STM32MP1 系列签名工具软件说明

引言

STM32CubeProgrammer(STM32CubeProg)已内置 STM32MP1 系列签名工具软件（本文档中称其为 STM32MP1-SignTool)。

STM32MP1-SignTool 是保证平台安全的重要工具，它能够确保在二进制文件签名时使用 STM32MP1-KeyGen 软件生成的 ECC 密钥对（参见用户手册 *STM32MP1 系列密钥生成软件说明*（UM2542）了解详细信息）。

当使用支持可信任启动链的 STM32MP1 系列 MPU 进行安全启动时，将使用已签名的二进制映像。此操作可确保已加载的映像通过认证和完整性检查。

STM32MP1-SignTool 可生成二进制映像文件、公钥文件和私钥文件。

二进制映像文件包含有用于设备编程的二进制数据。

公钥文件包含使用 STM32MP1-KeyGen 生成的 PEM 格式 ECC 公钥。

私钥文件包含使用 STM32MP1-KeyGen 生成的 PEM 格式加密 ECC 私钥。

另外，也可以在批处理文件模式下利用现有的已签名文件生成签名的二进制文件。在这种情况下，不需要提供映像入口点、映像加载地址和映像版本参数。

1 安装 STM32MP1-SignTool

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-SignTool 命令行接口

以下各节介绍如何由命令行来使用 STM32MP1-SignTool。

2.1 指令

以下列出了可供使用的命令：

- --binary-image (-bin)
  - 说明：二进制映像文件路径（扩展名.bin）
  - 语法：-bin /home/User/binaryFile.bin
- --image-version (-iv)
  - 说明：输入已签名映像文件的映像版本。
  - 语法：-iv <version_number>
- --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
- --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
- --load-address (-la)
  - 说明：映像加载地址
  - 示例：-la <load_address>
- --entry-point (-ep)
  - 说明：映像入口点
  - 示例：-ep <entry_point>
- --option-flags (-of)
  - 说明：映像选项标志（默认值 = 0）
  - 示例：-of <option_flags>
- --algorithm (-a)
  - 说明：指定 prime256v1（数值 1，默认值）或 brainpoolP256t1（数值 2）中的一个。
  - 示例：-a <2>
- --output (-o)
  - 说明：输出文件路径。此参数为可选参数。如果未明确指定路径，则会在相同的源文件路径下生成输出文件（例如，二进制文件为 *C:\BinaryFile.bin*）。已签名的二进制文件为 *C:\BinaryFile_Signed.bin*。
  - 语法：-o <Output_File_Path>
- --type (-t)
  - 说明：二进制类型。可能的数值为 ssbl、fsbl、teeh、teed、teex 和 copro。
  - 语法：-t <type>
- --silent (-s)
  - 说明：替换现有输出文件不会显示任何消息
- --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-SignTool：

- 示例 1

```
-bin /home/User/BinaryFile.bin -pubk /home/user/publicKey.pem -prvk /home/user/
privateKey.pem -iv 5 -pwd azerty -la 0x20000000 -ep 0x08000000
```

选择默认算法（prime256v1）并且选项标志数值为 0（默认值）。已签名的输出二进制文件创建在*/Home/user/* 文件夹中

- 示例 2

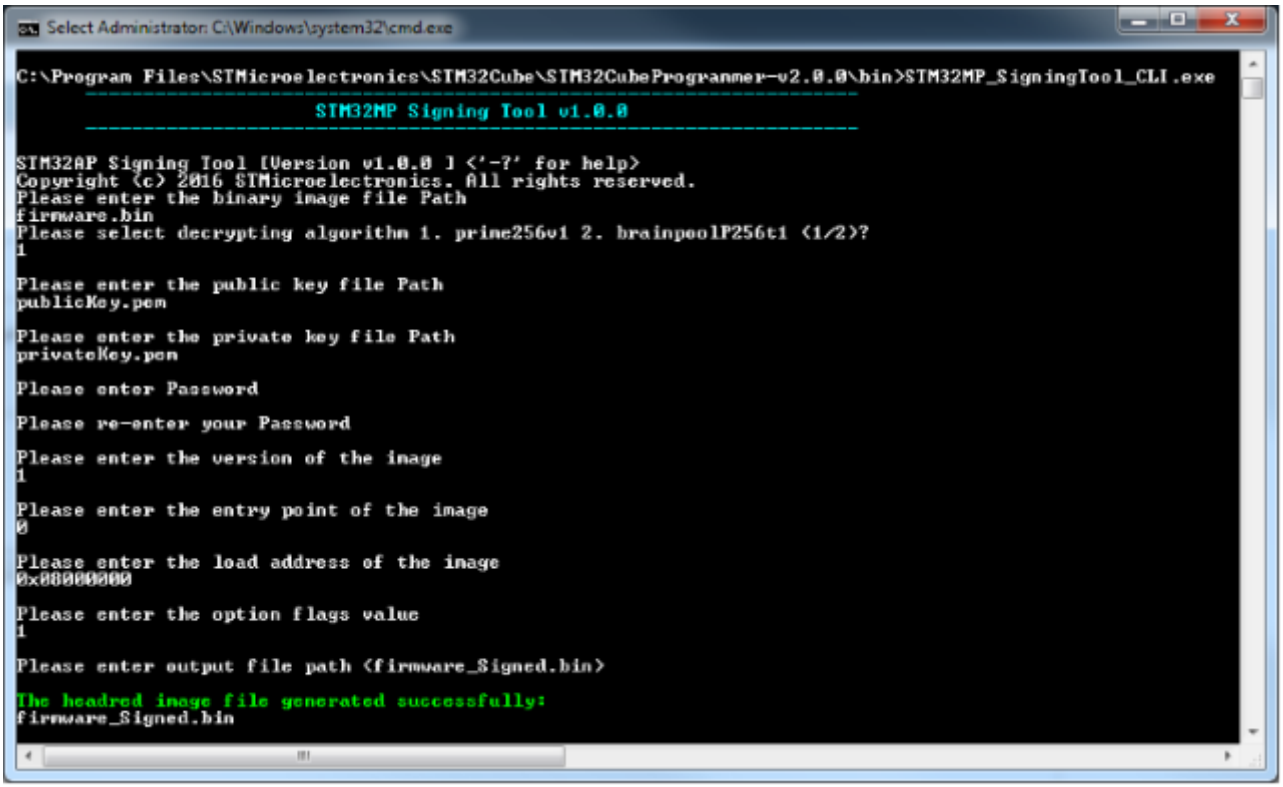
```
-bin /home/User/Folder1/BinaryFile.bin -pubk /home/user/publicKey.pem -prvk /home/user/
privateKey.pem -iv 5 -pwd azerty -s -la 0x20000000 -ep 0x08000000 -a 2 -o /home/user/
Folder2/Folder3/signedFile.bin
```

在这种情况下选择 BrainpoolP256t1 算法。文件夹 2 和文件夹 3 即使不存在也会被创建。使用`-s` 命令时，使用同一指定名称的文件将被自动替换并且不显示任何消息。

2.3 独立模式

在独立模式下运行 STM32MP1-SignTool 时，必须按照以下图示首先输入绝对路径，然后输入两次密码进行确认。

图 1. 独立模式下的 STM32MP1-SignTool



以下是后续操作步骤：

- 从两个算法中选择一个算法。
- 输入映像版本、映像入口点和映像加载地址。
- 输入选项标志数值。

如有需要，可指定其他输出文件路径或按下 enter 键继续使用现有输出文件路径。

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。