CV180X & CV181X 安全启动使用手册

Version: 0.4

Release date: 2023-02-06

©2022 北京晶视智能科技有限公司
本文件所含信息归北京晶视智能科技有限公司所有。
未经授权，严禁全部或部分复制或披露该等信息。

目录

1 声明 **2**

2 安全启动介绍 **3**
2.1 镜像结构 3
2.2 安全启动流程 4

3 安全镜像生成 **5**
3.1 秘钥列表 5
3.2 生成密钥 5
3.3 签署加密镜像 6
3.3.1 生成镜像 6
3.3.2 签署 FIP.bin 镜像 6
3.3.3 签署并加密 FIP.bin 镜像 6

4 eFuse 烧写 **8**

修订记录

Revision	Date	Description
0.1	2022-06-01	初稿
0.2	2022-09-28	更改 processor 名称
0.3	2023-02-01	更新安全启动使用流程
0.4	2023-02-06	CV181x/CV180x 文档融合

1 声明

法律声明

本数据手册包含北京晶视智能科技有限公司（下称“晶视智能”）的保密信息。未经授权，禁止使用或披露本数据手册中包含的信息。如您未经授权披露全部或部分保密信息，导致晶视智能遭受任何损失或损害，您应对因之产生的损失/损害承担责任。

本文件内信息如有更改，恕不另行通知。晶视智能不对使用或依赖本文件所含信息承担任何责任。

本数据手册和本文件所含的所有信息均按“原样”提供，无任何明示、暗示、法定或其他形式的保证。晶视智能特别声明未做任何适销性、非侵权性和特定用途适用性的默示保证，亦对本数据手册所使用、包含或提供的任何第三方的软件不提供任何保证；用户同意仅向该第三方寻求与此相关的任何保证索赔。此外，晶视智能亦不对任何其根据用户规格或符合特定标准或公开讨论而制作的可交付成果承担责任。

联系我们

地址 北京市海淀区丰豪东路 9 号院中关村集成电路设计园（ICPARK）1 号楼

深圳市宝安区福海街道展城社区会展湾云岸广场 T10 栋

电话 +86-10-57590723 +86-10-57590724

邮编 100094（北京）518100（深圳）

官方网站 https://www.sophgo.com/

技术论坛 https://developer.sophgo.com/forum/index.html

2 安全启动介绍

2.1 镜像结构

图 2.1 是 CV181x/CV180x 的镜像结构。使用安全启动时，FIP.bin 镜像被签名并加密（可选），开机时由处理器进行校验。

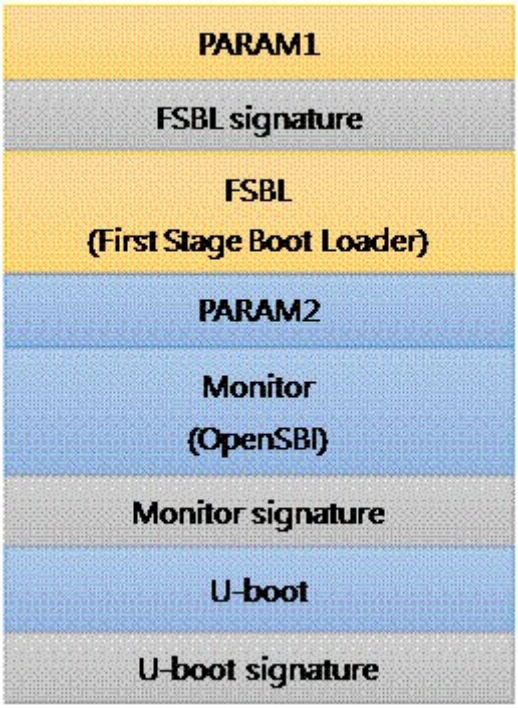
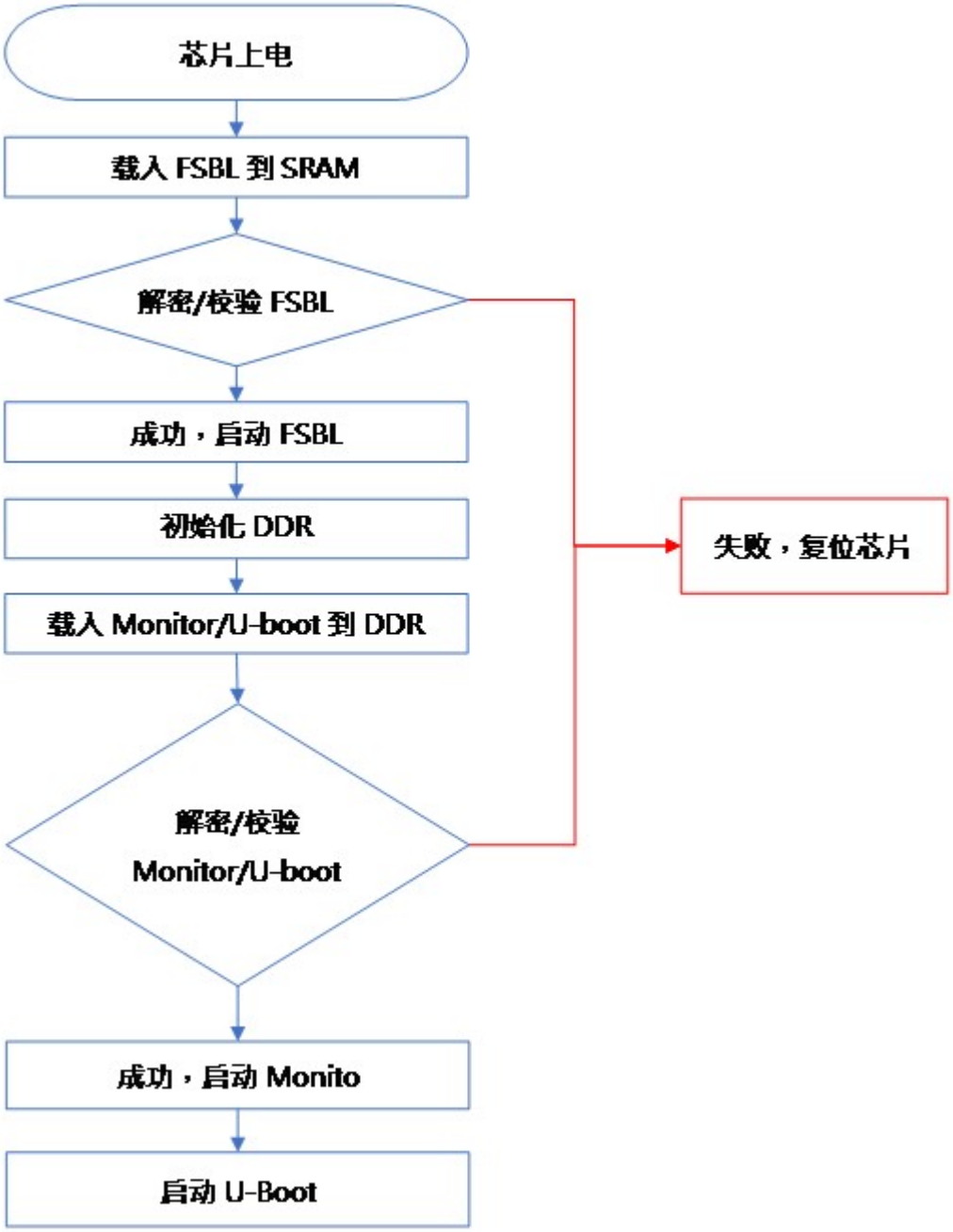


图 2.1: Layout of FIP.bin.

2.2 安全启动流程



注解: 注意：CV180x 只支持签名/验签功能，请勿使用加密/解密功能，会导致 IC 启动不了。

3 安全镜像生成

3.1 秘钥列表

1.	rsa_hash0.pem	用于签署 FSBL 的 RSA 私钥
2.	loader_ek.key	用于加密 FSBL 的 AES 秘钥
3.	bl_priv.pem	用于签署 Monitor/u-boot 的 RSA 私钥
4.	bl_ek.key	用于加密 Monitor/u-boot 的 AES 秘钥

3.2 生成密钥

1. 生成签名私钥 rsa_hash0.pem 和 bl_priv.pem.

   * RSA 密钥使用 2048 bits 和第 4 费马数.

```
host$ openssl genrsa -out rsa_hash0.pem -F4 2048
host$ openssl genrsa -out bl_priv.pem -F4 2048
```

2. 生成加/解密秘钥 loader_ek.key 和 bl_ek.key.

   * 如果只签署不加密可以不用生成该秘钥

   * 以下使用随机数生成秘钥

```
host$ head -c 16 /dev/random > loader_ek.key
host$ head -c 16 /dev/random > bl_ek.key
```

3.3 签署加密镜像

3.3.1 生成镜像

参考 <U-boot 移植应用开发指南 > 产生 FIP.bin 镜像

3.3.2 签署 FIP.bin 镜像

注解: 注意事项

为避免量产秘钥被窃，建议量产密钥应单独保管，并使用签名工具单独于安全的环境下进行签名和加密

执行下列命令签名 FIP 镜像，fip.bin 为原始镜像，fip_sign.bin 为签名后镜像.

```
cv_crypt$ ./fipsign.py sign \
        --root-priv= rsa_hash0.pem \
        --bl-priv=bl_priv.pem \
        fip.bin fip_sign.bin
```

工具参数:

```
cv_crypt$ ./fipsign.py sign
usage:  fipsign.py sign [-h] [--root-priv ROOT_PRIV] [--bl-priv BL_PRIV] SRC_FIP DEST_FIP
```

3.3.3 签署并加密 FIP.bin 镜像

执行下列命令签名并加密 FIP 镜像，fip.bin 为原始镜像，fip_enc.bin 为签名并加密后镜像.

```
cv_crypt$ ./fipsign.py sign-enc \
        --root-priv= rsa_hash0.pem \
        --bl-priv=bl_priv.pem \
        --ldr-ek=loader_ek.key \
        --bl-ek=bl_ek.key \
        fip.bin fip_enc.bin
```

工具参数:

```
cv_crypt$ ./fipsign.py sign-enc
usage: fipsign.py sign-enc [-h] [--ldr-ek LDR_EK] [--bl-ek BL_EK] [--root-priv ROOT_PRIV] [--bl-priv␣
↪BL_PRIV] SRC_FIP DEST_FIP
```

* 注意: 加密是可选的，如果需要加密，编译 FIP.bin 时需要配置 CONFIG_FSBL_SECURE_BOOT_SUPPORT = y, 配置方法:

```
host$ source build/envsetup_soc.sh
```

```
host$ defconfig xxxxxx
```

```
host$ menuconfig --> FIP setting --> 选择 [ ] Add secure boot support to FSBL
```

4 eFuse 烧写

参考 <eFuse 使用指南 > 烧写 eFuse

注解: 注意事项

eFuse 烧写为不可逆行为，执行前请确认镜像已签署