PHYTIUM 飞腾

腾锐 D2000 安全 CPU

固件打包工具说明

v1.0

飞腾信息技术有限公司

2021 年 6 月

更新记录

版本号	发布部门	作者	发布日期	备　注
1.0	飞腾通用软件部	粟梁虎	2021-06-10	初稿

目录

1 介绍

在 D2000 网安版调试使用中，经常需要对 bl32 和 bl33 镜像进行更换，以验证新镜像的功能和性能等。此外，网安版中每个镜像需要相应的签名才能正常使用，需要有相关工具能简单地完成相关工作。为此，飞腾提供了固件的打包工具，以方便进行 bl32 和 bl33 镜像的替换。本文档主要介绍如何替换 bl32 和 bl33 以及相关参数和 key 的要求。

2 环境要求

2.1 硬件要求

硬件要求如表 2.1 所示。

表 2.1 硬件要求

项目	说明
CPU	Armv8 系列
网络	无要求
存储	无要求
内存	无要求

2.2 操作系统要求

操作系统要求如表 2.2 所示。

表 2.2 操作系统要求

项目	说明
OS	Linux 系统

3 安装说明

3.1 软件获取

请联系飞腾信息技术有限公司获取工具软件包。

3.2 安装过程

执行如下命令，将工具包解压即可。

```
tar -xf image_fix_v0.2.tar
```

3.3 运行验证

解包没有报错即可。

4 使用说明

1) 进入工具包目录 image_fix_v0.2。

2) 如果需要更新飞腾 PBF 固件，拿到固件解压后内部的 xxx.bin 即为升级文件，执行如下指令将其更新为当前环境使用的 PBF 固件。

```
./my_scripts/pbf_update.sh      xxx.bin
```

3) 执行如下指令，生成 SM2 密钥。

```
gmssl genpkey -algorithm EC -pkeyopt ec_paramgen_curve:sm2p256v1 -out pri_key.pem
```

4) 执行如下指令，提取密钥中的公钥。

```
gmssl pkey -in pri_key.pem -pubout -text_pub > pub_key.txt
```

5) 将该公钥 pub_key.txt 提交给飞腾，由飞腾签名后返回对应厂商的签名文件 xxxxxx.bin。

6) 将签名文件存放到目录 key，同时，将之前生成的 SM2 密钥也存放到该目录。

7) 进入 key 目录，执行如下命令，将密钥和签名文件链接到工具使用的默认路径，具体文件名请替换为自己实际的文件名。其中 xxxxxx.bin 代表飞腾签名文件，pri_key.pem 代表对应该签名文件的 SM2 密钥，bl32 和 bl33 可以使用同一个密钥，也可以使用不同的密钥，在链接时一一对应好即可。

```
ln -sf xxxxxx.bin bl32_key.bin
ln -sf xxxxxx.bin bl33_key.bin
ln -sf pri_key.pem bl32_key.pem
ln -sf pri_key.pem bl33_key.pem
```

8) 返回工具包根目录，执行如下命令，将 bl32 和 bl33 文件链接到工具使用的默认路径。请将具体文

件名替换为自己实际使用的文件名，其中 tee.bin 代表 bl32 镜像文件名，uefi.bin 代表 bl33 镜像文件名。

```
ln -sf tee.bin bl32_new.bin
ln -sf uefi.bin bl33_new.bin
```

9) 工具运行需要 OpenSSL 库 libcrypto.so.1.0.0 和国密库 libcrypto.so.1.1，如果系统没有安装对应版本的库，工具包中包含了 ARM 环境的这两个库，可以执行如下指令使用。该配置修改了当前 SHELL 的库加载顺序，工具使用完后请退出该 SHELL 避免系统下某些命令使用不正常。

```
export LD_PRELOAD=$PWD/libcrypto.so.1.1:$PWD/libcrypto.so.1.0.0
```

10) 该版本固件默认配置的 bl33 的启动偏移地址为 0x300000，如需修改，请打开文件./my_scripts/image-fix.sh，修改文件开头的 bl33_base 参数即可，同时，修改了该参数后，bl33 镜像内部也需要将引导地址替换为该地址。

11) 如果不打算更新 bl33，可以从工具包当前固件中提取该固件的 bl33 镜像使用，执行如下命令可获取到当前固件的 bl33 镜像。

```
dd if=./build/PBF.bin of=./uefi.bin bs=1k skip=3072
```

12) 执行如下命令，重新打包固件，并将固件内 bl32 和 bl33 替换成 bl32_new.bin 和 bl33_new.bin，最终生成新的固件名为 fip-all.bin。

```
./my_scripts/image-fix.sh bl32 cot
```

5 使用举例

在 D2000 网安版设备上，安装了 CentOs-8.2 系统，按照使用说明逐步操作，使用了自己的 tee（bl32）镜像和固件原有的 uefi（bl33）镜像，生成了新的固件 fip-all.bin，并将其烧写到 Flash 上，该网安版设备能正常验签启动成功。