

UNISOC NPI SimLock User Guide

Version: 3.0

Date: 2018-06-25

Unisoc Confidential

声明

本文件所含数据和信息都属于紫光展锐机密及紫光展锐财产，紫光展锐保留所有相关权利。当您接受这份文件时，即表示您同意此份文件内含机密信息，且同意在未获得紫光展锐同意前，不使用或复制、整个或部分文件。紫光展锐有权在未经事先通知的情况下，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，紫光展锐均不负责任何与文件相关的直接或间接的、任何伤害或损失。

前 言

文档说明

本文档主要介绍展讯平台 SimLock 方案工厂测试使用方法。

阅读对象

本文档适用于研发测试和产线测试技术人员。

内容介绍

本文档包括五个章节，分别为：

- 第一章：概述；
- 第二章：使用加密狗
- 第三章：使用 RSA Key
- 第四章：FAQ

文档约定

本文档采用下面醒目标志来表示在操作过程中应该特别注意的地方。



注意：

提醒操作中应注意的事项。



说明：

说明比较重要的事项。

目录

第 1 章 概述	- 6 -
1.1 概述	- 6 -
1.1.1 什么是 SimLock	- 6 -
1.1.2 名词解释	- 6 -
1.1.3 SimLock 类型	- 7 -
1.2 SimLock 产线流程介绍	- 8 -
1.2.1 准备流程	- 8 -
1.2.2 生产流程	- 8 -
1.2.3 工具版本推荐	- 9 -
第 2 章 使用加密狗	- 10 -
2.1 定制加密狗	- 10 -
2.2 加密狗生成或导入密钥	- 11 -
2.3 白名单加密	- 12 -
2.4 SimLock 服务端配置	- 13 -
2.5 配置 SecSIMLock.ini 文件	- 14 -
2.6 WriteIMEI 工具写 SIMlock	- 15 -
2.7 检查 SimLock 标志位及白名单	- 16 -
第 3 章 使用 RSA Key	- 17 -
3.1 RSAKeyGen 生成密钥	- 17 -
3.2 白名单加密	- 18 -
3.3 SimLock 服务端配置	- 19 -
3.4 配置 SecSIMLock.ini 文件	- 20 -
3.5 WriteIMEI 工具写 SIMlock	- 21 -
3.6 检查 SimLock 标志位及白名单	- 22 -
第 4 章 FAQ	- 23 -
4.1 写完 SimLock 后，是否可以修改 IMEI？	- 23 -
4.2 写 SimLock 常见问题有哪些？	- 23 -

4.3 如何添加多个 Project.....	- 23 -
附录 Revision History	- 24 -

Unisoc Confidential

第1章 概述

1.1 概述

1.1.1 什么是 SimLock

SIMLOCK, 可以简单理解为, 手机运营商通过 USIM 相关信息来限制用户手机 (或者其他可以使用 USIM 的终端设备) 使用的国家、注册的网络、子网等的一种软件锁, 该软件锁的实现遵循 3GPP 协议标准。

当开启 SIM LOCK 锁卡功能后, 在开机的过程中, 会去检验 SIM 卡的对应信息是否匹配 (如 MCC, MNC 等), 如果匹配则正常开机, 如果被锁则通过解锁码解锁后才能使用手机所有功能, 否则手机与 SIM 卡相关的通信业务不可用。

1.1.2 名词解释

RSA Key	由 RSA 算法生成的密钥对, 包含公钥 (Public Key)、私钥 (Private Key), 如果用其中一个密钥加密, 必须用另一个密钥解密
Public Key	公钥是密钥对中公开的部分, 一般用于加密、验证数字签名
Private Key	私钥则是非公开的部分, 一般用于解密、签名
加密狗	用来存储 RSA 密钥, 并提供了加密/解密、导入导出的接口
白名单	通过 xml 配置文件, 设定 SimLock 需要锁的类型, 通过加密生成二进制 bin 文件; 写 SimLock 时会把白名单信息写进 NV
PIN/PUK	PIN/PUK 解锁码

1.1.3 SimLock 类型

SimLock 有五种锁，通过 xml 文件来配置白名单，然后对 xml 文件进行加密生成二进制的 bin 文件，以防止恶意篡改白名单信息。产线写 SimLock 就是将白名单中的信息写到手机 NV 中，同时也会将 Public key 写入 Efuse，防止任意篡改白名单信息。

➤ NetWork Lock:

网络锁，通过锁定 MCC/MNC 限制手机只能用特定网络运营商的(U)SIMs

➤ NetWork subset Lock:

网络子集锁，通过锁定 MCC/MNC/network subset(IMSI 的第 6/7 位，代表运营商发行的某一类型卡)进一步限制网络锁

➤ SP Lock:

服务供应商锁，通过锁定 MCC/MNC/SP 来限制手机只能用于特定服务供应商的(U)SIMs

➤ Corporate Lock

集团业务锁，通过锁定 MCC/MNC/SP/Corporate 来限制手机只能用于集团用户内的(U)SIMs

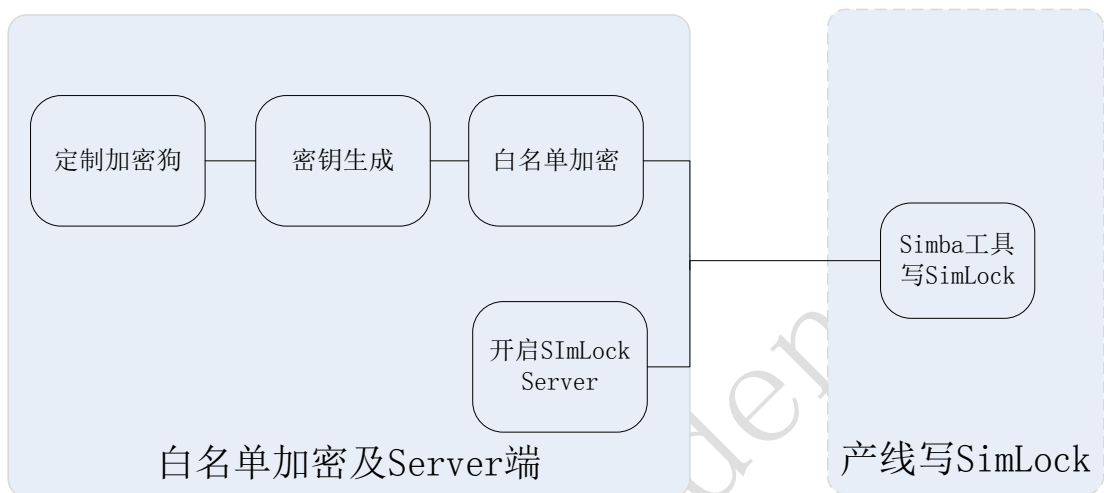
➤ User Lock

用户锁，通过锁定 imsi_len imsi_val[0]---[7]来限制手机只能用特定的(U)SIMs，即某张特定的卡

1.2 SimLock 产线流程介绍

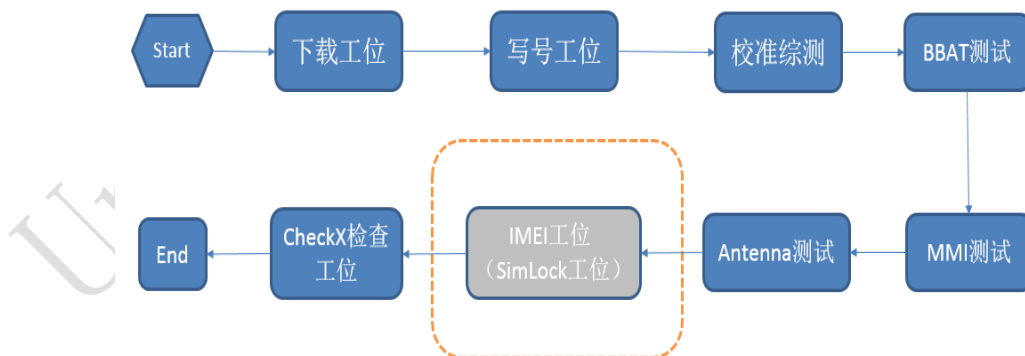
1.2.1 准备流程

产线准备流程如下图，后面章节将做详细的介绍。



1.2.2 生产流程

写 SimLock 与 IMEI 需要设置在同一站位，写完 SimLock 后 IMEI 不能随意更改。



1.2.3 工具版本推荐

WriteIMEI 工具支持写 SimLock 功能，推荐版本如下，如有新版本建议取新版本进行测试。

WriteIMEI_R21.0.0001 及以上版本

CSSimLock_Server_R4.0.0001 及以上版本

 说明：

CSSimLock_Server_R4.0.0001 同时支持 WriteIMEI 和 Simba 写 SimLock 的操作

第2章 使用加密狗

2.1 定制加密狗

加密狗型号：

SPRD SIMLOCK 方案建议使用型号为 Ucode 3000 的加密狗，如果需要使用加密狗写 SimLock，需要客户自己准备加密狗，由展讯进行二次开发。

加密狗定制：

展讯需要对加密狗 ROMCODE 做二次开发，将定制后的 ROMCode 烧写至加密狗。

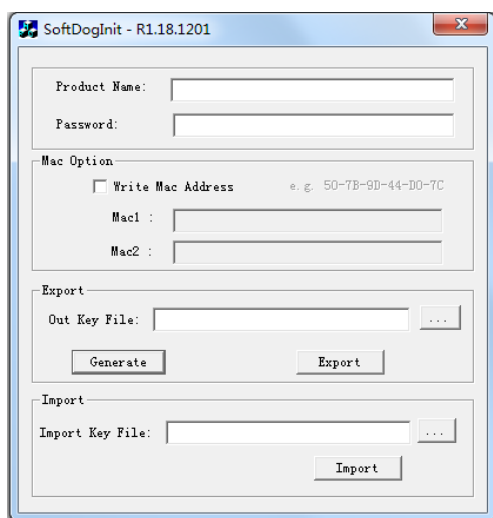
密钥对管理：

密钥对在整个 SimLock 生成过程中至关重要，客户需要对密钥对进行妥善管理，防止遗失泄漏。

2.2 加密狗生成或导入密钥

客户拿到定制的加密狗后，需要使用 SoftDogInit 工具进行初始化（即生成或导入 RSA 密钥到加密狗），每个加密狗只能使用 SoftDogInit 生成或导入一次密钥，如果需要重新生成或导入 RSA 密钥，需要重返回 SPRD 处理（重新烧写 ROMCode），见上一章节。

SoftDogInit: 加密狗初始化工具，用于密钥生成、备份、导入，见下图：



Product Name: RSA Key 的名称，最大为 16 个字节的字符

Password: 加密狗密码，最大为 16 个字节的字符

Out Key File: 密钥对导出到本地的路径，用于备份密钥（生成密钥对到加密狗的同时会默认保存到该路径下）

Generate: 生成密钥对文件，加密狗如果已经做过初始化或已导入密钥则不能生成

Export: 导出加密狗的密钥对文件，需要输入正确的 Product Name、PassWord 及路径

Import: 导入密钥对文件，加密狗如果已经做过初始化或已导入密钥则不能再次导入

Mac Option: 绑定电脑 Mac 地址，支持生成密钥时将加密狗与指定 Mac 地址绑定



注意：

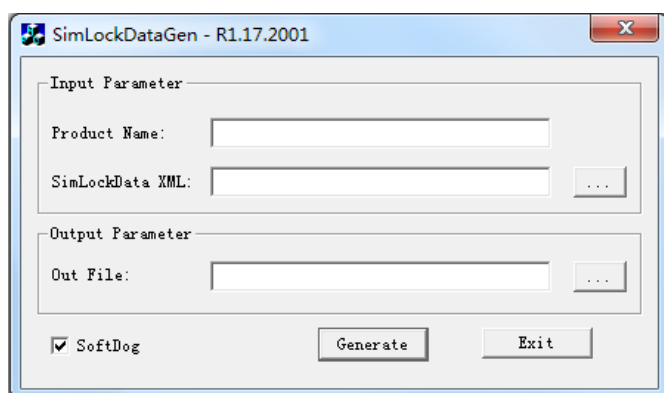
1. 每次生成的密钥对都是唯一的，即使输入相同的 Product Name，生成密钥也会不一样，为防止加密狗损坏，建议将生成的密钥对文件进行备份并妥善保管

2. 如要对已初始化的加密狗生成或导入密钥，请返回 SPRD 处理。

2.3 白名单加密

将配置好白名单的 xml 文件，使用 SimLockDataGen 工具将 xml 配置信息转换成二进制 bin 文件。

1. 将已有密钥的加密狗插上电脑，然后打开 SimLockDateGen 工具
2. 勾选 SoftDog，选择需要加密的 xml 文件进行加密，并指定生成 bin 文件的路径。



Product Name: 对应的 RSAKey 的名称

SimLockData XML: 需要加密的白名单 xml 文件的完整路径

Out File: 加密后 bin 文件生成路径

2.4 SimLock 服务端配置

1. 在 Server 端的电脑上插上加密狗
2. 启动 Server 前需要检配置文件 ServerCommMgr.ini:

```
SIMLockServerPort = 38888
```

```
//与客户端设置保持一致，默认不需修改
```

```
PIN/PUK_LENGTH = 8
```

```
//设置解锁码的长度
```

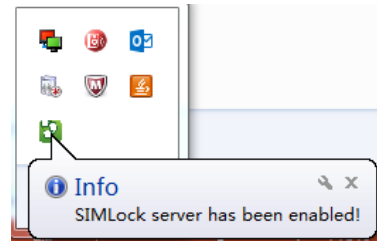
```
IsSoftDog = 1
```

```
//1:使用加密狗 0:不使用加密狗
```

```
RSA_KeyDB=
```

```
//当使用加密狗时不需要设置
```

3. 设置好 ServerCommMgr.ini 配置后，打开 server，查看 Server 当前状态栏，SIMLockServer 图标显示为绿色，表示开启，灰色表示关闭



注意:

1. 开启 Server 之前需确保电脑插上加密狗
2. 建议使用局域网，而且不要设置在产线生产工位上。

2.5 配置 SecSIMLock.ini 文件

打开 WriteIMEI 工具下的 SecSIMLock.ini 配置文件，设置 ServerIP、RSA Key 的名称、白名单文件路径、是否生成 PIN/PUK 解锁码文件等，各配置项说明如下：

```
ServerIP=127.0.0.1      //设置 SimLock Server 的 IP 地址

ServerPort=38888        //设置 SimLock Server 的端口号，一般默认不需要修改；

ProductName=admin       //RSA Key 的名称

SIMLockFile=\\xx.bin    //白名单加密后 bin 文件绝对路径，如 D:\\simlock.bin

Log=0                   //是否输出 log 文件；0：关闭，1：开启

RewritePublicKey=0      //是否支持重写 publicKey(写入 NV 中的部分)，0：不支持，1：支持

JobNumber=Test          //Server 端生成 Pin/Puk 解锁码文件的名，部署设置表示不生成文件

WriteIMEI=1             //写 SimLock 时加密处理 IMEI 并存入 NV 中
```

以下是 Reliance Subsidy Lock 相关设置，按需进行配置：


; Reliance Subsidy Lock set

WriteBlobPuk=0 //For Reliance Subsidy Lock: 0,关闭； 1： 开启支持

BlobPukFile= //For Reliance Subsidy Lock : 配置 Reliance Subsidy Lock csv 文件信息

例如，如果不写 Reliance Subsidy Lock，可配置该文件如下所示：

```
[9832A]
ServerIP=127.0.0.1
ServerPort=38888
ProductName=admin
SIMLockFile=D:\\CSSimLock\\Bin\\SimLockDataGen\\simlock.bin
Log=1
RewritePublicKey=1
JobNumber=9832A
WriteIMEI=1
```

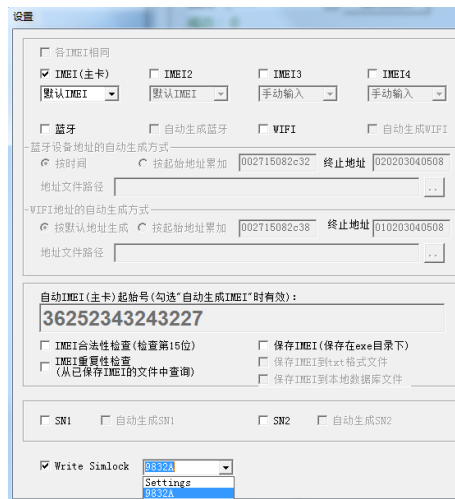
 注意：

1. SIMLockFile=\\xx.bin，需要配置白名单加密后 bin 文件的完整路径(包括文件名及后缀)
2. RewritePublicKey 功能：如果使用同一个 RSAKey 则允许重新写白名单及公钥信息，如果 RSAKey 不同则不允许重写。

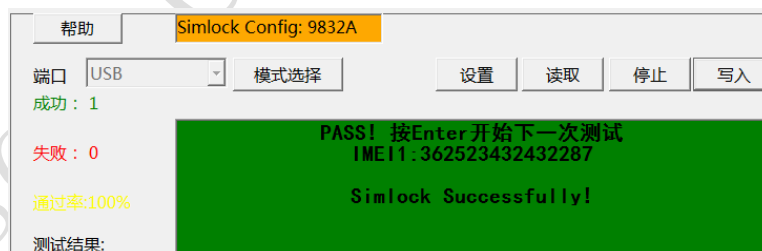
2.6 WritelMEI 工具写 Simlock

在写 SimLock 之前需开启 SimLock Server 并配置好 WritelMEI 工具下的 SecSIMLock.ini 文件（参照上一小节）。

1. 打开 WritelMEI 工具，勾选 IMEI1（写 SimLock 时必须勾选 IMEI1）、Write SimLock 勾选框，并选择对应的 Project，点击确定后，主界面上左上角会显示当前显示的 Project 信息。



2. 点击工具界面写入按钮，连接手机，进行写 SimLock 操作，写 Pass 后，界面如下图，左上黄色部分显示当前选择的 Project 信息：



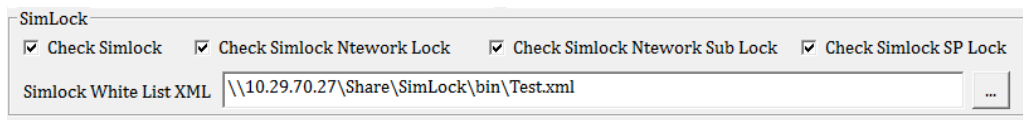
注意：

1. 写 SimLock 成功后，主卡 IMEI1 不能随意修改（如果支持多卡，修改 IMEI2 不影响 SimLock 功能）。
2. 如果需要重新写 IMEI1，需要设置 SecSIMLock.in 配置文件 RewritePublicKey=1，使用相同的 RSAKey（即相同的加密狗）重新进行 SimLock 操作

2.7 检查 SimLock 标志位及白名单

CheckX_R21.0.0001 工具支持 Simlock 标志位检查、以及白名单检查功能。

设置界面中勾选需要检查项，如果要检查白名单，还要指定白名单文件（非加密文件），如下图所示



支持以下工具检查：

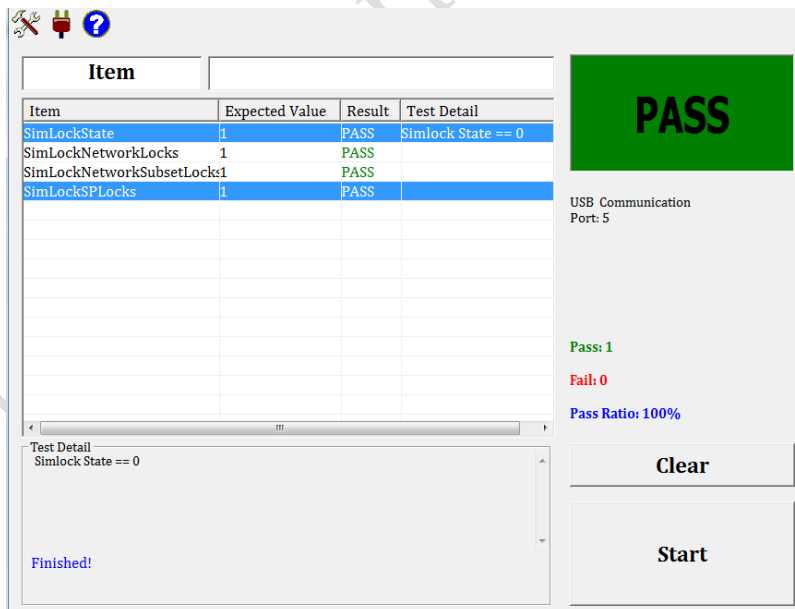
CheckSimlock：检查 SImLock 标志位，需要软件支持该命令

Check Simlock Network Lock：检查手机 NV 中写入网络锁白名单是否与 xml 配置文件中一致

Check Simlock Network Sub Lock：检查手机 NV 中写入网络子锁白名单是否与 xml 配置文件中一致

Check Simlock SP Lock：检查手机 NV 中写入服务供应商锁白名单是否与 xml 配置文件中一致

设置好后，工具主界面点击 Start 按钮，开始测试，测试 Pass 界面如下图所示：

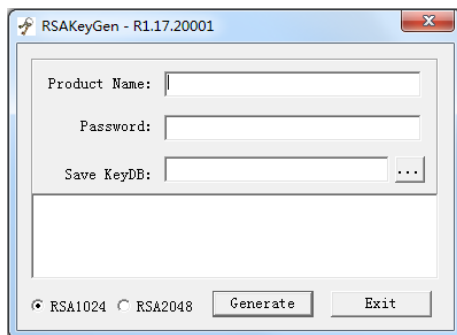


第3章 使用 RSA Key

3.1 RSAKeyGen 生成密钥

对于无加密狗方案，需要用 RSAKeyGen 工具生成密钥对，将生成的 RSA Key 密钥保存在可访问的位置使用。

打开 RSAKeyGen 工具，输入以下信息、指定生成 RSA Key 的路径，选择软件支持的加密方式如 RSA1024 或者 RSA2048，如下所示：



Product Name: RSA Key 的名称

Password: RSA Key 密码

Save KeyDB: 生成 RSA Key 的存储路径

RSA1024/RSA2048: 1024/2048 位的加密算法，不同软件支持的加密算法可能不同

👁 说明：

1. 不推荐使用该方式，推荐使用加密狗。
 2. 该方案需要选择软件匹配的加密算法
-

3.2 白名单加密

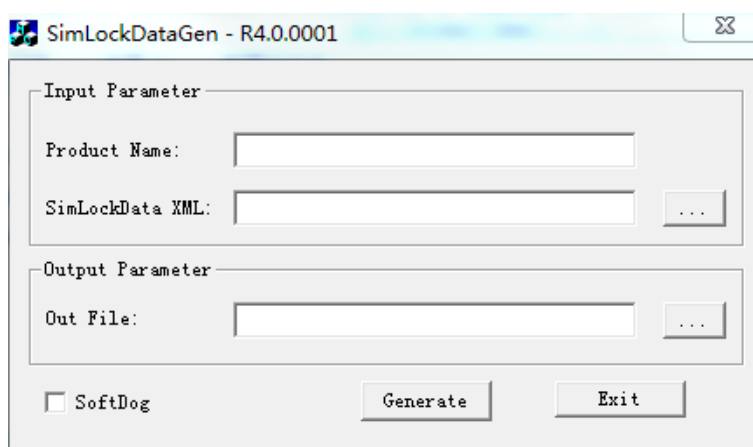
将配置好白名单的 xml 文件，使用 SimLockDataGen 工具将 xml 配置信息转换成二进制 bin 文件。

1. SimLockDataGen.ini 文件中需设置 RSAKey 的完整路径：

[Settings]

RSA_KeyDB==D:\SimLock 验证\key\2048key.db

2. 打开 SimLock DataGen 工具，不要勾选 SoftDog 选项，选择需要加密的 xml 文件。



Product Name: 对应的 RSAKey 的名称

SimLockData XML: 需要加密的白名单 xml 文件的完整路径

Out File: 加密后 bin 文件生成路径

3.3 SimLock 服务端配置

1. 启动 Server 前需要检配置文件 ServerCommMgr.ini:

```
SIMLockServerPort = 38888
```

```
//与客户端设置保持一致，默认不需要修改
```

```
PIN/PUK_LENGTH = 8
```

```
//设置解锁码的长度
```

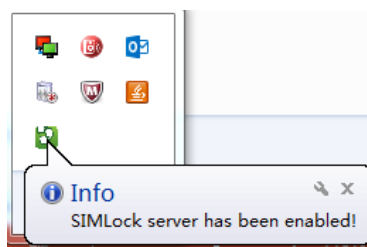
```
IsSoftDog = 0
```

```
//1:使用加密狗 0:不使用加密狗
```

```
RSA_KeyDB= RSAKey 文件完整路径
```

```
//如果不设置该路径，这需要将 RSAKey 命名为 key.db，放在该工具目录下
```

2. 设置好 ServerCommMgr.ini 配置后，打开 server，查看 Server 当前状态栏，SIMLockServer 图标显示为绿色，表示开启，灰色表示关闭



注意:

1. Server 端需要配置使用的 RSAKey 的完整路径
2. 建议使用局域网，而且不要设置在产线生产工位上。

3.4 配置 SecSIMLock.ini 文件

打开 WriteIMEI 工具下的 SecSIMLock.ini 配置文件，设置 ServerIP、RSA Key 的名称、白名单文件路径、是否生成 PIN/PUK 解锁码文件等，各配置项说明如下：

```
ServerIP=127.0.0.1      //设置 SimLock Server 的 IP 地址

ServerPort=38888        //设置 SimLock Server 的端口号，一般默认不需要修改；

ProductName=admin       //RSA Key 的名称

SIMLockFile=\\xx.bin    //白名单加密后 bin 文件绝对路径，如 D:\\simlock.bin

Log=0                  //是否输出 log 文件；0：关闭，1：开启

RewritePublicKey=0      //是否支持重写 publicKey(写入 NV 中的部分)，0：不支持，1：支持

JobNumber=Test         //Server 端生成 Pin/Puk 解锁码文件的名，部署设置表示不生成文件

WriteIMEI=1            //写 SimLock 时加密处理 IMEI 并存入 NV 中
```

以下是 Reliance Subsidy Lock 相关设置，按需进行配置：

; Reliance Subsidy Lock set

WriteBlobPuk=0 //For Reliance Subsidy Lock: 0,关闭； 1： 开启支持

BlobPukFile= //For Reliance Subsidy Lock : 配置 Reliance Subsidy Lock csv 文件信息

例如，如果不写 Reliance Subsidy Lock，可配置该文件如下所示：

```
[9832A]
ServerIP=127.0.0.1
ServerPort=38888
ProductName=admin
SIMLockFile=D:\\CSSimLock\\Bin\\SimLockDataGen\\simlock.bin
Log=1
RewritePublicKey=1
JobNumber=9832A
WriteIMEI=1
```



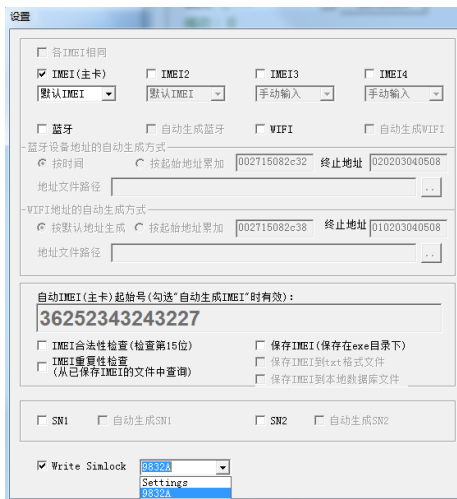
注意：

1. SIMLockFile=\\xx.bin，需要配置白名单加密后 bin 文件的完整路径(包括文件名及后缀)
2. RewritePublicKey 功能：如果使用同一个 RSAKey 则允许重新写白名单及公钥信息，如果 RSAKey 不同则不允许重写。

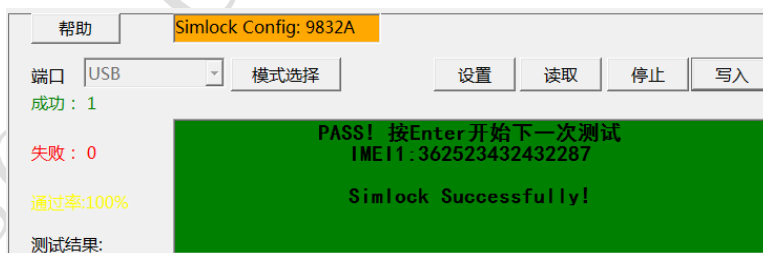
3.5 WritelMEI 工具写 Simlock

在写 SimLock 之前需开启 SimLock Server 并配置好 WritelMEI 工具下的 SecSIMLock.ini 文件（参照上一小节）。

3. 打开 WritelMEI 工具，勾选 IMEI1（写 SimLock 时必须勾选 IMEI1）、Write SimLock 勾选框，并选择对应的 Project，点击确定后，主界面上左上角会显示当前显示的 Project 信息。



4. 点击工具界面写入按钮，连接手机，进行写 SimLock 操作，写 Pass 后，界面如下图，左上黄色部分显示当前选择的 Project 信息：



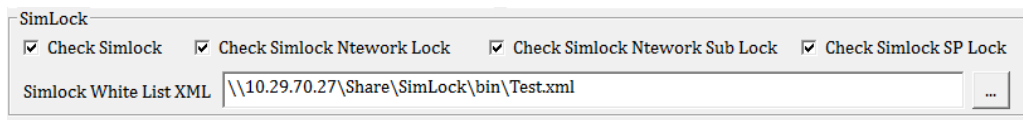
 注意：

1. 写 SimLock 成功后，主卡 IMEI1 不能随意修改(如果支持多卡，修改 IMEI2 不影响 SimLock 功能)。
2. 如果需要重新写 IMEI1，需要设置 SecSIMLock.in 配置文件 RewritePublicKey=1，使用相同的 RSAKey(即相同的加密狗)重新进行 SimLock 操作

3.6 检查 SimLock 标志位及白名单

CheckX_R21.0.0001 工具支持 Simlock 标志位检查、以及白名单检查功能。

设置界面中勾选需要检查项，如果要检查白名单，还要指定白名单文件（非加密文件），如下图所示



支持以下工具检查：

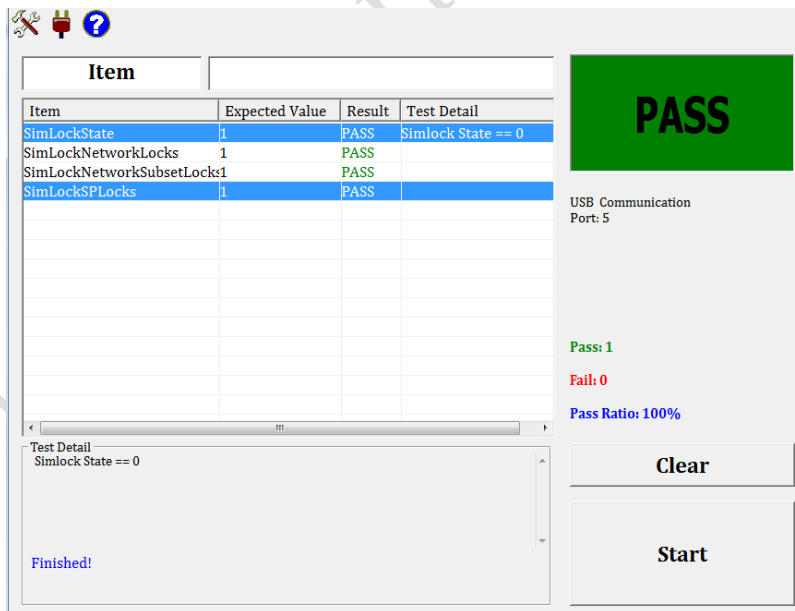
CheckSimlock：检查 SImLock 标志位，需要软件支持该命令

Check Simlock Network Lock：检查手机 NV 中写入网络锁白名单是否与 xml 配置文件中一致

Check Simlock Network Sub Lock：检查手机 NV 中写入网络子锁白名单是否与 xml 配置文件中一致

Check Simlock SP Lock：检查手机 NV 中写入服务供应商锁白名单是否与 xml 配置文件中一致

设置好后，工具主界面点击 Start 按钮，开始测试，测试 Pass 界面如下图所示：



第4章 FAQ

4.1 写完 SimLock 后，是否可以修改 IMEI1？

写完 SimLock 后，不能只修改 IMEI1，如果需要修改 IMEI1 必须重新使用相同的 RSA Key 重写 SimLock。因此一般把写 IMEI 与 SimLock 放在同一站位。

4.2 写 SimLock 常见问题有哪些？

1. 工具版本与 Server 版本不匹配，建议使用指定的版本。
2. Server 开启异常：检查加密狗是否正常、Server 配置是否正确
3. 写 SimLock 是连接 Server 失败：检查工具配置的 Server IP、Server Port、KeyName 配置是否正确，其中 KeyName 必须与加密狗或使用的 RSAKey 的 ProductName 一致（见 [2.2](#) 节）

4.3 如何添加多个 Project

可以在 SecSIMLock.ini 文件中添加多个 Project

不要将 Settings 当作一个 Project，而应在 Settings 下面添加各个 Project，与 Setting 的结构保持一致，如在 Settings 下面添加 Project 7731：

```
[7731]
ServerIP=127.0.0.1
ServerPort=38888
ProductName=ad
SIMLockFile=xx\xx.bin
Log=0
RewritePublicKey=1
```

附录 Revision History

Version	Date	Owner	Notes
1.0	2017/08/12	HWE-NPI	Created
2.0	2018/04/01	HWE-NPI	Updated
3.0	2018/06/25	HWE-NPI	Updated