Hi3559A/C V100 安全启动使用指南

文档版本　　00B02

发布日期　　2018-07-06

商标声明

 、HISILICON、海思和其他海思商标均为深圳市海思半导体有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受海思公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，海思公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

深圳市海思半导体有限公司

地址：深圳市龙岗区坂田华为基地华为电气生产中心　　邮编：518129

网址：http://www.hisilicon.com

客户服务电话：+86-755-28788858

客户服务传真：+86-755-28357515

客户服务邮箱：support@hisilicon.com

前 言

概述

本文档主要介绍 Hi3559A/C V100 安全启动的使用方法，主要内容包括：安全启动介绍、安全镜像生成步骤及 OTP 烧写说明。

支持如下启动介质：SPI NOR FLASH、并口 NAND FLASH、eMMC。

说明

未有特殊说明，Hi3559CV100 与 Hi3559AV100 内容一致。

产品版本

与本文档相对应的产品版本如下。

产品名称	产品版本
Hi3559A	V100
Hi3559C	V100

读者对象

本文档（本指南）主要适用于以下工程师：

- 技术支持工程师
- 软件开发工程师

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

修订日期	版本	修订说明
2018-07-06	00B02	1.2 小节，更新图 1-2 并添加注意
2018-02-12	00B01	第 1 次临时版本发布。

目 录

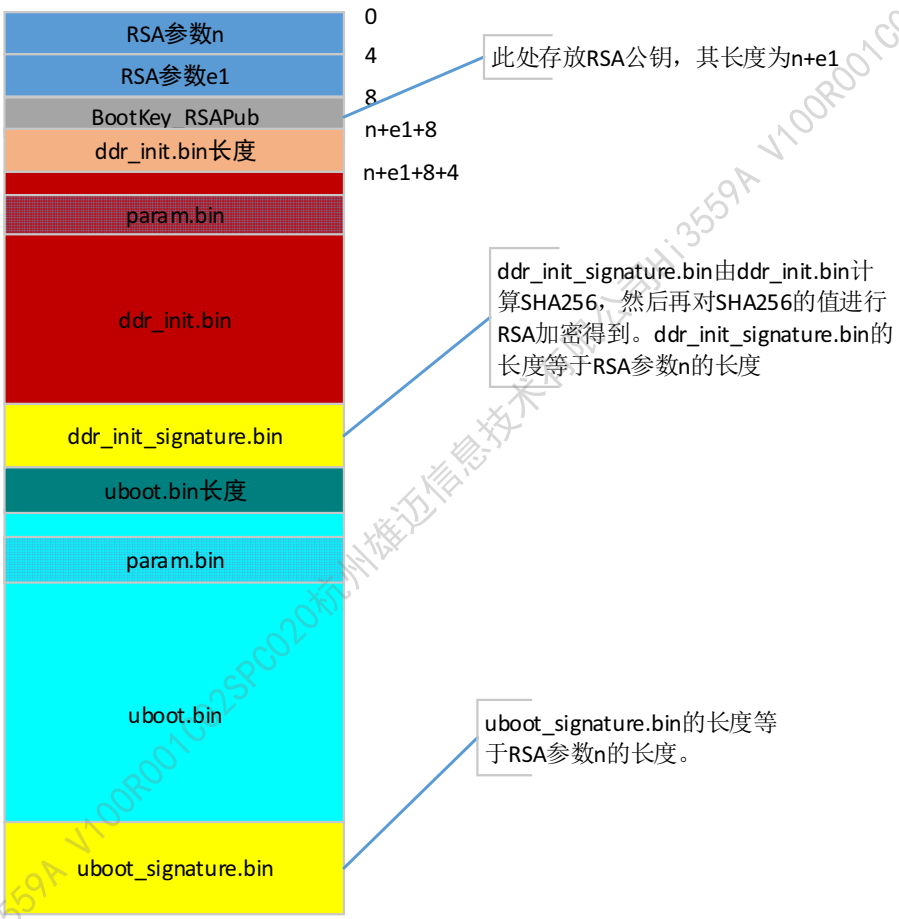
插图目录

1 安全启动介绍

1.1 镜像结构

Hi3559AV100 支持安全 U-boot 启动，安全 U-boot 镜像结构如图 1-1 所示。

图1-1 安全 boot 镜像结构图

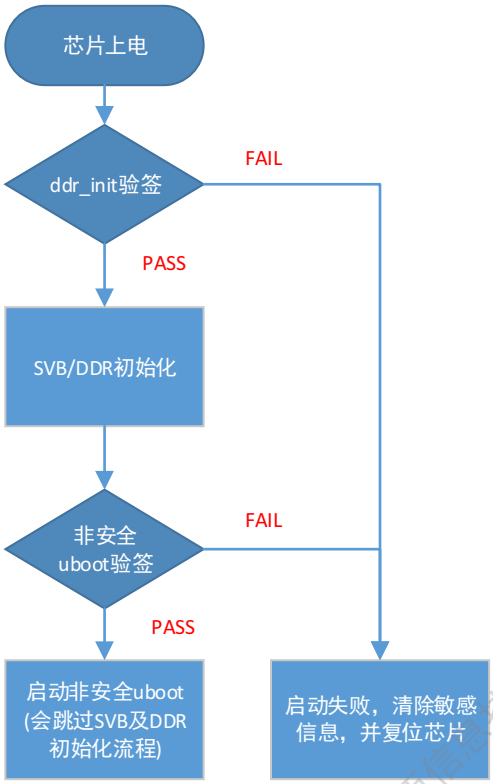


安全启动使用的 uboot 文件由公钥镜像、ddr_init.bin 镜像（包括 param.bin 和 ddr_init.bin）、非安全 uboot.bin 镜像和 ddr_init.bin 的数字签名（ddr_init_signature.bin）、非安全 uboot.bin 的数字签名（uboot_signature.bin）及它们各自的长度信息组成。

其中：RSA 支持 2048 和 4096 两种格式。

1.2 安全启动流程

图1-2 安全启动流程



注意

安全启动流程中，执行的是 hi3559av100_secureboot.tgz 下的 SVB 及 DDR 初始化代码，UBOOT 中的 SVB 及 DDR 初始化流程不会被执行！

因此在安全启动场景下，如果需要更新 SVB 或 DDR 初始化流程，须修改如下目录文件：

osdrv/opensoruce/uboot/hi3559av100_secureboot/drv/

```
├── ddr_ddrc_v500.h
├── ddr_ddrc_v510.h
├── ddr_ddrc_v520.h
├── ddr_ddrt_s40.h
├── ddr_ddrt_t12_v100.h
├── ddr_ddrt_t16.h
├── ddr_ddrt_t28.h
├── ddr_interface.h
├── ddr_phy_s40.h
├── ddr_phy_t12_v100.h
├── ddr_phy_t16.h
├── ddr_phy_t28.h
├── ddr_training_boot.c
├── ddr_training_console.c
├── ddr_training_ctl.c
├── ddr_training_custom.c
├── ddr_training_custom.h
├── ddr_training_impl.c
├── ddr_training_impl.h
├── ddr_training_internal_config.h
├── lowlevel_init_v300.c
```

发布包下，安全 BOOT 中 SVB、DDR 初始化流程同 UBOOT 中 SVB、DDR 初始化流程保持一致。

2 安全镜像生成

2.1 安全 U-boot 生成步骤

步骤 1. 生成非安全 U-boot 镜像：

参考《Hi3559A/C V100 U-boot 移植应用开发指南》中“移植 U-boot 章节”。

步骤 2. 解压安全 U-boot 发布包：

tar xvf hi3559av100_secureboot.tgz

将步骤 1 生成的非安全 U-boot 镜像 u-boot-hi3559av100.bin 拷贝至 hi3559av100_secureboot/secbin 目录

步骤 3. cd hi3559av100_secureboot

执行 make rsa2048 或 make rsa4096

最终在 hi3559av100_secureboot/secbin/目录下生成对应的安全镜像

----结束

注意

发布包脚本会在第一次编译时产生公钥和私钥文件，后续编译的安全镜像均采用第一次生成的公钥和私钥，如果要更新公钥和私钥，需手动删除 secbin/rsa2048pem 或 secbin/rsa4096pem 目录下的文件。

2.2 密钥文件介绍

```
├── rsa2048pem
│   ├── rsa2048_pem_key.txt        //文本格式的公钥 HASH 和寄存器配置命令
│   ├── rsa_priv_2048_base64.bin   //二进制格式私钥
```

```
|   ├── rsa_priv_2048_base64.pem   //PEM 格式私钥
|   ├── rsa_pub_2048_base64.bin    //二进制格式公钥
|   ├── rsa_pub_2048_base64.pem    //PEM 格式公钥
|   ├── rsa_pub_2048.bin           //二进制格式公钥 HASH
|   └── rsa_pub_2048_SHA256.txt    //文本格式公钥 HASH
├── rsa4096pem
|   ├── rsa4096_pem_key.txt        //文本格式的公钥 HASH 和寄存器配置命令
|   ├── rsa_priv_4096_base64.bin   //二进制格式私钥
|   ├── rsa_priv_4096_base64.pem   //PEM 格式私钥
|   ├── rsa_pub_4096_base64.bin    //二进制格式公钥
|   ├── rsa_pub_4096_base64.pem    //PEM 格式公钥
|   ├── rsa_pub_4096.bin           //二进制格式公钥 HASH
|   └── rsa_pub_4096_SHA256.txt    //文本格式公钥 HASH
```

3 OTP 烧写步骤

步骤 1. 烧写非安全 U-boot，并启动 U-boot 至命令行；

步骤 2. 公钥 HASH 烧写（必选）：

mw 0x10240008 0x6

mw 0x1024000c 0xxxxxxxxx

mw 0x10240010 0xxxxxxxxx

mw 0x10240014 0xxxxxxxxx

mw 0x10240018 0xxxxxxxxx

mw 0x1024001c 0xxxxxxxxx

mw 0x10240020 0xxxxxxxxx

mw 0x10240024 0xxxxxxxxx

mw 0x10240028 0xxxxxxxxx

说明

以上公钥 HASH 配置命令，可从 rsa2048_pem_key.txt 或 rsa4096_pem_key.txt 中直接 copy。

mw 0x10240000 0x2

mw 0x10240004 0x1acce551

步骤 3. DDR 加扰 BIT 烧写（可选）：

mw 0x10240034 0x1

mw 0x10240030 0x2

mw 0x10240000 0x4

mw 0x10240004 0x1acce551

步骤 4. 安全启动 BIT 烧写（必选）：

mw 0x10240034 0x0

mw 0x10240030 0x1

mw 0x10240000 0x4

mw 0x10240004 0x1acce551

步骤 5. 通过 U-boot 命令烧写安全镜像至启动介质，或通过 hitool 工具烧写安全镜像至启动介质

----结束

注意

以上每个烧写步骤都必须谨慎小心，以免烧写错误导致芯片不可用。