



Unisoc Confidential For hiar

# SIMLOCK 安全方案配置说明

文档版本  
发布日期

V1.0  
2020-04-27

**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 SIMLOCK 安全方案配置说明和校验测试建议，并提供了一个具体配置的实例。适应 SIMLOCK V5 及以上版本。

## 读者对象

本文档主要适用于展锐 SIMLOCK 安全方案配置、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 SIM 卡相关知识。

## 缩略语

缩略语	英文全名	中文解释
SIM	Subscriber Identity Module	用户识别模块

## 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	2020-04-27	第一次正式发布。

## 关键字

SIMLOCK、XML 配置

Unisoc Confidential For hiar

# 目 录

1 配置说明 .....	1
1.1 配置总开关及锁类型 .....	1
1.2 配置锁类型 <code>simlock_status</code> .....	1
1.3 配置白名单 .....	2
1.4 配置密码类型 .....	2
1.5 配置解锁功能关闭 .....	2
1.6 配置最大解锁次数限制 .....	3
1.7 配置五种锁的关系 .....	3
1.8 配置 <code>SIMLOCK PUK</code> 开关 .....	4
1.9 配置两卡白名单独立控制 .....	4
1.10 配置 <code>IMEI</code> 选择性保护控制 .....	5
2 校验测试 .....	6
2.1 防篡改测试 .....	6
2.2 常规功能测试 .....	6
2.3 稳定性测试 .....	7
2.4 校准测试 .....	7
3 配置实例 .....	8

## 图目录

---

图 1-1 网络锁卡 1 卡 2 名单分开配置示例.....	5
--------------------------------	---

Unisoc Confidential For hiar

# 1 配置说明

本章节详细说明 SIMLOCK NV 配置，V5 以后的版本是通过 XML 文件配置，XML 文件值设置按十进制，工具写入。其他版本要用 NEditor 工具手动配置。

## 1.1 配置总开关及锁类型

NV: TD\_TIANJI2\_NV\_TYPE --> NV\_PARAM\_TYPE\_SIM\_CFG1 --> is\_support\_gsm\_only

XML 项:

```
<CUSTOMIZE_DATA>
  <support value="19"/>
```

取值按位配置 bit0~bit7 :

- 第 1 位(bit0): 卡 1 simlock 开关
- 第 2 位(bit1): 卡 2 simlock 开关
- 第 3 位(bit2): 卡 3 simlock 开关, 暂时没有卡 3, 预留位
- 第 4 位(bit3): 开启网络锁 network lock
- 第 5 位(bit4): 开启网络子锁 networksubset lock
- 第 6 位(bit5): 开启 SP 锁
- 第 7 位(bit6): 开启 CP 锁
- 第 8 位(bit7): 开启 user 锁

比如: 要开启卡 1 卡 2 的网络锁, is\_support\_gsm\_only 应该配置为: 0x0B, 开启卡 1 卡 2 的网络子锁, is\_support\_gsm\_only 应该配置为: 0x13

对于非 SIMLOCK 版本 (open market), 确保关闭 SIMLOCK 总开关 (is\_support\_gsm\_only 设置为 0x00。默认是打开的 (0x0F), 如果同时开启了 unlock\_diable 功能会导致所有卡都不能用, 注意关闭。

## 1.2 配置锁类型 simlock\_status

NV: SIM\_LOCK\_CUSTOMIZE\_DATA --> sim\_lock\_status

SIM\_LOCK\_USER\_DATA --> sim\_lock\_status

XML 项:

```
<USER_DATA>
  <simlock_status value="5"/>
```

按位配置，置 1 开该种锁，置 0 不开该种锁。

- 第 0 位：network locks;
- 第 1 位：network subset locks;
- 第 2 位：SP locks;
- 第 3 位：corporate locks;
- 第 4 位：SIM locks。

## 1.3 配置白名单

以网络锁为例：

NV: SIM\_LOCK\_CUSTOMIZE\_DATA --> network\_locks

XML 项：

```
<CUSTOMIZE_DATA>
  <NETWORK_LOCKS sim1_locks="3">
    <ITEM mcc="460" mnc="00"/>
    <ITEM mcc="460" mnc="02"/>
    <ITEM mcc="460" mnc="07"/>
  </NETWORK_LOCKS>
```

例如对于网络锁配置（其他锁内容参照 NV 结构做类似配置）：

XML 配置白名单时，MCC 请配置非零的数据，如果某种锁没开启，XML 该锁名单项不要填写内容。  
sim1\_locks 配置说明参考 1.9 内容。

## 1.4 配置密码类型

NV: BaseParam->SIM\_LOCK\_CONTROL\_KEY --> control\_key\_type

XML 项：

```
<CUSTOMIZE_DATA>
  <control_key_type value="4"/>
```

根据客户需要配置，安全方案 V5 以后版本配置为 4。

## 1.5 配置解锁功能关闭

NV: BaseParam --> SIM\_LOCK\_CUSTOMIZE\_DATA --> dummy3.bit2=1(bit7,...,bit0)

XML 项：

```
<CUSTOMIZE_DATA>
```



```
<dummy3 value="4"/>
```

BaseParam --> SIM\_LOCK\_CUSTOMIZE\_DATA --> dummy3.bit2=1(bit7,...,bit0) 配置为 1（默认值为 0），同时需要按开启的锁类型配置 is\_support\_gsm\_only 高五位。

## 1.6 配置最大解锁次数限制

NV: BaseParam --> SIM\_LOCK\_USER\_DATA --> max\_num\_trials

XML 项:

```
<CUSTOMIZE DATA>
  <max_num_trials value="50000"/>
```

BaseParam --> SIM\_LOCK\_USER\_DATA --> nck\_trials/ nsck\_trials/ spck\_trials/ cck\_trials/ pck\_trials

网络锁/网络子锁/SP 锁/CP 锁/user 锁 默认最大解锁次数为 10 次,输错至最大解锁次数后就进入永久锁卡状态。可以通过 NV 配置修改为客户期望的最大解锁次数。

## 1.7 配置五种锁的关系

NV: BaseParam --> SIM\_LOCK\_CUSTOMIZE\_DATA --> dummy3 .bit3=1(bit7,...,bit0)

XML 项:

```
<CUSTOMIZE DATA>
  <dummy3 value="8"/>
```

BaseParam --> SIM\_LOCK\_CUSTOMIZE\_DATA --> dummy3 .bit3=1(bit7,...,bit0):

- 按位控制，默认值为 0。
- 按‘与’的关系进行控制，需要同时符合所有开启的锁的卡才能使用。同时配置多种锁，注意各种锁的逻辑关系。如果相互包含就不必配置，否则要多次解锁才能用，密码维护繁琐。
- ‘或’的关系是满足所配置任何一种锁的卡就可以正常使用；多种锁的或关系，要注意各种锁所锁定 IMSI 字段的相互包含关系。
- 强烈建议客户简化锁类型，避免多重锁配置。
- 对于运营商，一般情况下网络锁/网络子锁就能满足定制要求。
- 网络锁锁的是 PLMN，其他四种锁都包含了 PLMN 字段，所以其他四种锁有设置，网络锁就没必要同时开启且设置一样的 PLMN。

举例:

要配置网络子锁，该子锁的 PLMN 配置在网络锁白名单，就会导致网络子锁失效，说明如下:

开启联通网络锁/移动网络子锁，配置白名单网络锁填 46001，网络子锁填 4600205，插入联通卡，预期正常驻留，插入移动 4600205 的卡，预期正常驻留，插入移动其他子锁，如 4600208 或 460007xx 的卡，被锁。而如果移动 PLMN 46002 配置在网络锁白名单，则 4600205 的子锁失效，所有 46002 的移动卡都可用。

## 1.8 配置 SIMLOCK PUK 开关

NV: BaseParam --> SIM\_LOCK\_CUSTOMIZE\_DATA --> dummy3 .bit0=1(bit7,...,bit0)

BaseParam --> SIM\_LOCK\_CUSTOMIZE\_DATA --> dummy3 .bit1=1(bit7,...,bit0)

XML 项:

```
<CUSTOMIZE_DATA>
  <dummy3 value="3"/>
```

支持 SIMLOCK PUK, 需开启如下两个 NV 比特位:

BaseParam --> SIM\_LOCK\_CUSTOMIZE\_DATA --> dummy3 .bit0=1(bit7,...,bit0)

BaseParam --> SIM\_LOCK\_CUSTOMIZE\_DATA --> dummy3 .bit1=1(bit7,...,bit0)

PUK 功能并没有太多实际意义, 不建议客户使用。如果担心用户容易尝试完最大解锁次数而进入永久锁状态, 可以按 1.6 章节将最大解锁次数 NV 配置为一个较大的值 (比如 100 次, 默认 10 次), 且 PUK 态下不支持 1.9 章节所描述的卡 1 卡 2 独立锁卡功能。

## 1.9 配置两卡白名单独立控制

NV: SIM\_LOCK\_CUSTOMIZE\_DATA.dummy3.bit4 (bit7,...,bit0)

XML 项:

```
<CUSTOMIZE_DATA>
  <dummy3 value="16"/>
```

SIM\_LOCK\_CUSTOMIZE\_DATA.dummy3.bit4 (bit7,...,bit0):

- 设置为 0 (默认值), 则是默认的卡 1 卡 2 共用白名单(也就是两卡的白名单是一样的), XML 中 **sim1\_locks** 配置项需配置为对应锁所有白名单个数 (此时不要依据名字判断含义)。
- 设置为 1, 表示卡 2 的名单不同于卡 1。
  - 锁名单先配置卡 1 名单, 再连续配置卡 2 名单, XML 中参数 **sim1\_locks** 配置项设置为卡 1 白名单数目。
  - **sim1\_locks** 与实际 XML 配置的卡 1 白名单数目保持一致。
  - 卡 2 名单数目不需要配置。
  - 任何一张卡开启了某种锁, **user\_data.simlock\_status** 及 **is\_support\_gsm\_only** 对应的 bit 置为 1。如果某 bit 位对应的锁, 其实只有一张卡用, 那么另一张卡名单不配置就可以。比如: 卡 1 开 SP 锁, 卡 2 开网络锁, 则 **user\_data.simlock\_status = 5**, **is\_support\_gsm\_only=43**, 网络锁 **sim1\_locks=0** 配置的名单为卡 2 网络锁名单, SP 锁 **sim1\_locks=n** 配置的 n 个名单为卡 1 的 SP 锁名单。参考配置实例 3 章。
  - 独立配置白名单的情况下暂时不支持解锁功能, 如果开启独立配置名单请同时按第 5 点关闭解锁功能。该功能暂时不支持与卡槽依赖功能的组合, 如果客户需要, 请客户充分测试验证。
  - 开启了卡槽白名单独立配置, 总开关请开启双卡 (双卡才存在独立配置, 锁单卡的情况, 保持默认关闭独立配置功能)。请保证每张卡都在某种开启的锁上有配置白名单 (如果没有白名单, 任何卡都可以用, 相当于总开关关闭了该卡的 SIMLOCK)。

举例网络锁卡 1 卡 2 名单分开配置, 如下 XML 中网络锁项配置情况如图中文字所述:

图1-1 网络锁卡 1 卡 2 名单分开配置示例

```
<NETWORK_LOCKS sim1 locks="6"> 数字6表示卡1网络锁
白名单个数
<ITEM mcc="460" mnc="00"/>
<ITEM mcc="460" mnc="02"/>
<ITEM mcc="460" mnc="07"/>
<ITEM mcc="520" mnc="00"/>
<ITEM mcc="520" mnc="04"/>
<ITEM mcc="520" mnc="99"/>
此6个名单为卡1网
络锁白名单个

<ITEM mcc="460" mnc="00"/>
<ITEM mcc="460" mnc="02"/>
<ITEM mcc="460" mnc="07"/>
<ITEM mcc="520" mnc="04"/>
<ITEM mcc="520" mnc="99"/>
<ITEM mcc="460" mnc="06"/>
<ITEM mcc="460" mnc="01"/>
<ITEM mcc="520" mnc="01"/>
<ITEM mcc="520" mnc="03"/>
<ITEM mcc="520" mnc="23"/>
<ITEM mcc="520" mnc="05"/>
<ITEM mcc="520" mnc="18"/>
<ITEM mcc="520" mnc="15"/>
此13个名单为卡2网
络锁名单

</NETWORK_LOCKS>
```

## 说明

user 锁不支持独立配置

如果 XML 有 sim1 locks 配置项，则该项一定要按 SIM\_LOCK\_CUSTOMIZE\_DATA.dummy3.bit4 的取值情况对应配置，如果配置错误，会影响锁卡逻辑。

## 1.10 配置 IMEI 选择性保护控制

IMEI 可通过 xml 配置进行选择保护控制

其中，

SIM\_LOCK\_CUSTOMIZE\_DATA.dummy4=0，IMEI1 参与保护

SIM\_LOCK\_CUSTOMIZE\_DATA.dummy4=1，IMEI2 参与保护

SIM\_LOCK\_CUSTOMIZE\_DATA.dummy4=2，IMEI3 参与保护

SIM\_LOCK\_CUSTOMIZE\_DATA.dummy4=3，IMEI4 参与保护

Xml 对应配置位置

```
<CUSTOMIZE DATA>
<dummy4 value=" "/>
```

# 2

## 校验测试

SIMLOCK 配置是否正确生效，需要进行验证与测试；可以按以下四大项测试项来测试每项的 case。

### 2.1 防篡改测试

对于已经使用过 NV 签名工具烧写过 simlock 数据后的手机，进行以下两项测试，出现以下测试现象表明已经生效。

- 任意篡改以下 16 条数据的任一处，将出现开机驻网失败：
  - BaseParam --> SIM\_LOCK\_CUSTOMIZE\_DATA --> max\_num\_trials
  - BaseParam --> SIM\_LOCK\_CUSTOMIZE\_DATA --> network\_locks
  - BaseParam --> SIM\_LOCK\_CUSTOMIZE\_DATA --> network\_subset\_locks
  - BaseParam --> SIM\_LOCK\_CUSTOMIZE\_DATA --> sp\_locks
  - BaseParam --> SIM\_LOCK\_CUSTOMIZE\_DATA --> corporate\_locks
  - BaseParam --> SIM\_LOCK\_CUSTOMIZE\_DATA --> dummy1~dummy4
  - BaseParam --> SIM\_LOCK\_USER\_DATA --> sim\_lock\_status
  - BaseParam --> SIM\_LOCK\_USER\_DATA --> user\_locks
  - BaseParam --> SIM\_LOCK\_USER\_DATA --> nck\_trials
  - BaseParam --> SIM\_LOCK\_USER\_DATA --> nsck\_trials
  - BaseParam --> SIM\_LOCK\_USER\_DATA --> spck\_trials
  - BaseParam --> SIM\_LOCK\_USER\_DATA --> cck\_trials
  - BaseParam --> SIM\_LOCK\_USER\_DATA --> pck\_trials
  - BaseParam --> SIM\_LOCK\_CONTROL\_KEY --> control\_key\_type
  - TD\_TIANJI2\_NV\_TYPE --> NV\_PARAM\_TYPE\_SIM\_CFG1 --> is\_support\_gsm\_only
  - TD\_TIANJI2\_NV\_TYPE --> NV\_PARAM\_TYPE\_MN\_CFG --> sim\_slot\_cfg(该项仅适用于 V6)
- 测试 SIMLOCK 版本清零以下两项 NV 值，查看是否能正常锁卡。
  - BaseParam->SIM\_LOCK\_CUSTOMIZE\_DATA --> sim\_lock\_status
  - BaseParam->SIM\_LOCK\_USER\_DATA --> sim\_lock\_status

### 2.2 常规功能测试

正常解完锁后，能够驻网，以下现象为正常，否则失败。

- 解锁之前只能拨打紧急呼叫
- 解完锁后，基本通信功能，像打电话、短信、电话簿查询正常。

- 对于支持 SIM 卡热插拔的产品，解锁前热插拔白名单卡/黑名单卡，确认是否能正常锁卡，解锁后热插拔白名单卡/黑名单卡，看是否正常驻网。

## 2.3 稳定性测试

驻网情况下，取多台样机进行压力测试，以下现象为正常：

- 驻网正常
- 基本通信功能正常
- 长时间开关飞行模式，正常驻网
- 长时间进行 ps 业务，能够正常打开网页，发送彩信
- 长时间进行 cs 业务，能够保持通话，不掉话

## 2.4 校准测试

通过以下测试为 OK

- 安排 common 校准综测，校准综测 GSM 和 WCDMA
- 安排 FDT 校准综测，校准综测 GSM 和 WCDMA
- 只校准 W AFC, AGC 和 APC，然后综测 WCDMA 性能
- 只校准 ADC, W AFC, AGC 和 APC，然后综测 WCDMA 性能
- 打开 SLOG，只校准 ADC, W AFC, AGC 和 APC，然后综测 WCDMA 性能

# 3

## 配置实例

开启卡 1 卡 2 SIMLOCK，卡 1 用 SP 锁，卡 2 用网络锁 XML 配置实例

```
<SIMLOCK version="3" max_locks="64">
  <CUSTOMIZE DATA>
    <support value="43"/> <!--开启卡 1 卡 2SIMLOCK，开启的锁为网络锁，SP 锁 -->
    <max_num_trials value="3"/> <!--最大解锁次数 -->
    <control key type value="4"/>
    <dummy1 value="0"/>
    <dummy2 value="0"/>
    <dummy3 value="20"/> <!--不支持解锁，卡 1 卡 2 白名单相互独立配置 -->
    <dummy4 value="0"/>
    <NETWORK_LOCKS sim1_locks="0"> <!--卡 1 网络锁名单个数为 0，其实就是只有卡 2 锁网络锁 -->
      <ITEM mcc="460" mnc="00"/>
      <ITEM mcc="460" mnc="02"/>
      <ITEM mcc="460" mnc="07"/>
      <ITEM mcc="520" mnc="04"/>
      <ITEM mcc="520" mnc="99"/>
      <ITEM mcc="460" mnc="06"/>
      <ITEM mcc="460" mnc="01"/>
      <ITEM mcc="520" mnc="01"/>
      <ITEM mcc="520" mnc="03"/>
      <ITEM mcc="520" mnc="23"/>
      <ITEM mcc="520" mnc="05"/>
      <ITEM mcc="520" mnc="18"/>
      <ITEM mcc="520" mnc="15"/>
    </NETWORK_LOCKS>
    <NETWORK SUBSET LOCKS sim1_locks="0">
      <ITEM mcc="0" mnc="0" subset1="0" subset2="0"/>
    </NETWORK SUBSET LOCKS>
    <SP LOCKS sim1_locks="6"> <!--卡 1 SP 锁名单个数为 6 且锁名单内容为 6 个，其实就是只有卡 1 锁 SP 锁 -->
      <ITEM mcc="520" mnc="00" sp="1"/>
      <ITEM mcc="520" mnc="04" sp="1"/>
      <ITEM mcc="520" mnc="99" sp="1"/>
      <ITEM mcc="460" mnc="00" sp="255"/>
      <ITEM mcc="460" mnc="02" sp="255"/>
      <ITEM mcc="460" mnc="07" sp="255"/>
    </SP LOCKS>

    <CORPORATE LOCKS sim1_locks="0">
      <ITEM mcc="0" mnc="00" sp="0" corporate="0"/>
    </CORPORATE LOCKS>

    <USER LOCKS sim1_locks="0">
      <ITEM imsi="0"/>
    </USER LOCKS>

    <encrypted CRC v1="0" v2="0" v3="0" v4="0"/>
  </CUSTOMIZE_DATA>
```

```
<USER_DATA>
  <simlock_status value="5"/><!--开启网络锁与 SP 锁 -->
  <nck_trials value="0"/>
  <nck_unlock_time value="0"/>
  <nsck_trials value="0"/>
  <nsck_unlock_time value="0"/>
  <spck_trials value="0"/>
  <spck_unlock_time value="0"/>
  <cck_trials value="0"/>
  <cck_unlock_time value="0"/>
  <pck_trials value="0"/>
  <pck_unlock_time value="0"/>
</USER_DATA>
</SIMLOCK>
```

Unisoc Confidential For hiar