Application Note

如何创建认证密钥并将其编程到 TI 电池电量监测计中

Kipp Hayes

摘要

大多数德州仪器 (TI) 电池电量监测计产品都支持电池组防伪认证。本应用手册介绍了以下几点：使用 BQKEYPACKAGER 创建 SHA 或 ECC 密钥的过程，使用 BQKEYPROGRAMMR 将选定的密钥编程到电量监测计中的过程，有关在生产环境中对密钥进行编程的指导。

使用这两个独立工具的目的是让 OEM 能够在一个文件中加密认证密钥，并将其发送至电池组制造商。然后，电池组制造商可以将该文件用作一个数据源，以便支持 BQKEYPROGRAMMER 将密钥编程到电量监测计中。因此，电池组制造商无法看到密钥。

- BQKEYPACKAGER
- BQKEYPROGRAMMER
- BQSTUDIO

内容

商标

1 使用 BQKEYPACKAGER 生成密钥文件

BQKEYPACKAGER 仅供 OEM 使用以用于封装打包身份验证密钥。输入身份验证密钥时，需要同时输入一个密码，用于在算法中对文件进行加密。使用 BQKEYPROGRAMMER 或 BQSTUDIO 进行测试后，OEM 可将创建的文件和密码发送给电池组制造商。德州仪器 (TI) 电池电量监测计具有 3 种身份验证方法：SHA1、SHA256 和 ECC。

BQKEYPACKAGER 工具的输出是一个 .bqk 文件。该文件是使用此工具生成的密钥经过加密后的输出结果。对于封装的 .bqk 文件，有 2 个输出选项。可以是一个包含完整密钥的单个文件，也可以是两个单独的文件（每个文件各包含密钥的一半，即密钥的 F 部分和 C 部分）。在生产环境中对密钥进行编程时，可以一次编程一半密钥，也可以同时对两部分密钥进行编程。因此，在生产过程中，密钥的不同部分能够在不同的时间和地点分别进行编程。例如，在您的一个生产流程中，电池组要经过两家制造商的处理。可以为每个制造商都分配一半的密钥用于编程到电量监测计中。由此可以提高密钥的安全性，只有 OEM 或设计人员拥有完整密钥，任何制造商都只拥有部分密钥。

备注

德州仪器 (TI) 对于分别使用 BQKEYPACKAGER 或 BQKEYPROGRAMMER 进行封装或编程的任何密钥的安全性概不负责。用户有责任确保密钥的安全，并对能够访问密钥任何部分的各方数量加以限制。

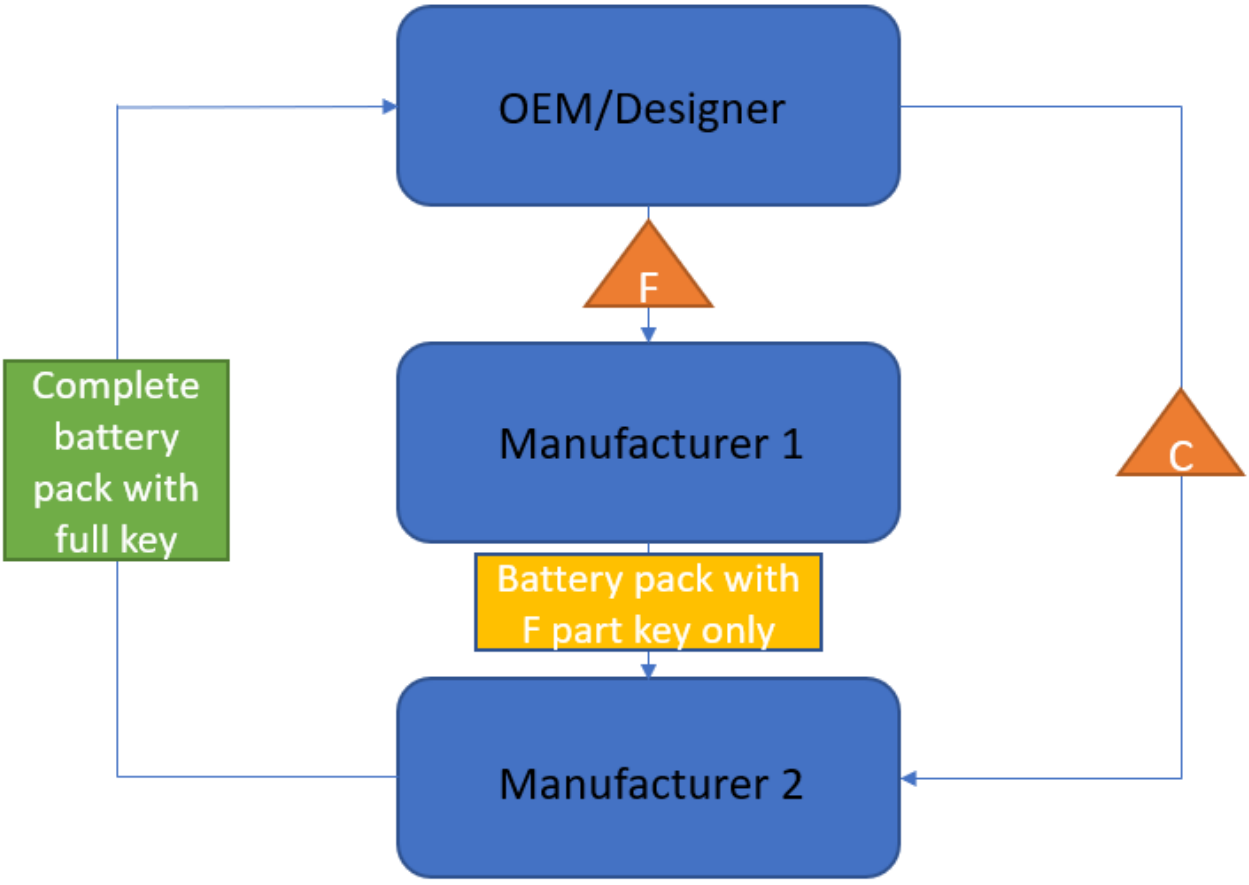

图 1-1. 密钥拆分生产示例

1.1 SHA1 流程

第 1 步：下载并安装 BQKEYPACKAGER。

第 2 步：打开 BQKEYPACKAGER 并选择正确的身份验证方案和相应的器件。本示例选择了 SHA1 密钥 BQ40Z80。

第 3 步：分别输入 SHA1 身份验证密钥 Key F 和 Key C 部分，这两个部分各占最终密钥的一半。在本例中，Key F 为 *AAAA1111BBBB2222CCCC3333DDDD4444EEEE5555*，Key C 为 *FFFF66667777888899990000AAAA1111BBBB2222*。

第 4 步：为生成的 .bqk 文件输入一个密码，并输入任何想要在 BQKEYPROGRAMMER 中显示的注释内容。对于本示例，密码为 *example1234567890*，注释为 *example*。

第 5 步：选择 *Create bqKey file*，然后选择输出目标位置和文件名。

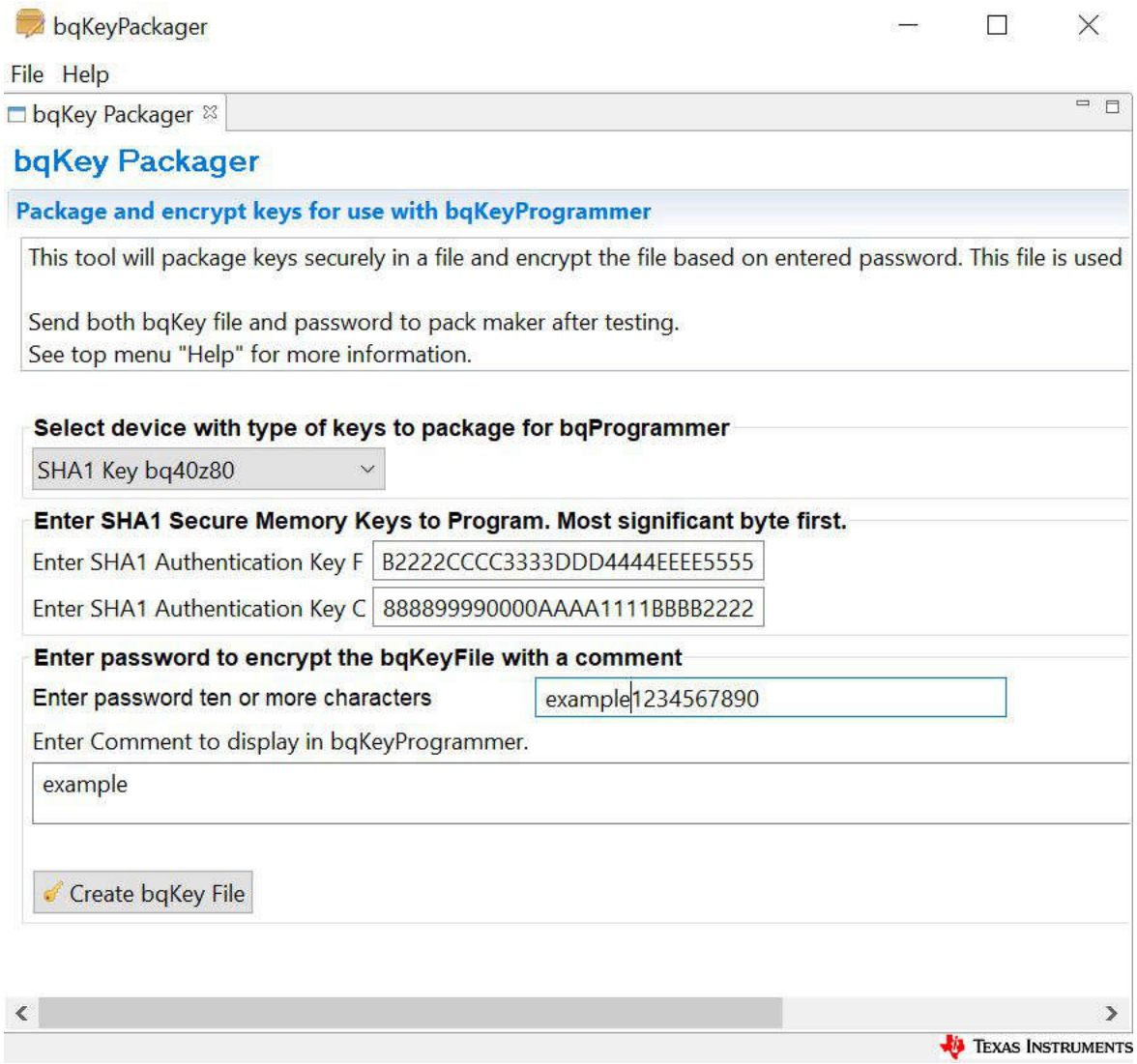

图 1-2. 使用 BQ40Z80 的 SHA1 示例

1.1.1 如何计算 SHA1 密钥

首先，按照与发送时相反的字节顺序，计算发送到电量监测计的 20 字节 Key F 的 SHA-1 哈希值。Key F 是最后 8 个字节。Key C 使用相同的步骤。最后一个密钥是附加到 Key F 的 Key C。

示例：

如果 2309BDC0A9F86B69111CA850B530339111000C47（小端）用于 KeyF

用于查找 keyF 的 SHA-1 哈希值输入：470C0011913330B550A81C11696BF8A9C0BD0923（大尾序）

SHA-1 哈希值输出：8877626BD64ABC4843E43F1E42C5413DB9EDBBA2

如果 330C0014913530B550A81D10696BF8A9C7BD0613（小端）用于 KeyC

用于查找 keyC 的 SHA-1 哈希值输入：1306BDC7A9F86B69101DA850B530359114000C33（大尾序）

SHA-1 哈希值输出：1B8689D48F55F5B5F81D30E012DFB96B7440433C

KeyF = 42C5413DB9EDBBA2，KeyC = 12DFB96B7440433C

针对全为 0 的挑战码的 SHA-1 哈希值输入：

KeyF + KeyC + 挑战码 =
42C5413DB9EDBBA212DFB96B7440433C00000000000000000000000000000000000000000000

响应：1625A385F73436792FD693D727BAC6EE47291D0B

第二个哈希值是第一个哈希值的响应并附加到密钥：

KeyF + KeyC + 第一个哈希值的响应 =
42C5413DB9EDBBA212DFB96B7440433C1625A385F73436792FD693D727BAC6EE47291D0B

响应：B0BEF440CAC492FAF09604A46C2C0996512331AF

在使用全 0 挑战码后，此响应需要与从电量监测计接收到的数据相对应。

1.2 SHA256 流程

对于 SHA256 而言，有两种生成密钥的方式，一种是输入 2 个挑战码，然后根据这些挑战码生成密钥；另一种是输入一个预先生成的密钥。

第 1 步：下载并安装 BQKEYPACKAGER。

第 2 步：打开 BQKEYPACKAGER 并选择正确的身份验证方案和相应的器件。在本示例中，我们选择了 SHA256 密钥 BQ9035。

第 3 步：输入 2 个挑战码或一个预先生成的密钥。在本例中，2 个挑战码输入分别为 *1234567890123456789012345678901234567890* 和 *09876543210987654321098765432109876543210987*。在本例中，预先生成的密钥为 *AAAA1111BBBB2222CCCC3333DDDD4444EEEE5555FFFF66667777888899990000*。

第 4 步：为生成的 .bqk 文件输入一个密码，并输入任何想要在 BQKEYPROGRAMMER 中显示的注释内容。对于这些示例，密码为 *example1234567890*，注释为 *example*。

第 5 步：选择 *Create bqKey file*，然后选择输出目标位置和文件名。如果使用 SHA256 挑战码方法，在创建文件之后，会弹出一个显示完整生成密钥的窗口。在本例中，输出密钥为 *CA1194A558362B5FA6E7887DA7B41EC65481031C133249274853B0559D887BA3*。

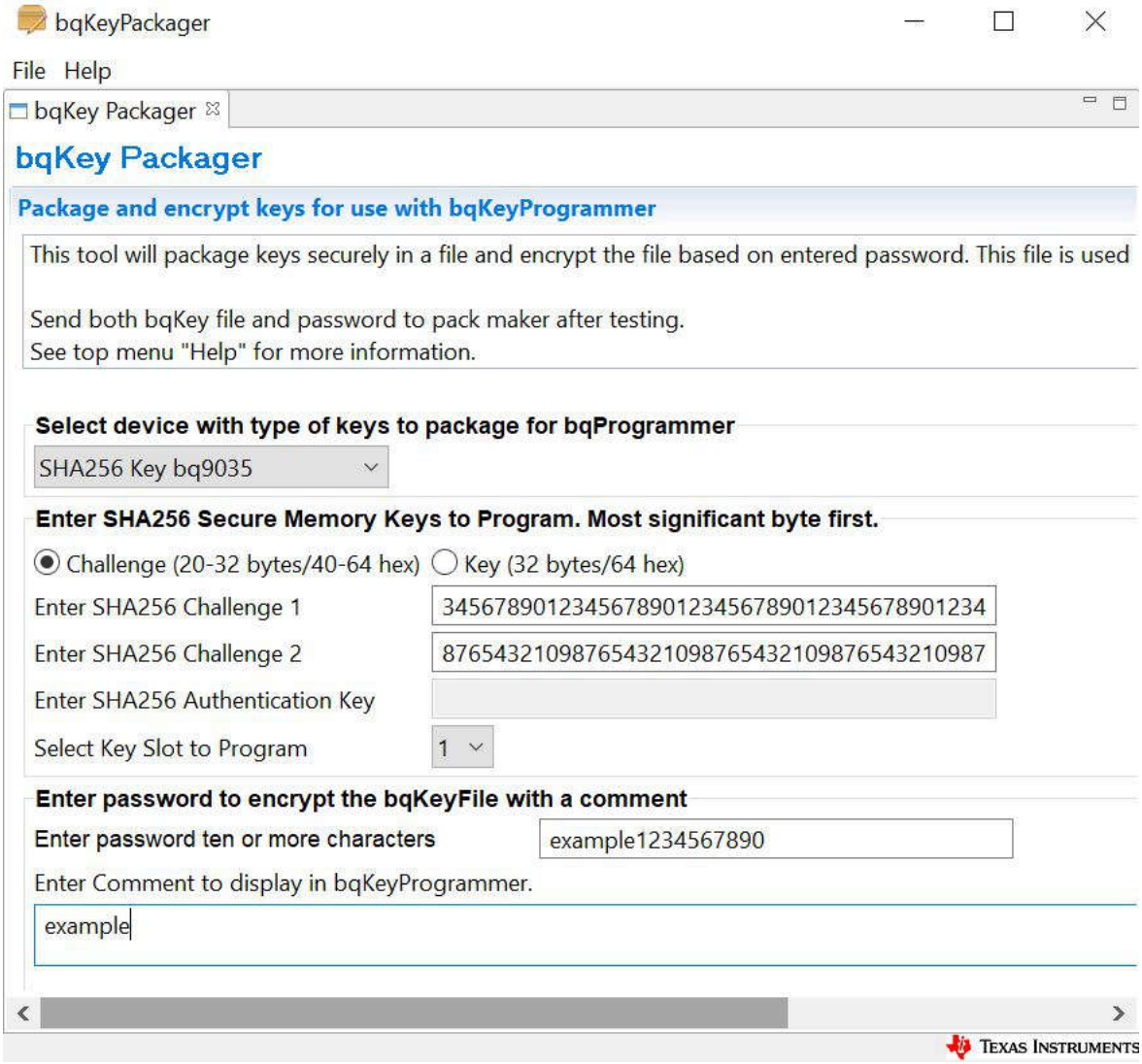

图 1-3. 使用 BQ9035 的 SHA256 挑战码示例

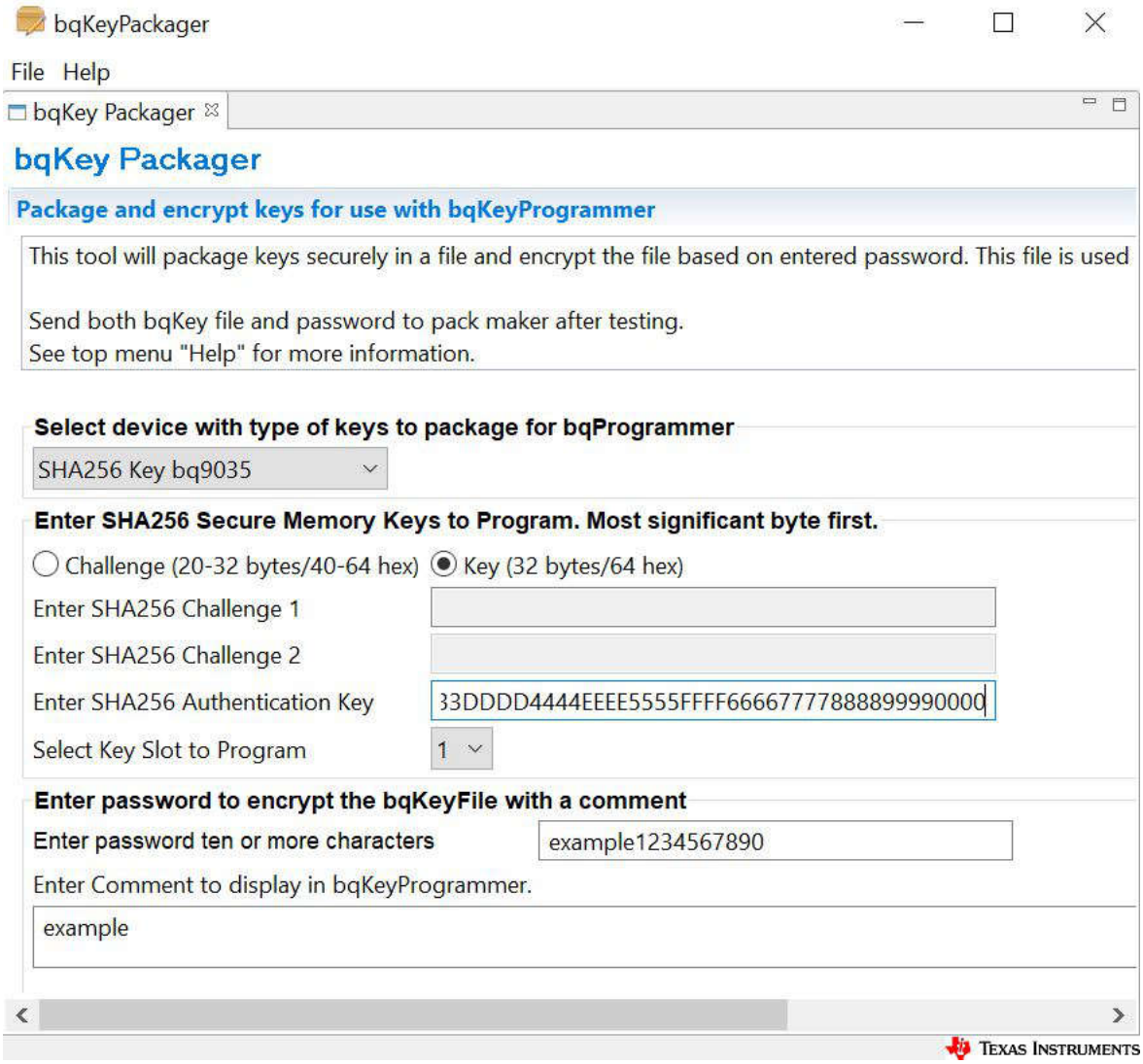

图 1-4. 使用 BQ9035 的 SHA256 密钥示例

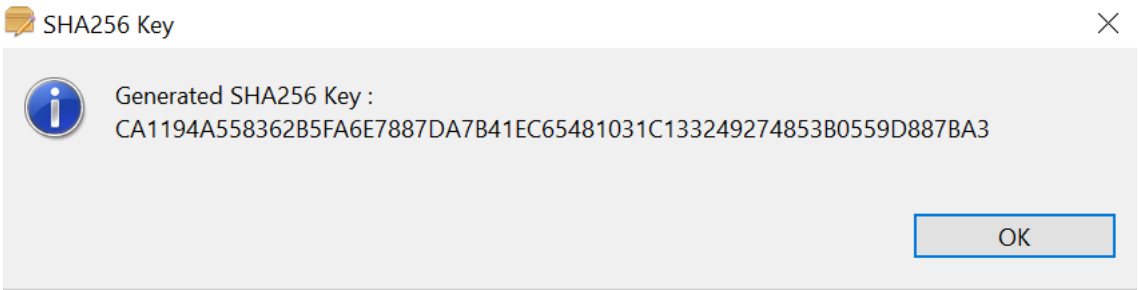

图 1-5. SHA256 生成的密钥输出

1.3 ECC 流程

ECC 密钥是成对提供的，包含私钥和匹配的公钥。每个密钥的长度为 163 位。

需要将这两个密钥都编程到电量监测计中，才能运行 ECC 身份验证。私钥（ECC 身份验证的机密）拆分为两个部分（称为 KeyF 和 KeyC）。每一半的密钥都可以由不同的实体（例如 TI、电池组制造商或系统制造商）进行编程。通过这种将密钥拆分后进行编程的方式，OEM 成为唯一知晓私钥实际值的一方，而任何进行编程的实体仅掌握私钥的部分信息。

第 1 步：下载并安装 BQKEYPACKAGER。

第 2 步：打开 BQKEYPACKAGER 并选择正确的身份验证方案和相应的器件。在本示例中，我们选择了 ECC 密钥 BQ40Z80。

第 3 步：输入身份验证密钥 Key F + Key C，在此示例中，密钥为 *AAAA1111BBBB2222CCCC3333DDDD4444EEEE5555FF*。输入公钥，在此示例中，密钥为 *FF6666777788889999000AAAA1111BBBB2222CCCC*。

第 4 步：为生成的 .bqk 文件输入一个密码，并输入任何想要在 BQKEYPROGRAMMER 中显示的注释内容。对于这些示例，密码为 *example1234567890*，注释为 *example*。

第 5 步：选择 *Create bqKey file*，然后选择输出目标位置和文件名。

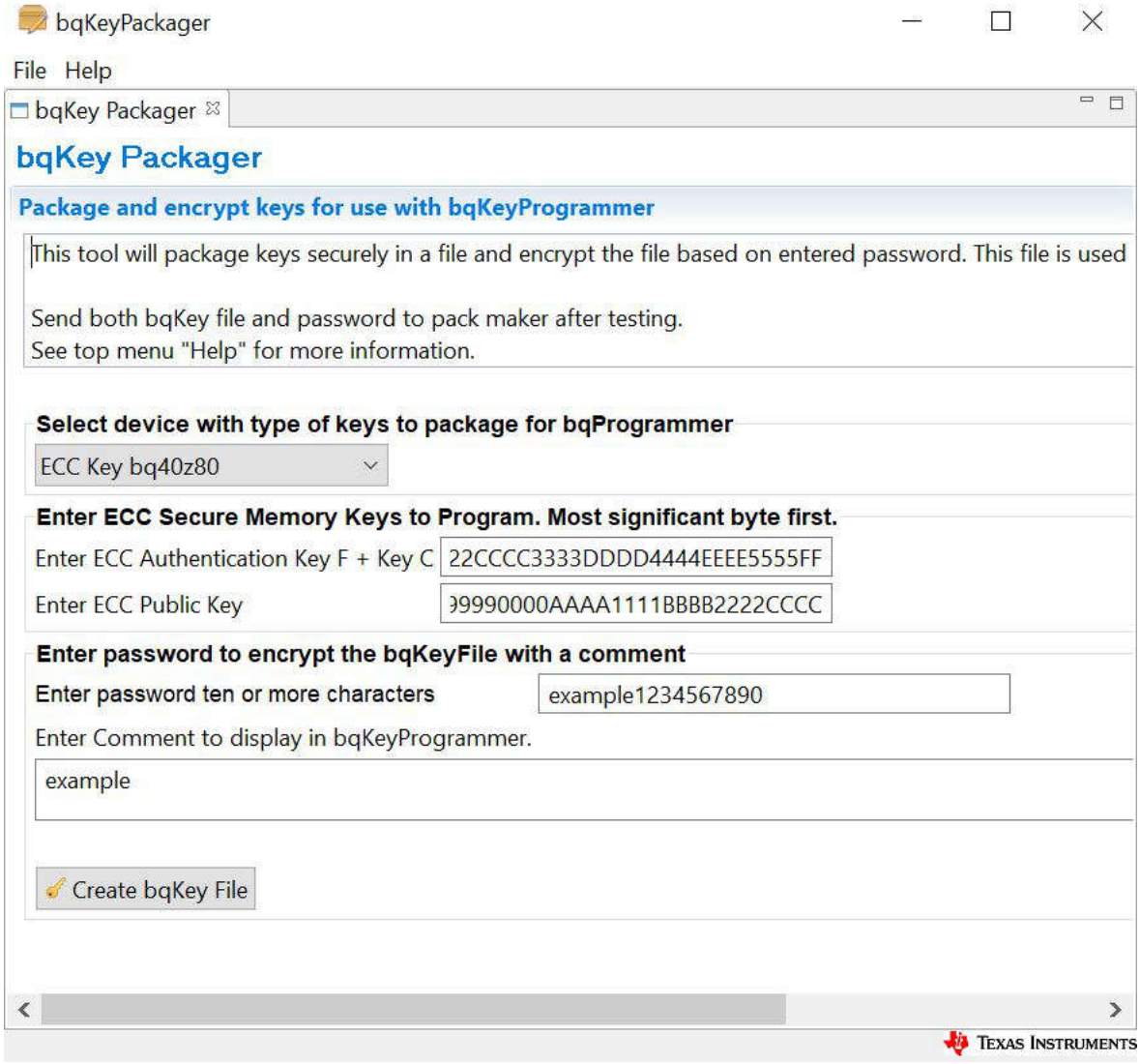

图 1-6. 使用 BQ40z80 的 ECC 示例

2 使用 BQKEYPROGRAMMER 将密钥编程到电量监测计中

BQKEYPROGRAMMR 可对 OEM 提供的 bqKey 文件中封装的信息进行编程，然后放入受支持的电量监测计中的安全一次性可编程存储器中。此工具需要一个可正常工作的带有驱动程序的 EV2x00 通信适配器，并需要将兼容的电量监测计连接到该适配器的通信端口。

第 1 步：将 EV2x00 连接至计算机。

第 2 步：通过器件的正确通信端口（SMBus、I2C、HDQ），将目标电量监测计连接到 EV2x00。

第 3 步：安装并打开 BQKEYPROGRAMMER。

第 4 步：点击 *Select File* 并选择 .bqk 文件。

第 5 步：输入密码，本例中的密码为“example12345678”。

第 6 步：点击 *Load File*，如果注释出现在注释框中，则表示文件已成功加载。

第 7 步：**编程操作仅能进行一次，且无法撤销。**点击 *Program Key*，如果密钥编程成功，应该会出现一个绿色方框，其中显示 *Key Programmed and verified Passed*，如 图 2-1 所示。

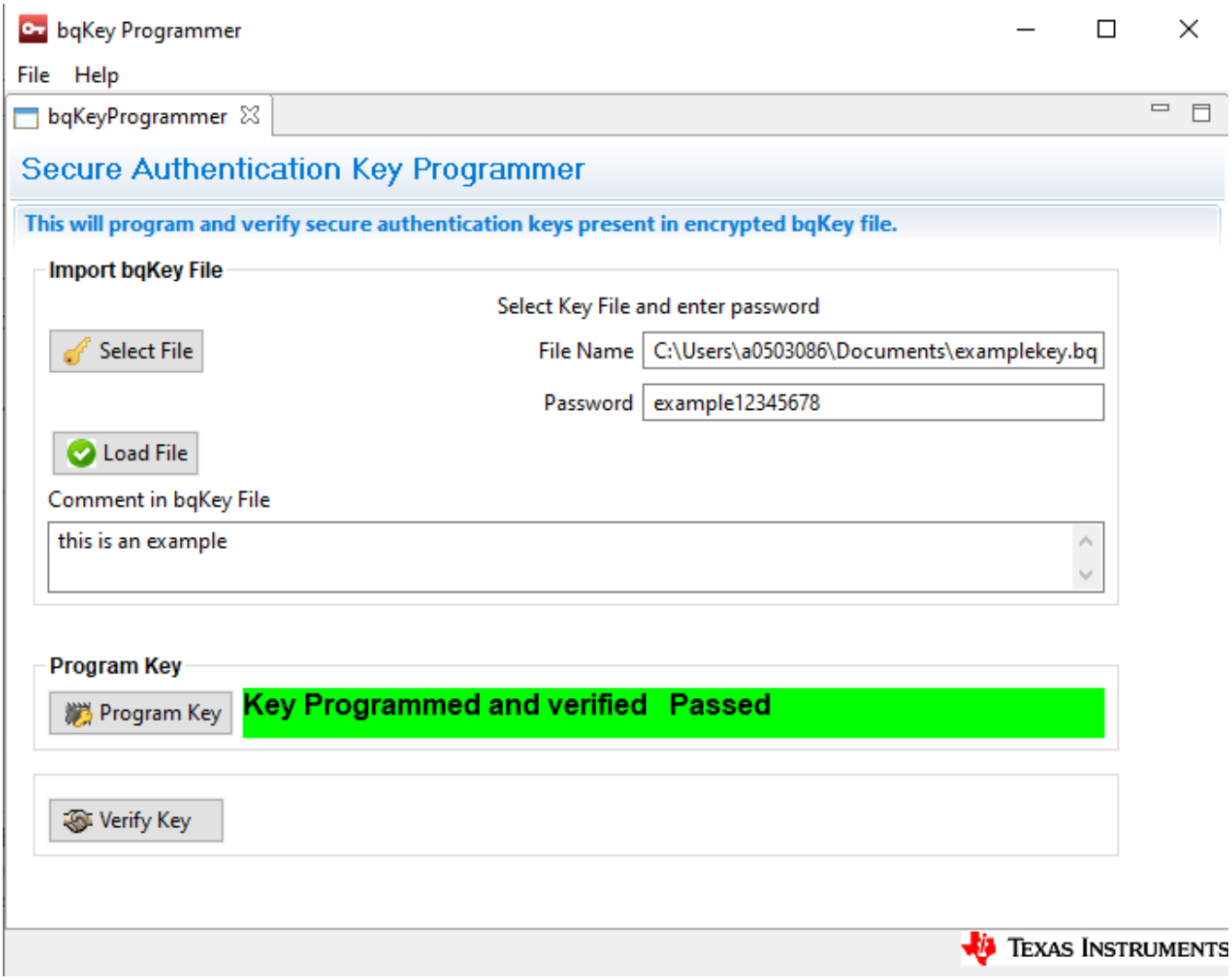

图 2-1. BQKEYPROGRAMMER 示例

备注

BQKEYPROGRAMMER 对一次性可编程存储器进行编程。如果通信中断或使用了不正确的 bqKey 文件，则该器件不可用于身份验证。请检查 bqKey 文件中的注释，以确保选择了正确的文件。在断开通信和电源之前，请确保编程器已完成操作。在通过编程操作锁定存储器之后，需要完整的上电复位。

测试身份验证是否成功的一种方法是使用 BQSTUDIO。

第 1 步：安装并打开 BQSTUDIO。

第 2 步：打开 Authentication 选项卡。

第 3 步：在 *Gauger Authentication By Host* 框中，输入密钥，然后点击 *Load Gauge Key*。

第 4 步：点击 *Generate Random Challenge*，然后选择 *Authenticate Gauge*。

如果出现绿色复选标记，则表示已成功验证电量监测计上的身份验证功能。

图 2-2. BQSTUDIO 密钥验证示例

3 在生产环境中对密钥进行编程

为了帮助在生产环境中进行身份验证编程，BQKEYPROGRAMMER 提供了 *“生成 FlashStream 文件”* 功能，可以导出一个包含 I2C 命令的 FlashStream 文件，以便将身份验证功能编程到电量监测计中。然后，可以将此 FlashStream 文件解析到生产环境中，以将该特定的身份验证密钥或密钥的一半编程到相应的电量监测计中。此 FlashStream 文件中包含了经过解密的原始身份验证密钥，因此并、不安全。

备注

BQKEYPACKAGER 和 BQKEYPROGRAMMER 并不是直接用于生产环境，因此也不受相应的支持。德州仪器 (TI) 对于分别使用 BQKEYPACKAGER 或 BQKEYPROGRAMMER 进行封装或编程的任何密钥的安全性概不负责。用户有责任确保密钥的安全，并对能够访问密钥任何部分的各方数量加以限制。

4 总结

总之，本应用手册介绍了以下几点：使用 BQKEYPACKAGER 创建 SHA 或 ECC 密钥的过程，使用 BQKEYPROGRAMMR 将选定的密钥编程到电量监测计中的过程，有关在生产环境中对密钥进行编程的指导。

5 参考资料

1. 德州仪器 (TI)，*[常见问题解答] 对 SHA-1 安全密钥进行编程的过程是什么？*
2. 德州仪器 (TI)，*TI 电量监测计认证密钥封装器和编程器工具*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、某特定用途方面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功能安全、信息安全、监管或其他要求。

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。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/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。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265