STM32MP1 系列密钥生成器软件说明

引言

STM32CubeProgrammer(STM32CubeProg)已经内置 STM32MP1 系列密钥生成器软件（本文档中称其为 STM32MP1-KeyGen)。

STM32MP1-KeyGen 可生成二进制映像签名所需的 ECC 密钥对。STM32 签名工具在签名时会使用已生成的密钥。

STM32MP1-KeyGen 可生成公钥文件、私钥文件和哈希公钥文件。

公钥文件包含已生成的 PEM 格式 ECC 公钥。

私钥文件包含 PEM 格式加密 ECC 私钥。加密操作可使用 aes 128 cbc 或 aes 256 cbc 密码算法。利用--prvkey-enc 选项可选择密码算法。

哈希公钥文件包含二进制格式公钥 SHA-256 哈希值。该 SHA-256 哈希值是基于公钥计算得出的、无任何编码格式的数值。公钥的第一个字节仅用于指示该公钥的格式是压缩格式还是非压缩格式。由于仅支持非压缩格式，因此可删除该字节。

1 安装 STM32MP1-KeyGen

此工具随 STM32CubeProgrammer 软件包（STM32CubeProg）一同安装。有关配置规程的详细信息，请参见用户手册 *STM32CubeProgrammer 软件说明* 中的第 1.2 章（UM2237）。

此软件适用于基于 Arm®的 STM32MP1 系列 MPU。

提示 *Arm 是 Arm Limited（或其子公司）在美国和/或其他地区的注册商标。*

2 STM32MP1-KeyGen 命令行接口

以下各节介绍如何由命令行来使用 STM32MP1-KeyGen。

2.1 指令

以下列出了可供使用的命令：

- --private-key (-prvk)
  - 说明：私钥文件路径（扩展名.pem）
  - 语法：-prvk <private_key_file_path>
  - 示例：-prvk ../privateKey.pem
- --public-key (-pubk)
  - 说明：公钥文件路径（扩展名.pem）
  - 语法：-pubk <public_key_file_path>
  - 示例：-pubk C:\publicKey.pem
- --public-key-hash (-hash)
  - 说明：哈希映像文件路径（扩展名.bin）
  - 语法：-hash <hash_file_path>
- --absolute-path (-abs)
  - 说明：输出文件的绝对路径
  - 语法：-abs <absolue_path_folder_path>
  - 示例：-abs C:\KeyFolder\
- --password (-pwd)
  - 说明：私钥密码（此密码必须至少包含四个字符）
  - 示例：-pwd azerty
- --prvkey-enc (-pe)
  - 说明：加密私钥算法（aes128/aes256）（aes256 算法为默认算法）
  - 语法：-pe aes128
- --ecc-algo (-ecc)
  - 说明：ECC 密钥生成算法（prime256v1/brainpoolP256t1）（prime256v1 为默认算法）
  - 语法：-ecc prime256v1
- --help (-h and -?)
  - 说明：显示帮助。
- --version (-v)
  - 说明：显示工具版本。

2.2 示例

以下示例展示了如何使用 STM32MP1-KeyGen：

- 示例 1

```
-abs /home/user/KeyFolder/ -pwd azerty
```

所有文件（publicKey.pem、privateKey.pem 和 publicKeyhash.bin）都创建在*/home/user/KeyFolder/* 文件夹中。私钥使用默认算法 aes256 加密。

- 示例 2

```
-abs /home/user/keyFolder/ -pwd azerty -pe aes128
```

所有文件（publicKey.pem、privateKey.pem 和 publicKeyhash.bin）都创建在*/home/user/KeyFolder/* 文件夹中。私钥使用 aes128 算法加密。

- 示例 3

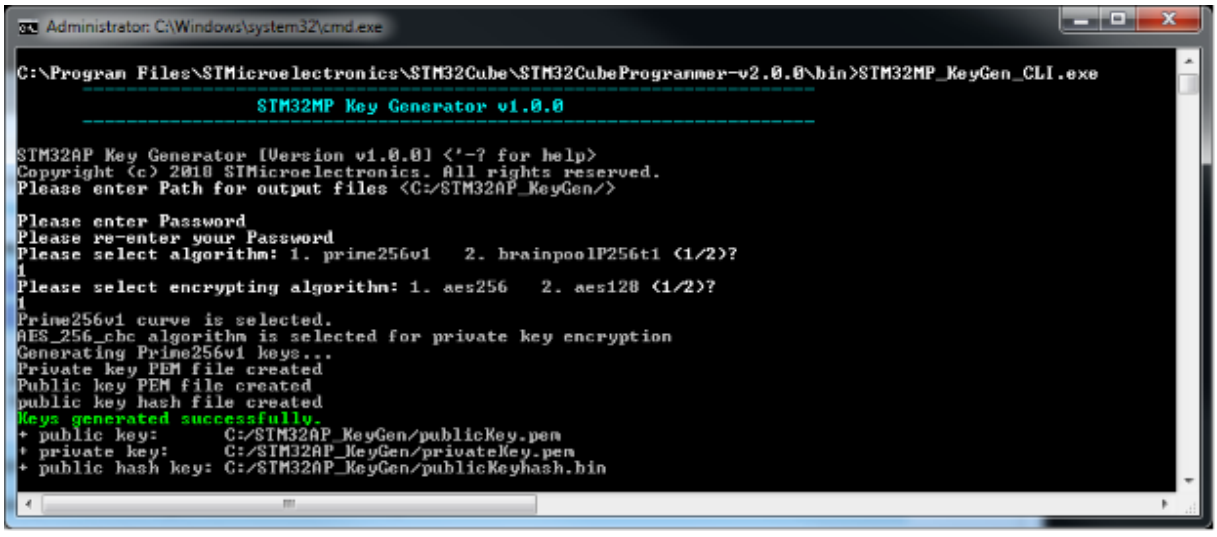
```
-pubk /home/user/public.pem -prvk /home/user/Folder1/Folder2/private.pem -hash /home/
user/pubKeyHash.bin -pwd azerty
```

文件夹 1 和文件夹 2 即使不存在也会被创建。

2.3 独立模式

在独立模式下运行 STM32MP1-KeyGen 时，需要按照以下图示提供绝对路径和密码。

图 1. 独立模式下的 STM32MP-KeyGen



当用户按下<Enter>时，*<C:\Users\User_Name\.STM32AP_KeyGen/>* 文件夹中将生成文件。

随后第二次输入密码，再从两个算法（prime256v1 或 brainpoolP256t1）中选择一个算法并按下对应按键（1 或 2）。

最后按下选择加密算法（aes256 或 aes128）对应的按键（1 或 2）。

版本历史

表 1. 文档版本历史

日期	版本	变更
2019 年 2 月 14 日	1	初始版本。

目录

重要通知 - 请仔细阅读

意法半导体公司及其子公司（“ST”）保留随时对 ST 产品和/或本文档进行变更、更正、增强、修改和改进的权利，恕不另行通知。买方在订货之前应获取关于 ST 产品的最新信息。ST 产品的销售依照订单确认时的相关 ST 销售条款。

买方自行负责对 ST 产品的选择和使用，ST 概不承担与应用协助或买方产品设计相关的任何责任。

ST 不对任何知识产权进行任何明示或默示的授权或许可。

转售的 ST 产品如有不同于此处提供的信息的规定，将导致 ST 针对该产品授予的任何保证失效。

ST 和 ST 徽标是 ST 的商标。所有其他产品或服务名称均为其各自所有者的财产。

本文档中的信息取代本文档所有早期版本中提供的信息。