



Unisoc Confidential For hiar

Android 11.0 SIMLOCK 安全方案下的 IMEI 保护方案使用指南

文档版本
发布日期

V1.0
2020-08-07

版权所有 © 紫光展锐科技有限公司。保留一切权利。

本文件所含数据和信息都属于紫光展锐所有的机密信息，紫光展锐保留所有相关权利。本文件仅为信息参考之目的提供，不包含任何明示或默示的知识产权许可，也不表示有任何明示或默示的保证，包括但不限于满足任何特殊目的、不侵权或性能。当您接受这份文件时，即表示您同意本文件中内容和信息属于紫光展锐机密信息，且同意在未获得紫光展锐书面同意前，不使用或复制本文件的整体或部分，也不向任何其他方披露本文件内容。紫光展锐有权在未经事先通知的情况下，在任何时候对本文件做任何修改。紫光展锐对本文件所含数据和信息不做任何保证，在任何情况下，紫光展锐均不负任何与本文件相关的直接或间接的、任何伤害或损失。

请参照交付物中说明文档对紫光展锐交付物进行使用，任何人对紫光展锐交付物的修改、定制化或违反说明文档的指引对紫光展锐交付物进行使用造成的任何损失由其自行承担。紫光展锐交付物中的性能指标、测试结果和参数等，均为在紫光展锐内部研发和测试系统中获得的，仅供参考，若任何人需要对交付物进行商用或量产，需要结合自身的软硬件测试环境进行全面的测试和调试。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。

Unisoc Confidential For hiar

紫光展锐科技有限公司



前言

概述

本文档详细地描述了基于 SIMLOCK 安全方案的 IMEI 保护方案的实现原理、启用以及配置。

读者对象

本文档主要适用于展锐 SIMLOCK 安全方案的 IMEI 保护方案配置、验证工作人员。配置、验证人员必须具备以下经验和技能：


- 了解展锐平台方案。
- 熟悉理解 IMEI 相关知识。

缩略语

缩略语	英文全名	中文解释
IMEI	International Mobile Equipment Identity	国际移动设备
AES	Advanced Encryption Standard	高级加密标准，常见的一种对称加密算法
UID	Unique Identifier	唯一标识符

符号约定

在本文中可能出现下列标志，它所代表的含义如下。

符号	说明
 说明	用于突出重要/关键信息、补充信息和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害。

变更信息

文档版本	发布日期	修改说明
V1.0	2020-08-07	第一次正式发布。

关键字

SIMLOCK、IMEI。

Unisoc Confidential For hiar

目 录

1 概述	1
2 IMEI 方案启用和配置	2
2.1 启用	2
2.2 配置	2
3 Q&A	4

Unisoc Confidential For hiar

图目录

图 1-1 IMEI 的校验和恢复流程.....	1
图 2-1 WriteIMEI 工具设置.....	2

Unisoc Confidential For hiar

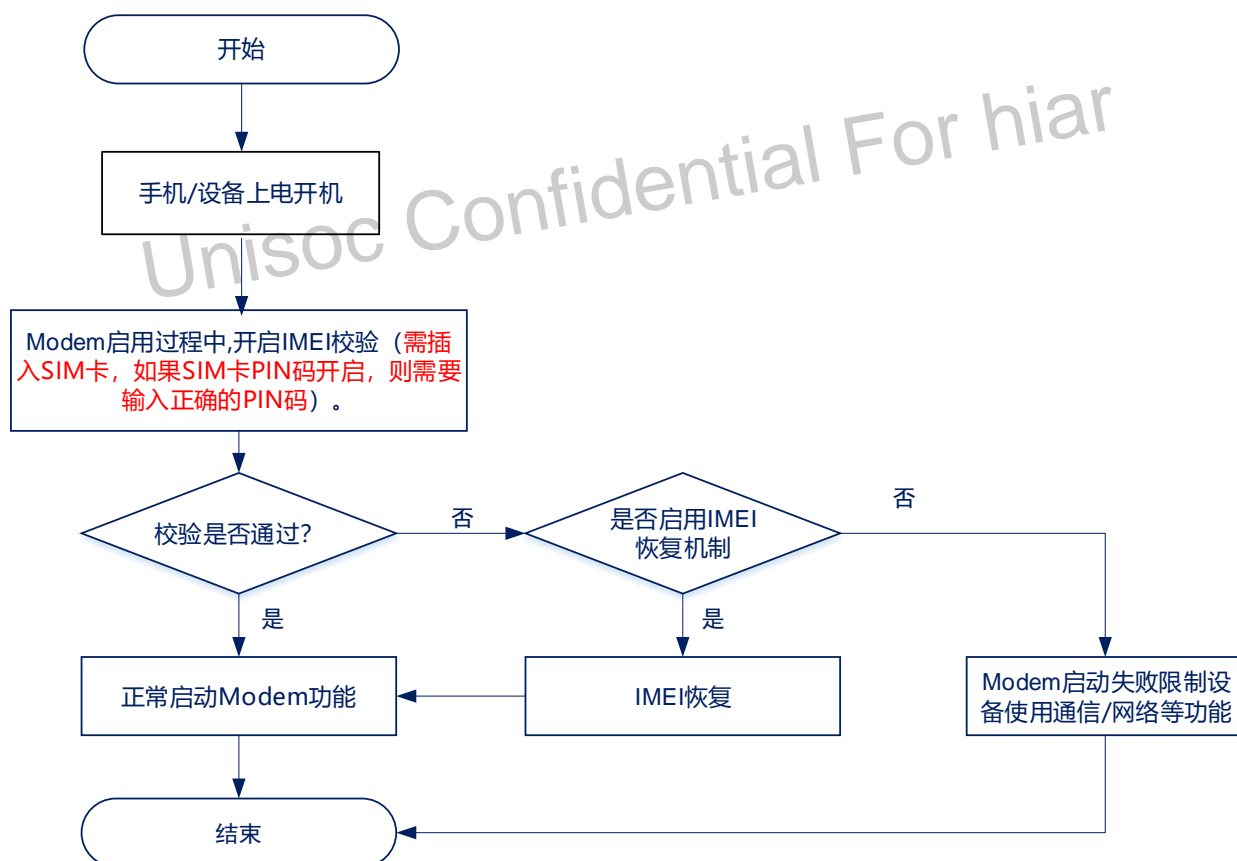
1 概述

基于 SIMLOCK 安全方案的 IMEI 保护方案，具有以下特点：

- 该 IMEI 保护方案采用 AES 对称加密算法来实现加密保护，由每一颗芯片自带的 UID 通过 Hash 算法生成密钥。所以，在 IMEI 明文相同的场景下，每一台设备加密之后的密文都是不同的，以此来最大化的保护每一台设备的 IMEI 数据。
- 该 IMEI 保护方案可以在 IMEI 受到非法篡改的场景下，纠正非法 IMEI，恢复原有的 IMEI 数据，保证设备的正常运行。
- 该 IMEI 保护方案当前仅支持一个 IMEI 的保护，可以通过配置文件指定需要保护的 IMEI，具体配置方式请参见 2.2 节配置。

该 IMEI 保护方案的校验和恢复流程如图 1-1。

图1-1 IMEI 的校验和恢复流程



2 IMEI 保护方案启用和配置

2.1 启用

基于 SIMLOCK 安全方案实现的 IMEI 保护方案，是通过 SIMLOCK 的配置工具 WriterIMEI 写入配置数据，启动 SIMLOCK 的 Verify 流程来启动 IMEI 保护方案的。

客户端在 WriteIMEI 工具中写 SIMLOCK 功能，需要在 WriterIMEI 的设置页面中勾选“Write Simlock”选项来开启写 SIMLOCK 功能，如图 2-1 所示。

图2-1 WriterIMEI 工具设置

设置

☐ 各IMEI相同

☒ IMEI (主卡) ☐ IMEI2 ☐ IMEI3 ☐ IMEI4

默认IMEI 手动输入 手动输入 手动输入

☐ 蓝牙 ☐ 自动生成蓝牙 ☐ WIFI ☐ 自动生成WIFI

- 蓝牙设备地址的自动生成方式 -

☐ 按时间 ☒ 按起始地址累加 002715082c32 终止地址 00203040508

地址文件路径 ..

- WIFI地址的自动生成方式 -

☒ 按默认地址生成 ☐ 按起始地址累加 002715082c38 终止地址 010203040508

地址文件路径 ..

自动IMEI (主卡) 起始号 (勾选“自动生成IMEI”时有效):

36252343242537

☒ IMEI合法性检查 (检查第15位) ☐ 保存IMEI (保存在exe目录下)

☐ IMEI重复性检查 (从已保存IMEI的文件中查询) ☐ 保存IMEI到txt格式文件

☐ 保存IMEI到本地数据库文件

☐ SN1 ☐ 自动生成SN1 ☐ SN2 ☐ 自动生成SN2

☒ Write SimLock

2.2 配置

通过配置 XML 文件可以开启/关闭 SIMLOCK 功能，以及保护指定的 IMEI。

IMEI 保护方案具体配置说明、SIMLOCK 功能说明以及对应配置项在 XML 文件中的位置具体如下：

- IMEI 保护方案配置项说明：

IMEI 选择保护配置：dummy4 value

- Dummy4 value=0：启用 IMEI1 的保护
- Dummy4 value=1：启用 IMEI2 的保护
- Dummy4 value=2：启用 IMEI3 的保护
- Dummy4 value=3：启用 IMEI4 的保护

- Simlock 功能

Simlock 功能开关：Support value

- Support value=0：SIMLOCK 功能关闭
- Support value=1：打开卡 1 的 SIMLOCK 功能
- Support value=2：打开卡 2 的 SIMLOCK 功能
- Support value=3：打开双卡的 SIMLOCK 功能

- 对应配置项在 XML 文件中的位置如下：

```
<SIMLOCK version="3"max locks="128">
<CUSTOMIZE DATA>
<support value="0"/>
<max num trials value="3"/>
<control key type value="4"/>
<dummy1 value="0"/>
<dummy2 value="0"/>
<dummy3 value="0"/>
<dummy4 value="0"/>
```

Unisoc Confidential For hiar

3

Q&A

Q: 如何不启用 SIMLOCK, 只启用 IMEI 的保护方案?

A: 可以通过 Support Value 的设置关闭 SIMLOCK 功能, 在启用 IMEI 而不启用 SIMLOCK (Support Value=0) 功能的情况下, SIMLOCK 的所有缺省内容仍然会被校验, 只是 SIMLOCK 功能被关闭, 在实际应用场景下不生效。

Unisoc Confidential For hiar