Hi3516EV200/Hi3516EV300/Hi3518EV300 安全启动使用指南

文档版本　00B04

发布日期　2019-01-30

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 Hi3516EV200/Hi3516EV300/Hi3518EV300 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、SPI NAND FLASH 和 eMMC。

说明

- 未有特殊说明，Hi3516EV200/Hi3518EV300 与 Hi3516EV300 内容一致。
- arm- himix200-linux-工具链暂不支持。

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
Hi3516E	V200
Hi3516E	V300
Hi3518E	V300

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
2019-01-30	00B04	第 4 次临时版本发布。 1.4 小节，涉及更新。 2.1 小节，步骤 4 涉及更新。
2019-01-14	00B03	第 3 次临时版本发布。 第 3 章涉及更新。
2018-12-26	00B02	第 2 次临时版本发布。 1.4 小节和 2.1 小节，涉及更新。 新增 2.3 小节。 第 3 章节，涉及更新。
2018-11-30	00B01	第 1 次临时版本发布。

目 录

插图目录

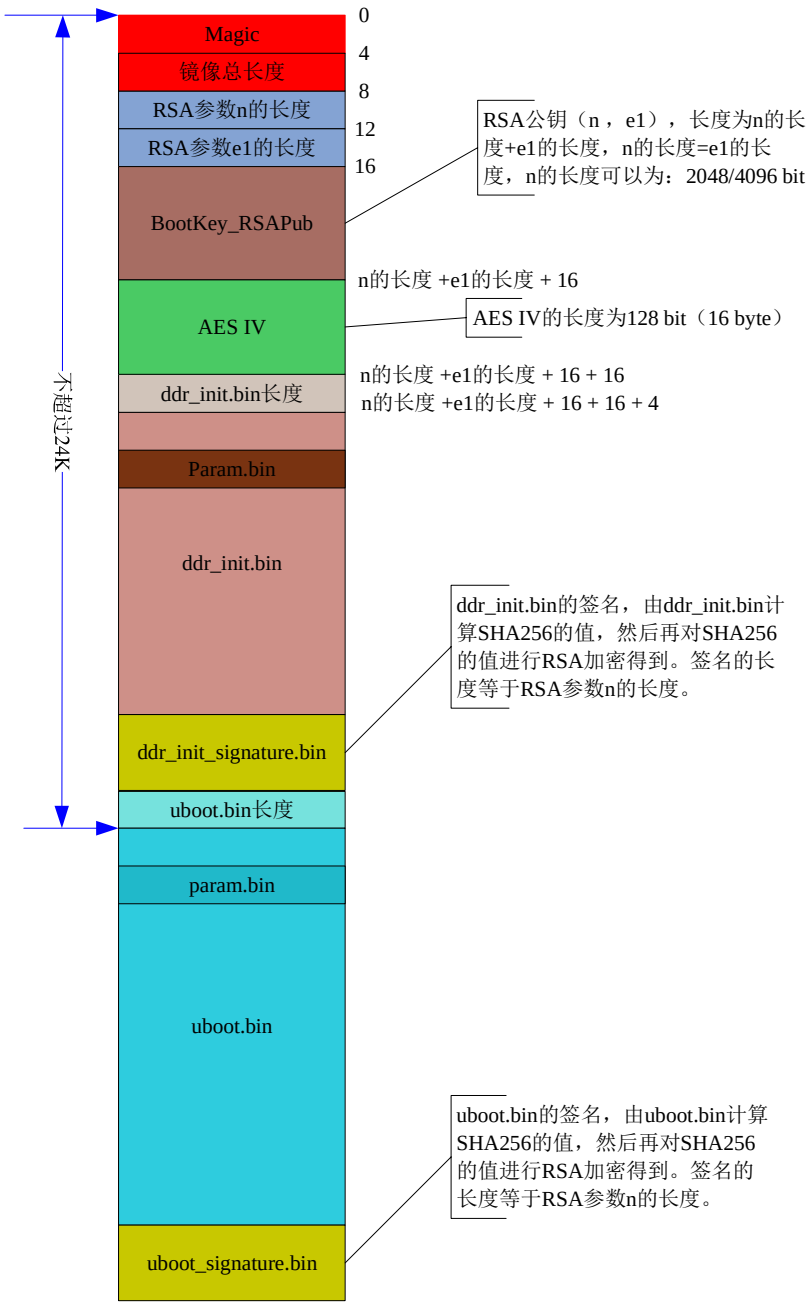
1 安全启动介绍

Hi3516EV200 支持普通安全 boot 启动和加密安全 boot 启动，其差异在于普通安全 boot 镜像中，ddr_init.bin 和 u-boot.bin 是明文；加密的安全 boot 镜像中，ddr_init.bin 和 u-boot.bin 是密文。

1.1 普通安全 boot 镜像结构

Hi3516EV200 普通安全 U-boot 镜像结构如图 1-1 所示。

图1-1 普通安全 boot 镜像结构图

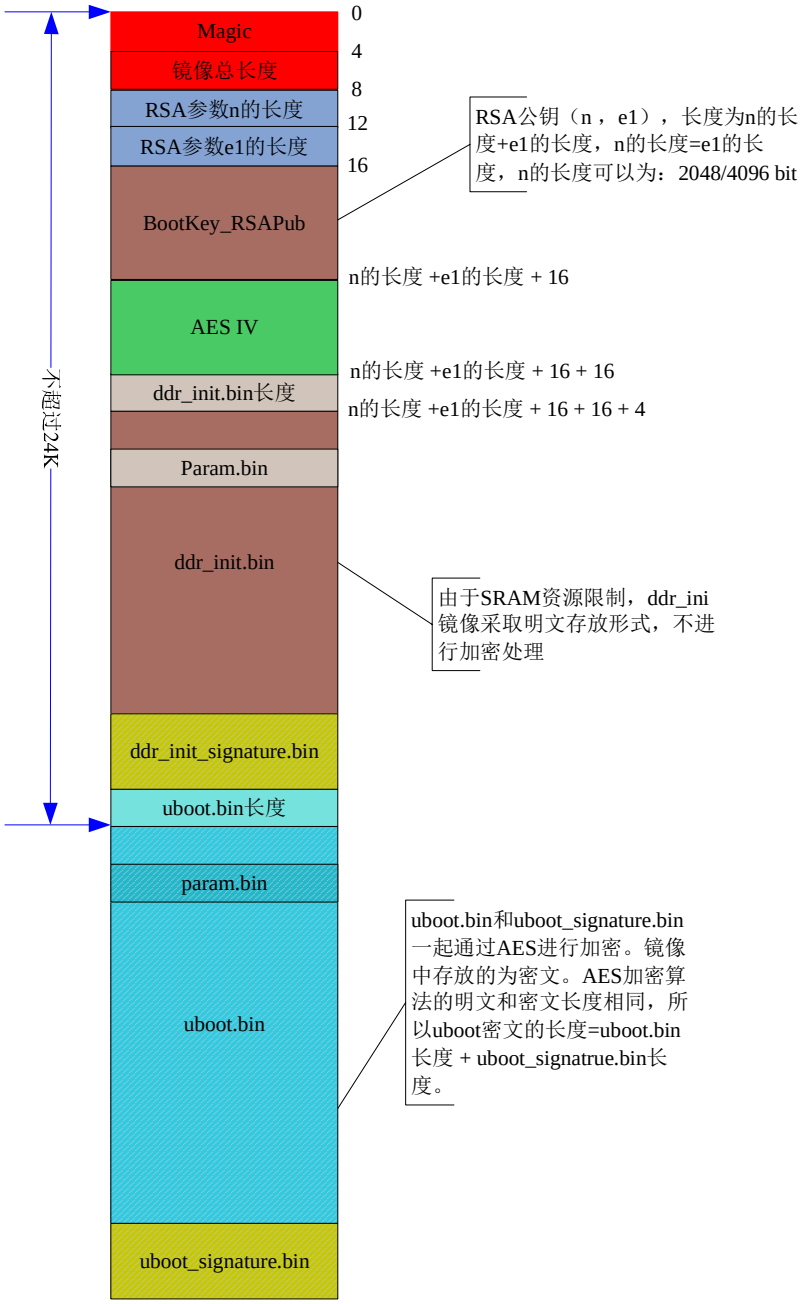


普通安全启动 uboot 镜像由公钥镜像、ddr_init.bin 镜像（包括 param.bin 和 ddr_init.bin）、非安全 uboot.bin 镜像和 ddr_init.bin 的数字签名（ddr_init_signature.bin）、非安全 uboot.bin 的数字签名（uboot_signature.bin）及它们各自的长度信息组成。

其中：RSA 支持 2048 和 4096 两种格式。AES IV 的值为 0。

1.2 加密安全 boot 镜像结构

图1-2 加密安全 boot 镜像结构图

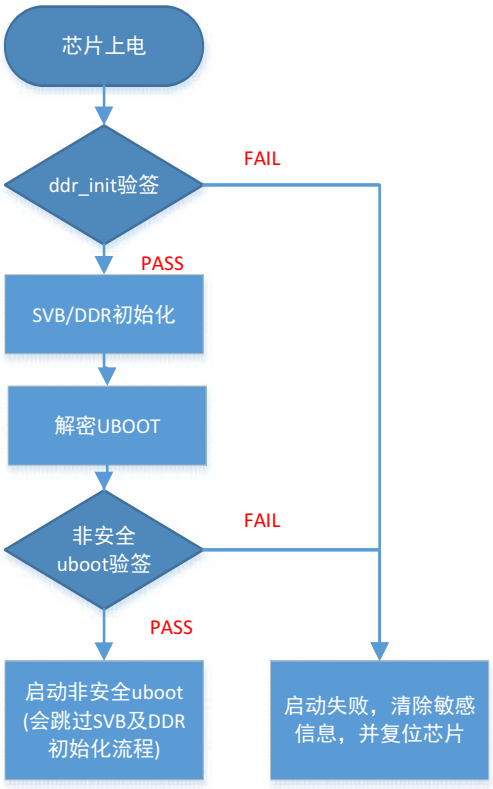


加密安全启动 uboot 镜像由公钥镜像、ddr_init.bin 镜像（包括 param.bin 和 ddr_init.bin）及其数字签名通过 AES 加密后的密文、非安全 uboot.bin 镜像及其数字签名通过 AES 加密后的密文和它们各自的长度信息组成。

其中：RSA 支持 2048 和 4096 两种格式。AES IV 的值为非 0 值。

1.3 安全启动流程

图1-3 安全启动流程



1.4 安全启动源代码目录说明

安全启动源代码目录为 secureboot_release，其详细目录结构如下：

```
├──── create_secure_boot.sh ----------------------------生成安全镜像脚本
├──── ddr_init ------------------------------------------- DDR 初始化源代码目录
|     ├──── boot
|     ├──── cfg.mk
|     ├──── ddr_init_ reg_info.bin
|     ├──── drv
|     ├──── include
|     ├──── linker.lds
|     ├──── linker.lds.mk
```

```
│   ├──── Makefile
│   ├──── mkddrinit.sh
├──── ddr_init_reg_info.bin ---------- 生成的 DDR 初始化镜像。
├──── HASH ---------- 由 hash_modify.c 文件生成的 RSA Pub Key hash 值解析工具。
├──── hash_modify.c
├──── AES ---------- 由 aeskey2reg.c 文件生成的 AES KEY 值解析工具。
├──── aeskey2reg.c
├──── Makefile ---------- 安全启动发布包总 Makefile。
├──── rsa2048pem ---------- 长度为 2048 Bit 的密钥文件存放目录。
├──── rsa2048pem.sh ---------- 生成长度为 2048 Bit 密钥的脚本。
├──── rsa4096pem ---------- 长度为 4096 Bit 的密钥文件存放目录。
├──── rsa4096pem.sh ---------- 生成长度为 4096 Bit 密钥的脚本。
├──── sha256.cfg ---------- 该文件设置执行的算法，已设置为 SHA256，不需要修改。
└──── u-boot- original.bin ---------- 非安全 uboot 镜像。
```

注意

安全启动流程中，执行的是 secureboot_release 目录下的 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/secureboot_release/ddr_init/drv/

```
├──── cmd_bin
├──── cmd_ddr_training_v2.c
├──── ddr_cmd_ctl.c
├──── ddr_cmd_loc.S
├──── 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_t12_v101.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
└─── Makefile
```

osdrv/opensoruce/uboot/secureboot_release/ddr_init/boot/hi35xx/lowlevel_init_v300.c

hi35xx 代指 hi3516ev200，hi3516ev300，hi3518ev300 等。

发布包下，安全 BOOT 中 SVB、DDR 初始化流程同非安全 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《Hi3516EV200/Hi3516EV300/Hi3518EV300 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 secureboot_release.tgz

将步骤 1 生成的非安全 U-boot 镜像改名为 u-boot-original.bin，并拷贝至 secureboot_release 目录。

步骤 3. 配置 create_secure_boot.sh 文件中的 KEY 和 IV：

如果要生成普通安全启动 uboot 镜像，create_secure_boot.sh 文件中的 KEY 和 IV 的值都设置为空；如果要生成加密安全启动 uboot 镜像，create_secure_boot.sh 文件中的 KEY 和 IV 的值需要设置。如：KEY= 67452301efcdab8998badcfe10325476332211007766554 4bbaa9988ffeeddcc IV= 00112233445566778899aabbccddeeff

步骤 4. 编译安全启动 uboot 镜像：

cd secureboot_release

执行 make CHIP=hi35xx all

最终在 secureboot_release 目录下生成对应的安全镜像。

说明

编译时必须指定芯片，hi35xx 代指 hi3516ev200，hi3516ev300，hi3518ev300。

举例：如编译 Hi3516EV200 的安全镜像时。

- 执行 make CHIP=hi3516ev200 all
- 清除编译文件时执行 make CHIP=hi3516ev200 clean

----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 rsa2048pem 或 rsa4096pem 目录下的文件。

2.2 密钥文件介绍

```
├──── rsa2048pem
|    ├──── rsa2048_pem_hash_val.txt   //文本格式的公钥 HASH 和寄存器配置命令
|    ├──── rsa_priv_2048.pem          //PEM 格式私钥
|    ├──── rsa_pub_2048.bin           //二进制格式公钥
|    ├──── rsa_pub_2048.pem           //PEM 格式公钥
|    └──── rsa_pub_2048_sha256.txt    //文本格式的公钥的 HASH 值
├──── rsa4096pem
|    ├──── rsa4096_pem_hash_val.txt   //文本格式的公钥 HASH 和寄存器配置命令
|    ├──── rsa_priv_4096.pem          //PEM 格式私钥
|    ├──── rsa_pub_4096.bin           //二进制格式公钥
|    ├──── rsa_pub_4096.pem           //PEM 格式公钥
|    └──── rsa_pub_4096_sha256.txt    //文本格式的公钥的 HASH 值
├────aes_otp_cfg.txt                  // AES KEY 寄存器配置命令
```

2.3 错误码介绍

- E0Dx：RSA 参数长度错误，或 uboot 格式错误。
- E1Dx：申请空间失败
- E2Dx：公钥验证失败
- E3Dx：ddr_init.bin 签名验证失败
- E4Dx：uboot.bin 签名验证失败
- E5Dx：计算 Hash 值失败
- E6Dx：RSA 解密失败
- E7Dx：清除 RSA RAM 失败
- E8Dx：计算出的 Hash 值与签名解密后得到的 Hash 值不相等

注意

字母“E”后面的数字表示错误类型，字母“D”后面的数字表示错误序号。

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 0x10090008 0x6

mw 0x1009000c 0xXXXXXXXX

mw 0x10090010 0xXXXXXXXX

mw 0x10090014 0xXXXXXXXX

mw 0x10090018 0xXXXXXXXX

mw 0x1009001c 0xXXXXXXXX

mw 0x10090020 0xXXXXXXXX

mw 0x10090024 0xXXXXXXXX

mw 0x10090028 0xXXXXXXXX

说明

以上公钥 HASH 配置命令，可从 rsa2048_pem_hash_val.txt 或 rsa4096_pem_hash_val.txt 中直接 copy。

mw 0x10090000 0x2

mw 0x10090004 0x1acce551

步骤 3. 安全启动 BIT 烧写（必选）：

mw 0x10090034 0x0

mw 0x10090030 0x1

mw 0x10090000 0x4

mw 0x10090004 0x1acce551

步骤 4. AES KEY 烧写（可选）：

mw 0x10090008 0x0

mw 0x1009000c 0xXXXXXXXX

mw 0x10090010 0xXXXXXXXX

mw 0x10090014 0xXXXXXXXX

mw 0x10090018 0xXXXXXXXX

mw 0x1009001c 0xXXXXXXXX

mw 0x10090020 0xXXXXXXXX

mw 0x10090024 0xXXXXXXXX

mw 0x10090028 0xXXXXXXXX

说明

以上 AES KEY 配置命令，可从"aes_otp_cfg.txt" 中直接 copy。

mw 0x10090000 0x2

mw 0x10090004 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。
- 十六进制的地址“0xXXXXXXXX”中，前缀 0x 中的 x 必需是小写字母。
- 如果要生成普通安全 uboot 镜像，secure_boot.cfg 文件中的 KEY 和 IV 都要设置为空。