



**Hi3861V100 / Hi3861LV100 二次开发网络安全**

## **注意事项**

文档版本 05

发布日期 2020-08-10

版权所有 © 上海海思技术有限公司2020。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



**HISILICON**、海思和其他海思商标均为海思技术有限公司的商标。

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。

# 上海海思技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <https://www.hisilicon.com/cn/>

客户服务邮箱： [support@hisilicon.com](mailto:support@hisilicon.com)



## 前言

### 概述

Hi3861V100、Hi3861LV100交付包为芯片解决方案交付包，主要包括芯片资料、硬件资料、SDK软件包、软件参考设计以及软件资料等。用户可基于此芯片解决方案交付包，开发各种自定义的产品。

本文档从网络安全的角度，重点分析基于本交付包开发的产品在使用过程中，可能面临的与本交付包中SDK软件包相关的网络安全的威胁，同时，针对性地给出相应的解决方案。

### 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
Hi3861	V100
Hi3861L	V100


### 读者对象

本文档主要适用于以下工程师：




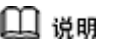
- 技术支持工程师
- 软件开发工程师

### 符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 危险	表示如不可避免则将会导致死亡或严重伤害的具有高等级风险的危害。



符号	说明
 <b>警告</b>	表示如不可避免则可能导致死亡或严重伤害的具有中等级风险的危害。
 <b>注意</b>	表示如不可避免则可能导致轻微或中度伤害的具有低等级风险的危害。
 <b>须知</b>	用于传递设备或环境安全警示信息。如不可避免则可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “须知”不涉及人身伤害。
 <b>说明</b>	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

## 修改记录

文档版本	发布日期	修改说明
05	2020-08-10	在“ <b>1.3.1 启动方法</b> ”中更新关于安全启动特性对客户建议的内容。
04	2020-08-04	在“ <b>1.4 Flash加密</b> ”中更新Flash加密工作原理；新增说明内容；删除须知内容。
03	2020-06-28	更新“ <b>1.5 Flash加扰</b> ”小节的全部内容。
02	2020-06-05	<ul style="list-style-type: none"> <li>更新“<b>1.3.2 方案说明</b>”小节。</li> <li>新增“<b>1.3.2.3 安全启动开启流程</b>”小节。</li> </ul>
01	2020-04-30	第一次正式版本发布。 <ul style="list-style-type: none"> <li>新增“<b>1.6 关键数据安全存储</b>”小节。</li> <li>在“<b>1.7.1 Cipher驱动</b>”中新增关于密钥派生算法KDF迭代次数的注意说明。</li> </ul>
00B02	2020-04-09	<ul style="list-style-type: none"> <li>在“<b>1.1 安全架构</b>”中新增关于固件代码安全的说明。</li> <li>在“<b>1.3.1 启动方法</b>”中补充关于写EFUSE相关步骤的操作目的说明，新增关于EFUSE各项说明及锁定位说明、产线烧写EFUSE方法需要参见手册的说明。</li> <li>新增“<b>1.4 Flash加密</b>”小节。</li> <li>在“<b>1.7.1 Cipher驱动</b>”中新增参见《Hi3861V100 / Hi3861LV100 API 开发参考》的说明。</li> <li>新增“<b>1.8.3 可维可测注意事项</b>”小节。</li> </ul>
00B01	2020-01-15	第一次临时版本发布。



# 目录

前言.....	i
1 产品安全解决方案.....	1
1.1 安全架构.....	1
1.2 设备安全.....	2
1.3 安全启动.....	2
1.3.1 启动方法.....	2
1.3.2 方案说明.....	3
1.3.2.1 启动流程.....	3
1.3.2.2 二级密钥 ID.....	4
1.3.2.3 安全启动开启流程.....	4
1.4 Flash 加密.....	5
1.5 Flash 加扰.....	5
1.6 关键数据安全存储.....	6
1.7 驱动安全注意事项.....	6
1.7.1 Cipher 驱动.....	6
1.7.2 串口.....	6
1.8 其他使用安全注意事项.....	6
1.8.1 JTAG 接口.....	6
1.8.2 代码安全注意事项.....	7
1.8.3 可维可测注意事项.....	7
2 结论.....	8



# 1 产品安全解决方案

- 1.1 安全架构
- 1.2 设备安全
- 1.3 安全启动
- 1.4 Flash加密
- 1.5 Flash加扰
- 1.6 关键数据安全存储
- 1.7 驱动安全注意事项
- 1.8 其他使用安全注意事项

## 1.1 安全架构

产品的网络安全是一个系统工程，涉及到整个产品的各个层面。

Hi3861/Hi3861L版本可能涉及的威胁包括：

- 开机启动安全  
该部分主要涉及到系统启动过程中每一级镜像的校验机制。Hi3861/Hi3861L提供安全启动方案，ROM中固化一个RomBoot程序作为一级Boot。引导启动时，先通过RomBoot验证FlashBoot的数字签名，然后在FlashBoot中验证Kernel的数字签名，保证运行程序的安全性。
- 系统升级安全  
系统升级方案存在的安全威胁是文件本身的合法性和完整性。FlashBoot和Firmware都可升级，采用数字签名方式对升级文件进行校验，FlashBoot和Firmware都有版本防回滚机制，其版本号分别与EFUSE中的tee\_boot版本及tee\_firmware版本进行认证，认证不通过将无法启动。
- 固件代码安全  
Flash加密功能支持通过二级密钥加密架构为用户提供Flash上关键代码的加密保护，避免用户关键代码被读取、反编译后盗取。
- JTAG安全调试



JTAG调试功能默认开启，建议产品量产时将EFUSE中的JTM字段烧写为1来关闭JTAG调试功能。

## 1.2 设备安全

基于安全性考虑，建议用户在最终产品中执行以下措施：

- 启用安全启动特性。
- 永久关闭JTAG调试功能。

## 1.3 安全启动

### 1.3.1 启动方法

Hi3861/Hi3861L支持安全启动特性，安全启动有两种形式：

- 第一种方式：FlashBoot用RSA/ECC签名，RomBoot通过EFUSE中的根密钥Hash及FlashBoot的签名数据判断其合法性后引导启动FlashBoot。
- 第二种方式：FlashBoot用RSA/ECC签名，并且其代码段使用AES-CBC方式加密，RomBoot先对代码段进行解密，然后再进行RSA/ECC验签，判断其合法性后引导启动FlashBoot。

对于第一种只验签方式，用户需在EFUSE中配置根公钥的HASH值，并且打开安全启动开关。操作方法如下：

**步骤1** 写RSA根公钥SHA256值到EFUSE的root\_pubkey，并锁定该区域。

**步骤2** 写EFUSE的Secured Boot标识为0xFF打开安全启动开关，并锁定该区域。

----结束

对于第二种验签并加密方式，用户需在EFUSE中配置根公钥的HASH值以及加密密钥的HUK，并且打开安全启动开关和FlashBoot加密标识。操作方法如下：

**步骤1** 写RSA根公钥SHA256值到root\_pubkey，并锁定该区域。

**步骤2** 写EFUSE的Secured Boot标识为0xFF打开安全启动开关，并锁定该区域。

**步骤3** 写加密密钥32byte HUK码到EFUSE的root\_key，并锁定该区域。

**步骤4** 写EFUSE的Encrypt Flag为0xFF打开FlashBoot加密标识，并锁定该区域。

----结束

安全启动特性需要对FlashBoot、Kernel、升级文件进行数字签名，建议客户使用第二种安全性能更高的启动方式，并且使用服务器签名，保护好私钥防止泄露。

#### 说明

- EFUSE各项说明及锁定位说明请参见《Hi3861V100 / Hi3861LV100 EFUSE 使用指南》。
- 产线烧写EFUSE方法请参见《Hi3861V100 / Hi3861LV100 产线工装 用户指南》。

- RSA/ECC根公钥明文存放在FlashBoot文件头结构中。
- RSA/ECC根公钥的SHA256值存放在EFUSE中。
- RSA/ECC二级公钥用根私钥签名。
- FlashBoot用RSA/ECC二级私钥签名。
- FlashBoot中预置用户根公钥，用于验证Firmware公钥的合法性。FlashBoot启动Firmware时，需要验证Firmware的签名。
- 根密钥为RSA4096或ECDH\_BRAIN\_POOL\_P256R1格式，二级密钥为RSA2048或ECDH\_BRAIN\_POOL\_P256R1格式。根密钥确定后不能更改。
- 用户可根据需要配置FlashBoot中预置的用户根密钥，用户根密钥确定后不能更改。
- Firmware密钥用户可根据需要进行配置。
- 加密密钥由KDF算法派生而成。
- 加密密钥的IV值存放于FlashBoot文件二级密钥结构中。

根密钥、二级密钥、用户根密钥、Firmware密钥的签名方式需统一，不支持RSA和ECC两种签名方式混用的情况。

安全启动流程如图1-1所示。

The diagram illustrates the FlashBoot structure and its components, organized into three main sections: eFuse, FlashBoot, and Firmware.

- eFuse (Hi38XX SoC):** Contains five fields: Root Pubk Hash, SubKey Category, Revoked Subkey ID Mask, Enrypt Flag, and Tee Boot Ver. These fields are linked to the FlashBoot Header via arrows labeled 1, 3, 3, 3, and 3 respectively.
- FlashBoot:**
  - FlashBoot Header:** Contains Root Pubk, SubKey Category, SubKey ID, SubKey, Encrypt Info, Boot Version, DIE ID, and Root PriK Signature. The Root Pubk field is linked to the Root Pubk Hash in eFuse via arrow 1. The SubKey Category, SubKey ID, SubKey, Encrypt Info, Boot Version, and DIE ID fields are linked to the SubKey Category, SubKey ID Mask, Enrypt Flag, and Tee Boot Ver fields in eFuse via arrows labeled 3. The Root PriK Signature field is linked to the Root PriK Signature field in the Firmware Code Section via arrow 4.
  - Code Section Signature:** Located below the FlashBoot Header.
  - FlashBoot Code Section:** A large section containing the User Root Cert field.
- Firmware:**
  - Firmware Code Section:** Contains the Firmware Pubk, Pubk Signature, and Firmware Signature fields. The User Root Cert field in the FlashBoot Code Section is linked to the Firmware Pubk field in the Firmware Code Section via arrow 2.

**步骤1** 检查是否为安全启动模式（推荐使用安全启动）。如果为非安全启动模式（不推荐），计算FlashBoot从头到代码段结尾区域的HASH值与FlashBoot末尾的HASH值对比，如果一致，则直接引导FlashBoot；如果为安全启动，进入步骤**步骤2**。

**步骤2** 用存放在EFUSE中的根公钥HASH值验证FlashBoot头部的根公钥。

**步骤3** 用FlashBoot头部的根公钥验证FlashBoot头部的二级公钥（Subkey）。





- 步骤4** 验证二级公钥的分类（Category）是否与EFUSE中存储的分类匹配。
- 步骤5** 验证二级公钥的ID是否在[0,23]范围内。
- 步骤6** 验证二级公钥的ID是否已被吊销（验证方法：与EFUSE中的RSIM项比对）。RSIM（Revoked Subkey Id Mask）是一个24bit位图，表示每个二级公钥的状态。如果RSIM的“Subkey ID”位为“1”（ $((1 \leq \text{Subkey\_ID}) \& \text{RSIM}) == 1$ ），则该公钥被吊销，身份验证失败。
- 步骤7** 如果EFUSE中的Encrypt Flag标志不是0x42，或二级密钥中的Encrypt Flag标志不是0x42，则对代码段进行解密。解密密钥由EFUSE中的HUK和salt通过KDF派生而来。salt是32byte，前16byte在二级密钥结构中，后16byte在RomBoot中硬编码。
- 步骤8** 验证FlashBoot版本，防版本回滚，先判断版本是否在[0,16]范围内，再通过EFUSE中的tee\_boot版本进行身份验证。算法如下：
- 如果boot\_ver==0且tee\_boot\_ver==0，验证通过。
  - 如果boot\_ver>0且（tee\_boot\_ver>>（boot\_ver-1））==1，验证通过。
- 步骤9** 用预置在FlashBoot中的用户公钥验证Firmware公钥的数字签名。
- 步骤10** 使用Firmware公钥验证Firmware的数字签名。
- 步骤11** 启动Firmware。

#### ----结束

单板维修调测流程（如果单板维修或取回外场模块在实验室定位问题时，需要烧写研发程序测试，将引入以下维修流程）：

- 步骤1** 提供DIE ID信息给客户，客户对FlashBoot签名时传入DIE ID生成维修FlashBoot。
- 步骤2** 启动时RomBoot判断FlashBoot为维修版本，对DIE ID进行验证，验证通过则启动FlashBoot。

#### ----结束

### 1.3.2.2 二级密钥 ID

二级密钥ID范围为0~23。

### 1.3.2.3 安全启动开启流程

安全启动开启流程如下：

- 步骤1** 通过工具生成安全启动需要的密钥证书，包括根密钥、二级密钥、用户根密钥、Firmware密钥四个证书及AES加解密需要的三组随机数（32byte HUK、16byte salt、16byte IV）。
- 步骤2** 读取用户根密钥的公钥，将其写入FlashBoot的代码中。
- 步骤3** 将所有证书及随机数放到签名工具目录下。
- 步骤4** 通过Menuconfig打开安全启动功能。
- 步骤5** 配置签名工具命令，编译时自动签名FlashBoot和Firmware。
- 步骤6** 读取根密钥的公钥，将其通过SHA256计算后的HASH值写入EFUSE对应区域。
- 步骤7** 根据需要配置EFUSE的加解密标志、二级密钥分类、二级密钥ID等区域。



**步骤8** 烧写编译生成的镜像。

----结束

#### 说明

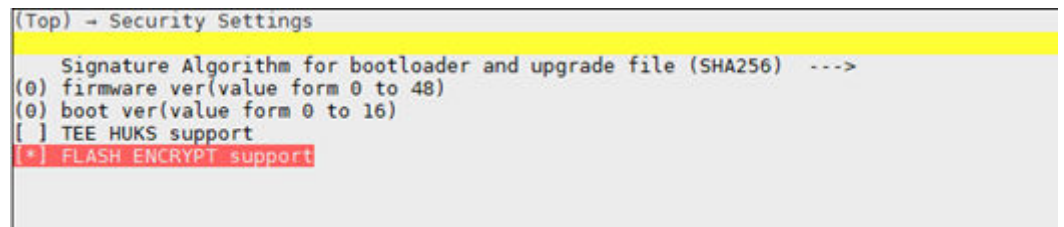
- EFUSE各项说明及锁定位说明请参见《Hi3861V100 / Hi3861LV100 EFUSE 使用指南》。
- 密钥配置具体方法请参见《Hi3861V100 / Hi3861LV100 Boot移植应用 开发指南》。

## 1.4 Flash 加密

Flash加密功能支持通过二级密钥加密架构为用户提供Flash上关键代码的加密保护，工作原理如下：

- Flash加密功能通过编译宏隔开，该宏可以从menuconfig开启：

图 1-2 menuconfig 开启 Flash 加密功能



- Flash加密功能开启，HiBurn烧写Flash完成后，会对代码段前4K进行加密；
- 烧写完成后重新启动，Flashboot引导程序将加密的数据解密到指定的内存中。

#### 说明

- Flash加密功能可有效避免关键代码被读取、反编译后盗取，建议用户在量产产品中开启此功能。
- Flash代码段加密功能详细介绍及使用方法请参见《Hi3861V100 / Hi3861LV100 安全模块使用指南》。

## 1.5 Flash 加扰

打开Flash加扰功能后通过加扰因子对写入Flash的数据进行了加扰，可有效保护固件和Flash上存储的用户数据被盗取。通过CPU读取Flash数据时会通过加扰因子进行解扰，不影响正常业务。

Flash加扰功能开启流程如下：

- 步骤1** 生成10bit的随机数做为加扰因子。
- 步骤2** 将加扰因子写入EFUSE的user\_flash\_ind区域并锁定。
- 步骤3** 将EFUSE的flash\_scramble\_en区域写为1并锁定。
- 步骤4** 通过Hiburn烧写编译生成的镜像。

----结束



## 说明

注意：开启Flash加扰后CPU读取Flash内原有数据时会经过加扰因子处理，与原值不同，所以需要先开启Flash加扰功能，再烧写镜像。

## 1.6 关键数据安全存储

用户记录账号、密码等保密信息时，需要保证这些数据的存储安全，所以要求这些数据在存储之前进行加密保护。用户关键数据的安全存储方案的详细设计请参见《Hi3861V100 / Hi3861LV100 安全模块 使用指南》。

## 1.7 驱动安全注意事项

### 1.7.1 Cipher 驱动

Cipher驱动实现了标准的对称加密AES、非对称加密RSA、ECDH、摘要算法SHA256/HMAC，密钥派生算法KDF等，未使用任何私有算法。使用时请注意：Cipher密钥的长度越长，安全等级越高，因此建议使用AES 128bit及以上的密钥、RSA 2048bit及以上的密钥，详细内容请参见《Hi3861V100 / Hi3861LV100 API 开发参考》。

#### 须知

密钥派生算法KDF迭代次数低于1000可能有被破解的风险，所以使用KDF派生密钥时，建议迭代次数设置不少于1000。

### 1.7.2 串口

串口属于通用设备通信的协议，根据业务可分为调试串口和业务串口：

- 调试串口：基于RS232的串口，主要用于设备的近端底层调测。
- 业务串口：基于RS232的串口，主要用于业务报文的收发。  
建议在条件允许的情况下，增加安全认证机制和报文加密机制。

如果不使用串口，可在产品出厂时配置EFUSE（写UTMx为1），将串口永久关闭。

#### 须知

串口永久关闭后将无法打开。

## 1.8 其他使用安全注意事项

### 1.8.1 JTAG 接口

恶意攻击者通过JTAG接口，可以篡改系统的任何配置，恶意破坏系统，因此建议用户采取措施：产品出厂时，配置EFUSE（写JTM为1），将JTAG永久关闭。



## 1.8.2 代码安全注意事项

代码错误引发的网络安全问题，一般都是源于最基本的代码规范问题，例如：指针越界、数组越界、入参不检查等错误。建议通过如下方法检查：

- 使用业界通用的代码健康扫描工具进行全覆盖扫描。
- 使用模糊测试工具，对所有API接口（包括设备驱动接口）进行全范围模糊测试。
- 使用业界通用的漏洞扫描工具对所使用的开源软件进行扫描。

## 1.8.3 可维可测注意事项

- 可维可测方案仅在调试时打开，Release版本建议用户关闭
- HSO调试工具目前仅用于SDK问题定位时的调测日志打印。
- 可维可测接口详细使用方法请参见《Hi3861V100 / Hi3861LV100 SDK 开发指南》。



## 2 结论

Hi3861/Hi3861L产品有必要基于安全威胁分析采取相对应的安全措施。以下安全原则供参考：

- 适度的安全  
安全设计是基于特定的安全危险场景分析，考虑到性能、成本、业务影响，决策采用最合适的安全措施。
- 最小授权  
根据职责的需要，给用户、维护人员、网络单元、程序、进程等授予最小的权限和资源。这样能减少潜在的安全风险。
- 主动协同防御  
及时识别恶意攻击源，并在攻击造成显著危害前自动删除恶意用户和网络之间的连接。也可以降低连接的带宽和服务质量，以尽量减少负面影响。
- 纵深防御  
纵深防御原则涉及到对威胁的多重防御。例如，当一个防御层不够时，另一个防御层将防止造成进一步破坏。