 **ATECC608-***.zip** 文件，然后单击 **Open**（打开）。

图 1-18. 导航到配置包位置



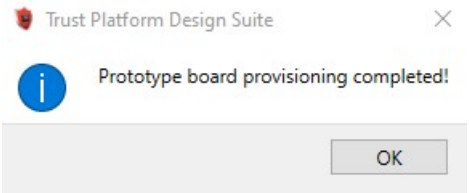
18. 选择 **No**（否）以使用 TPDS 工具生成 CA 密钥。

图 1-19. 导航到配置包位置



19. 将提示以下消息以指示密钥配置已完成。

图 1-20. 完成密钥配置



2. 总结

通过利用 TPDS 的密钥配置功能，密钥可存储在安全元件或硬件安全模块（Hardware Security Module，HSM）内的一个安全、防篡改的环境中。它使用户能够存储和管理对于各种安全功能（如加密、身份验证和安全通信）至关重要的加密密钥。

3. 资源

- 可信平台设计套件 v2
- 若要安装可信平台设计套件（TPDS）v2，请参见：
  - developerhelp.microchip.com/xwiki/bin/view/applications/security/trust-platform-v2/
- PIC32CM LS60 Curiosity Pro 评估工具包

4. 版本历史

版本 A——2025 年 4 月

这是本文档的初始版本。

Microchip 信息

商标

“Microchip”的名称和徽标组合、“M”徽标及其他名称、徽标和品牌均为 Microchip Technology Incorporated 或其关联公司和/或子公司在美国和/或其他国家或地区的注册商标或商标（“Microchip 商标”）。有关 Microchip 商标的信息，可访问 https://www.microchip.com/en-us/about/legal-information/microchip-trademarks。

ISBN： 979-8-3371-3057-6

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。您须自行确保应用符合您的规范。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。

Microchip“按原样”提供这些信息。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，包括但不限于针对非侵权性、适销性和特定用途的适用性的暗示担保，或针对其使用情况、质量或性能的担保。

在任何情况下，对于因这些信息或使用这些信息而产生的任何间接的、特殊的、惩罚性的、偶然的或附带的损失、损害或任何类型的开销，Microchip 概不承担任何责任，即使 Microchip 已被告知可能发生损害或损害可以预见。在法律允许的最大范围内，对于因这些信息或使用这些信息而产生的所有索赔，Microchip 在任何情况下所承担的全部责任均不超出您为获得这些信息向 Microchip 直接支付的金额（如有）。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损害、索赔、诉讼或费用时，会维护和保障 Microchip 免于承担法律责任。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。

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。