
UNISOC NPI Security User Guide

Version: 3.0

Date: 2018-06-20



www.unisoc.com

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

本文档主要针对展锐平台安全部署使用方法的指导说明。

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

本文档包括七个章节，分别为：

- 第一章：概述
- 第二章：SecurityServer 配置说明
- 第三章：ROTPK 部署
- 第四章：Attestation Keybox 部署
- 第五章：IFAA 部署
- 第六章：SOTER 部署
- 第七章：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	- 4 -
1.1 运行环境	- 5 -
1.1.1 硬件要求	- 5 -
1.1.2 软件要求	- 5 -
1.1.3 工具版本推荐	- 5 -
1.2 测试环境	- 6 -
1.2.1 安全部署前提条件	- 6 -
1.2.2 产线安全部署流程	- 6 -
1.2.3 产线安全部署 C/S 架构	- 7 -
第 2 章 SecurityServer 配置说明	- 8 -
2.1 SecureOperations.ini	- 8 -
2.2 SecureCenter.ini	- 9 -
2.3 运行 SecurityServer	- 10 -
第 3 章 ROTPK 部署	- 11 -
3.1 配置 SecurityServer	- 11 -
3.2 产线部署 ROTPK	- 12 -
3.3 检查 SecureBoot 标志位	- 13 -
第 4 章 Attestation KeyBox 部署	- 14 -
4.1 对 Keybox 中 DeviceID 要求	- 15 -
4.2 SecureToolBox 转换 Keybox 源文件	- 16 -
4.3 SecureToolBox 分割 Keybox db 文件	- 17 -
4.4 Attestation KeyBox 配置 SecurityServer	- 18 -
4.5 产线部署 Attestation KeyBox	- 19 -
4.6 检查 Attestation KeyBox 标志位	- 20 -
第 5 章 IFAA 部署	- 21 -
5.1 接入 IFAA 平台	- 21 -

5.2 IFAA 部署配置 SecurityServer.....	- 22 -
5.3 产线部署 IFAA	- 23 -
5.4 检查 IFAA 标志位及 Key Hash	- 24 -
第 6 章 SOTER 部署	- 25 -
6.1 MySQL 数据库的使用	- 26 -
6.1.1 安装 MySQL 数据库	- 26 -
6.1.2 导入 SQL 表文件	- 27 -
6.2 SecurityServer 与 MySQL 建立连接	- 29 -
6.3 SOTER 部署配置 SecurityServer.....	- 29 -
6.4 产线部署 SOTER.....	- 30 -
6.5 上传注册设备信息至微信服务器	- 31 -
6.6 检查 SOTER 标志位.....	- 32 -
第 7 章 FAQ.....	- 33 -
7.1 安装 MySQL 的常见问题	- 33 -
7.2 芯片未写 HUK，进行安全部署会有什么问题？	- 33 -
7.3 芯片 Secure Bit 未置位，进行安全部署会有什么问题？	- 33 -
7.4 安全部署是否可以重复部署？	- 34 -
7.5 IFAA/SOTER/Keybox 写在那里，是否可以重复写入？	- 34 -
7.6 维修更换 EMMC/BB 芯片，是否需要重新部署？	- 34 -
7.7 更换指纹模组是否需要重新进行部署	- 35 -
7.8 重新下载是否需要重新进行部署	- 35 -
7.9 常见 Error Code	- 35 -
7.10 Keybox db 文件新旧版本转换.....	- 36 -
7.11 安全部署各 Command ID 对应的操作.....	- 37 -
附录 Revision History	- 38 -

第1章 概述

TEE(Trusted Execution Environment)是存在于智能手机、平板电脑或任意移动设备主处理器中的一个安全区域，确保各种敏感数据在一个可信的环境中被存储、处理和受保护，是与设备上的 Rich OS（通常是 Android 等）并存的运行环境，并且给 Rich OS 提供安全服务。

TEE 为授权安全软件(也称为“可信应用”)提供一个安全的执行环境，通过实施保护、保密性、完整性和数据访问权限确保端到端的安全。

支持 TEE 功能产品在产线需要做安全部署，产线进行安全部署时，首先会根据硬件的 HUK(Hardware Unique Key)绑定并初始化 EMMC 的 RPMB 分区，用于提供安全存储；然后根据需求将 ROTPK、IFAA Key、SOTER Key 或者 Keybox 写入该 RPMB 分区，用来提供安全服务。

展锐 TEE 方案目前可支持写 ROTPK、IFAA Key、SOTER Key 以及 Attestation Keybox 等功能，各项功能相对独立，可以分不同站位部署，也可以在同一站位进行部署。

本文档主要介绍展锐 TEE 方案，适用于 SC9850KH 等平台。

SecurityServer 配置，参照[第2章](#)；

产线 ROTPK 部署，参照[第3章](#)；

产线 Attestation Keybox 部署，参照[第4章](#)；

产线 IFAA 部署，参照[第5章](#)；

产线 SOTER 部署，参照[第6章](#)；

1.1 运行环境

1.1.1 硬件要求

硬件	基本要求
PC	CPU: i5 及以上 内存: 4G 及以上
连接线	USB
电源	需提供稳定电压输出: 使用精密电源或普通直流电源加展锐稳压板

1.1.2 软件要求

软件	版本要求
操作系统	Win7、Win10
SPRD USB 驱动	版本 2.0.0.131
MySQL（按需选择）	5.6.24.0 及以上版本
FrameWork	.Net FrameWork 4.0

1.1.3 工具版本推荐

建议使用以下版本，如有新发布工具版本请取最新版本进行部署：

Client: WriteIMEL_R21.0.0001

SecurityServer: SecurityServer_R5.0.0001

1.2 测试环境

1.2.1 安全部署前提条件

➤ 芯片要求:

确保芯片在出货前就要完成写 HUK，否则会影响进行安全部署。

ATE 阶段 Enable Secure Bit

ATE 阶段写入 Secure Efuse 的 HUK (HardWare Unique Key)

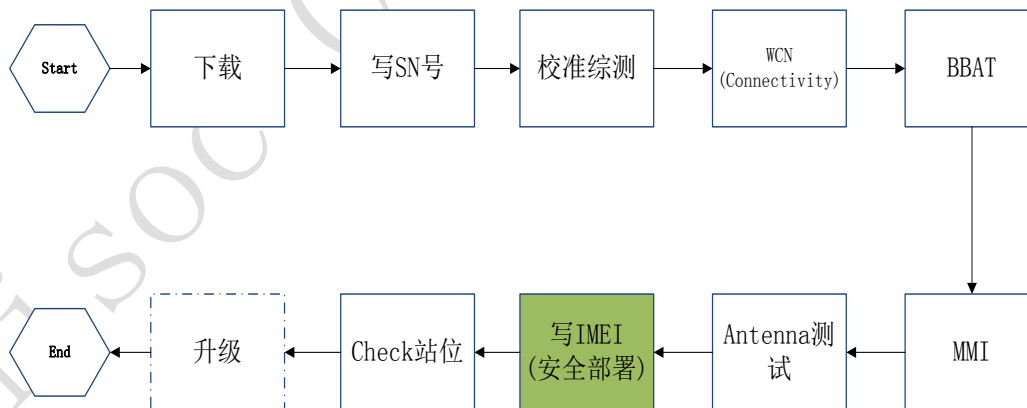
Block2: bonding Field			SharkL2
BIT	Value	Description	
BIT0		0 disable secure boot	Yes
		1 enable secure boot	Yes

➤ 软件版本:

软件需要做相应签名，支持产线安全部署功能。

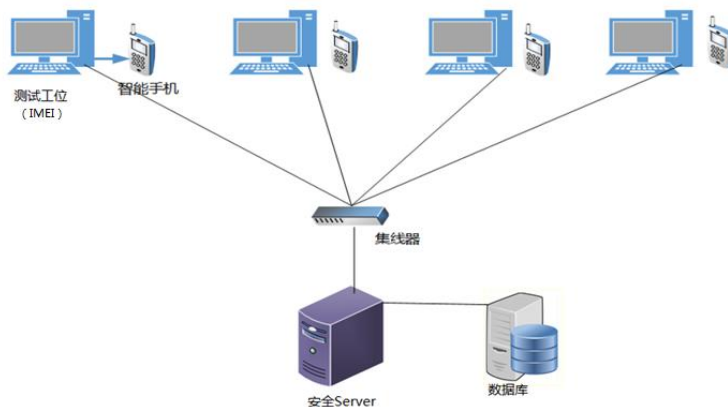
1.2.2 产线安全部署流程

产线安全部署是在写 IMEI 的站位进行的，如下图所示:



1.2.3 产线安全部署 C/S 架构

安全部署采用 C/S 架构，支持一台 Server 部署多台客户端；产线架构如下图所示：



- Security Server:

整个安全部署生产流程的发起方及管理方。

- 产线 Client 工具:

Simba 和 WriteIMEI 工具都支持安全部署，本文档主要介绍 WriteIMEI 工具。安全部署过程中，产线 Client 工具作用是透传 Security Server 的数据，是 Security Server 与手机通信“桥梁”。

- 数据库（仅部署 SOTER 时需要）:

存储 SOTER 部署时生成的 Key，并上传到微信服务器。

👁 说明:

1. 除 SOTER 部署仍需要依赖 MySQL 数据库外，其他如 SeureBoot/IFAA/Keybox 不再依赖 MySQL 数据库，很大程度上简化了产线部署流程。
 2. 在进行试产或者验证时，产线 Client 工具、Security Server 以及数据库可以使用同一台 PC；在进行量产时建议 Server 和 Client 分开在不同 PC 上。
-

第2章 SecurityServer 配置说明

SecurityServer 是安全部署流程的发起和管理方。通过配置 SecureOperations.ini 和 SecureCenter.ini 两个配置文件来配置安全 Server。

在 SecureOperations.ini 配置文件中设置安全部署执行的操作，在 SecureCenter.ini 配置文件中配置 IFAA/Keybox 等部署时需写入到设备的 key 文件路径、以及 SOTER 部署时需要使用的 MySQL 数据库。

2.1 SecureOperations.ini

通过 SecurityServer 的 SecureOperations.ini 的配置文件，设置安全部署需要执行的步骤。每次修改配置文件都需要重启 Server，目前支持选项如下：

```
;now support operations:
;   GetUID           //获取手机 UID 信息;
;   SystemInit       /*必选项：初始化 CA;
;   SetRTC           //RTC 信息写到 RPMB 分区;
;   SetROTPK         //写 ROTPK 到 Efuse;
;   GetROTPK         //获取 ROTPK 的信息;
;   GetDeviceID      //获取设备 DeviceID
;   SetKeybox        //Attestation keybox：写入 Keybox 到 RPMB 分区;
;   SetIfaaKey       //IFAA：写入指定 IFAA Key 到 RPMB 分区;
;   GetSoterATTK     //SOTER：生成密钥对，写入手机，并上传公钥到数据库;
;   SystemClose      /*必选项：关闭 CA;
;   DeployEnd        /*必选项：部署结束，将 Sever 与客户端断开连接;
```

在 SecureOperations.ini 配置文件添加多个 Project，格式如下所示：

```
[Example]
1=GetUID
2=SystemInit
3=SystemClose
4=DeployEnd
```

2.2 SecureCenter.ini

如果需要进行 IFAA/Keybox/Soter 部署，则还需要配置 SecurityServer 配置文件 SecureCenter.ini。

//端口配置，一般不需要修改

[Settings]

Project=SharkL2

Port=39998

TimeOut=60000

BigEndian=1

//设置 Keybox db 文件路径，注意设置时要删除前面注释的分号

[KeyBox]

;please configure the attestation keybox database files path;

;KeyBoxPath=D:\WorkSpace\attestation_Keybox.db

//设置 IFAA Key Pair 文件路径设置，注意设置是要删除前面注释的分号

[IFAA]

;please configure the ifaa rsa file

;Key=D:\pukpri.pem

//设置连接 MySQL 数据库，仅做 SOTER 部署时需要配置该项

[DataBase]

IP=127.0.0.1 //MySQL 的 IP

Port = 3306 //MySQL 的 Port Num，默认不需要修改

UserName=root //MySQL 用户登录名

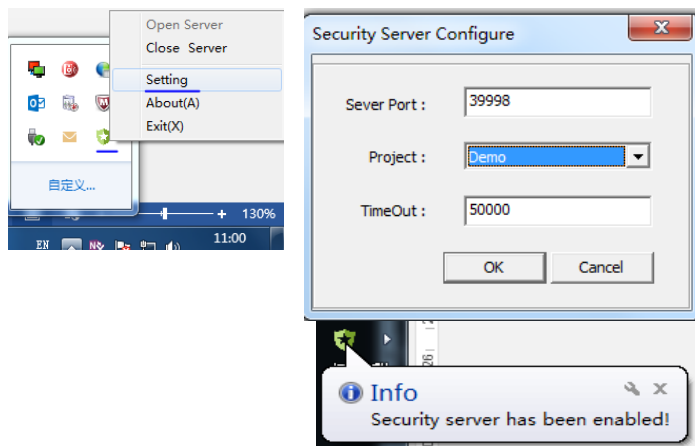
PassWord=12345678 //MySQL 用户登录密码

DataBase=itrust //MySQL 数据库名

2.3 运行 SecurityServer

如果正确配置了 SecurityServer，双击 SecurityServer.exe 则会在后台运行 SecurityServer。
右键/双击 SecurityServer 图标

选择 Setting 项进入设置界面，选择对应的 Project，如下图所示：



选择 About 项进入版本信息界面，可查看当前版本号，如下图所示，在该页面右击鼠标可直达 SecurityServer.exe 所在文件夹。



 说明：

修改配置文件，需要重启 Server 方能生效

第3章 ROTPK 部署

ROTPK 全称 Root of Trust Public Key Hash，是根据硬件的 ID 来生成的一组 KeyHash 值。产线部署 ROTPK，会将该 KeyHash 写入到 Efuse 中，即旧平台的 SecureBoot 功能。与旧的 SecureBoot 方案直接写 Efuse 不同的是：安全部署写 ROTPK 是在 TEE 环境中去完成写 Efuse，更加安全且易于拓展，后续平台项目都将采用该种方式。

3.1 配置 SecurityServer

在 SecurityServer 的 SecureOperations.ini 文件中配置安全部署需要执行的操作，可参考如下配置：

```
[ROTPK]
1=GetUID
2=SystemInit
3=SetROTPK
4=SystemClose
5=DeployEnd
```



说明：

1. GetUID/SystemInit 是安全部署开始必须执行的两个步骤
2. DeployEnd 部署的最后一步，部署结束，Server 与客户端端口连接。

3.2 产线部署 ROTPK

按照上一节介绍方法配置好 SecuritySever，开启 SecuritySever 并选项相应的 Project。

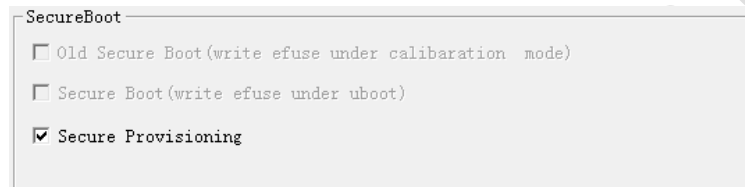
1. 配置 Client 与 SecurityServer 的连接：打开 WriteIMEI.ini 配置文件，配置 Server 端的 IP

[SECURE DEPLOYMENT]

Server IP=127.0.0.1 //设置 SecurityServer IP 地址

Server Port=39998 //设置 SecurityServer Port 口，默认不需要修改

2. 打开 WriteIMEI 工具，设置界面勾选安全部署测项，如下所示：



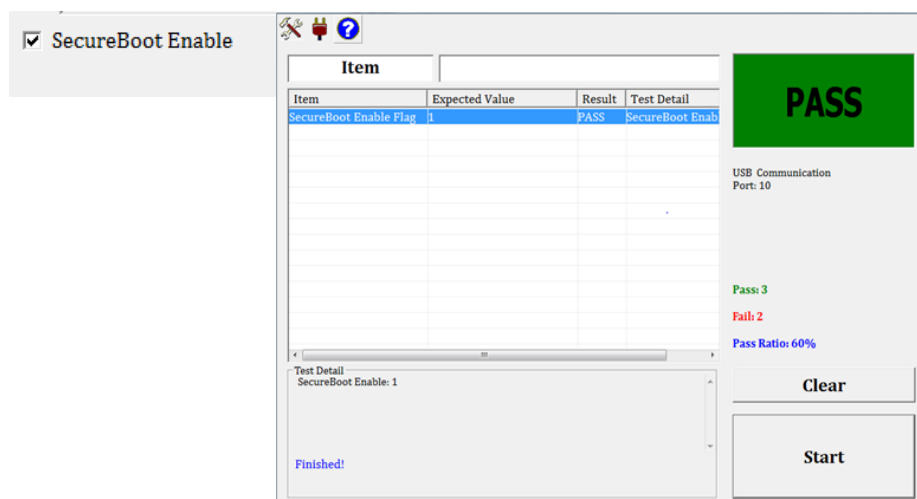
3. 产线部署：点击工具“写入”按钮，进行测试，测试成功界面如下图所示：



3.3 检查 SecureBoot 标志位

部署结束后使用 CheckX 工具检查 SecureBoot 标志位是否 Pass:

进入工具设置界面，勾选 SecureBoot Enable 选项，然后进行测试。



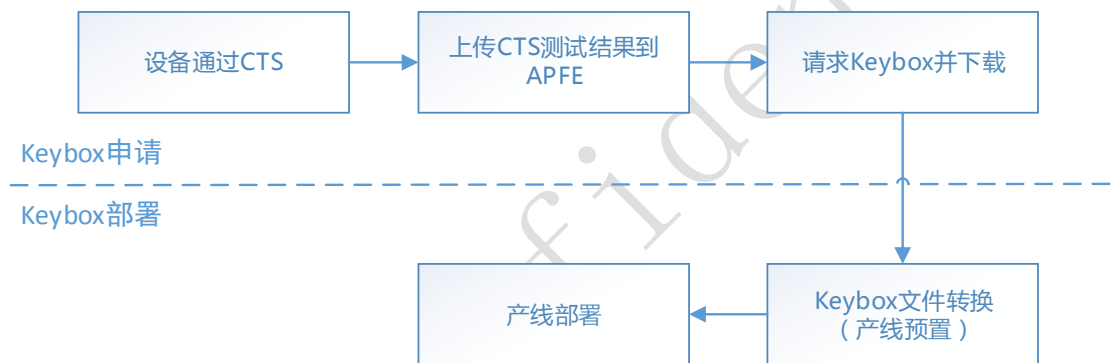
 说明:

步骤 SetROTPK 会写 Efuse，只有安全部署流程中设置了该步骤且部署 Pass，使用 CheckX 工具检查 Secure Boot Enable 标志位才会 Pass

第4章 Attestation KeyBox 部署

Attestation key 在 Android7.0(Nougat)被添加，Android8.0(Oreo)开始强制。所有的 Android 8.0 (Oreo)后续的全部设备都需要添加，并且必须拥有硬件支持的 Keystore。包括 Android 8.1 (Go Edition)所有有 GMS 认证设备都需要，目前 GTS 也已经强制测试。

Attestation Key 在产线部署前需要使用 DeviceID 从 Google APFE 申请 Keybox，并在生产线将申请到的 keybox 文件部署到每一台终端，流程如下：



 说明：

1. 每个 DeviceID 对应唯一硬件设备，通过 DeviceID 来申请 Keybox 确保 Keybox 的唯一性。
2. 一般可将 SN 作为 DeviceID 来申请 Keybox，因为 SN 也是对应着唯一的硬件设备；
3. 用 SN 作为 DeviceID 申请 Keybox，并不意味着 DeviceID 与 SN 绑定，在产线部署时只要保证每个硬件写入一个唯一的 Keybox 就可以。

4.1 对 Keybox 中 DeviceID 要求

用于申请 Keybox 的 DeviceID 必须包含软件预设的关键字。

展锐 Attestation Keybox 部署方案会检查当前写 keybox 文件中的 DeviceID 是否与预设值匹配，避免产线将其他项目申请的 Keybox 误写到当前项目中。

在正式介绍 Attestation Keybox 部署之前，有必要先介绍下是如何实现 Attestation Keybox 的防呆功能。

1. 软件预设 ro.keybox.id.value，即需要匹配的关键字，以 7731E 项目为例：在编译 pac 时，在 device/sprd/pike2/sp7731e_1h10/sp7731e_1h10_native.mk 文件中添加以下配置，配置需要检索的字段：

```
#add for keybox prop value
```

```
PRODUCT_PROPERTY_OVERRIDES += \
```

```
ro.keybox.id.value=SPRD_SC9850K
```

2. 写入前检查 Keybox 中 DeviceID 是否包含预设关键字：从 Google 申请到的 Keybox 文件中的 DeviceID 字段必须包含 ro.keybox.id.value 字段方可校验通过，如下图所示：

```
<?xml version="1.0"?>
<AndroidAttestation>
<NumberOfKeyboxes>120000</NumberOfKeyboxes>
<Keybox DeviceID="SPRD SC9850K 0000001"><Key algorithm="ecdsa"><PrivateKey format="pem">-
MHcCAQEIEU18FyuBBIG9jJz/9irB3UntoI8sBFN64LivnIUf7q/oAoGCCqGSM49
AwEHoUQDQgAE+XaqJBaimJnrBMZ5LeGnayaQJormVaOhvygbG1Ik2q60mEkABwj0
vnm5dVnQj2KCSQRPN2QTh28vxARsNF4RXg==
-----END EC PRIVATE KEY-----
```

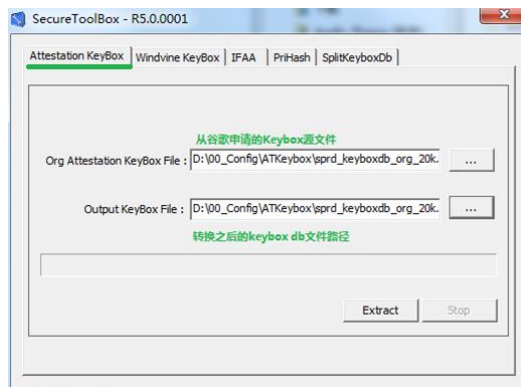
 说明：

1. ro.keybox.id.value 大小写敏感，为 keybox 文件中 DeviceID 字段中固定不变子串
2. 展锐方案默认是在 device/sprd/****/common/security_feature.mk 文件里面配置这个属性的，针对所有 board 都生效，客户在配置 keybox 属性的时候，需要在各自的 board 里面合理配置该属性，修改 security_feature.mk 中的 ro.keybox.id.value=SPRD_SC9850K 属性配置。

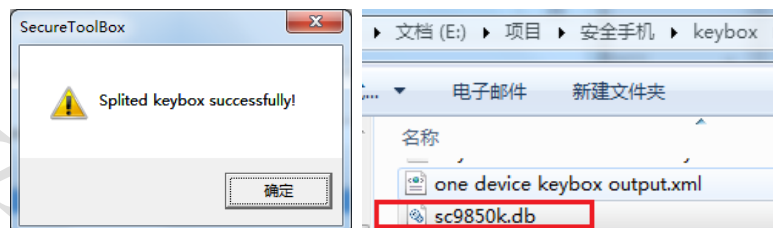
4.2 SecureToolBox 转换 Keybox 源文件

从 Google APFE 申请到 Keybox 源文件后，在生产前需要通过展锐专用转换工具将从 Google 申请到 Keybox 源文件转换成适合部署的.db 文件，即 SecurityServer 目录 \Bin\ToolBox\下的 SecureToolBox.exe 工具。

打开 SecureToolBox.exe 工具，在 Attestation Keybox 页面，选择 keybox 源文件和目标文件路径，点击 Extract，将 Keybox 源文件转换成适合产线部署使用的 db 文件，如下图所示：



转换成功后，工具提示 Splited keybox successfully，并在目标路径下会生成目标 db 文件，如下图所示。



 注意：

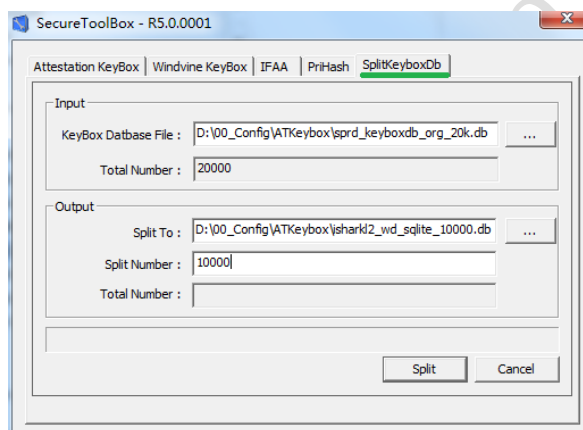
1. Attestation KeyBox 必须在[Attestation Keybox]页面进行转换
2. 若 Keybox 源文件较大，可能需要花费一定时间，请耐心等待
3. R5.0.0001 版本工具与之前的 R4.18.2101 不兼容，处理方法详见 FAQ

4.3 SecureToolBox 分割 Keybox db 文件

一般地，从谷歌申请到的 Keybox 源文件包含 keybox 的数量比较多，可能实际生产并不需要把所有的 keybox 都保存到同一个 db 文件中。

SecureToolBox.exe 工具另外还提供了一个比较实用的功能：分割 Keybox db 文件的功能，支持从一个比较大的 Keybox db 文件中分割出指定数量的 keybox 到另一个 db 文件中。

打开 SecureToolBox 工具，切换到 SplitKeyboxDb 页面，选择需要分割的 Keybox db 文件和输出文件，如下图所示：



keyBoxDatabase File: 选择需要分割的 db 文件（不能直接指定为 keybox 源文件）

Split To: 指定分割出 keybox 存储的 db 文件

Split Number: 指定分割的数量

Total Number: 显示当前 db 文件中 keybox 的数量。

4.4 Attestation KeyBox 配置 SecurityServer

将从谷歌申请的 keybox 源文件转换成适合产线部署的 db 文件后，在配置文件 SecureCenter.ini 中指定该 keybox db 文件的路径、在配置文件 SecureOperations.ini 中添加 Keybox 的步骤，如下所示：

1. 配置 Keybox db 文件路径：在 SecureCenter.ini 配置文件 KeyBox 文件的路径，如下所示：

```
[KeyBox]
;please configure the keybox files path;
KeyBoxPath=D:\KexBox //注意：前面不能有分号
```

2. 添加 keybox 部署操作：SecureOperations.ini 中对应的项目添加 SetKeyBox 步骤，可参考如下配置：

```
[AT Keybox]
1=GetUID
2=SystemInit
3=GetDeviceID
4=SetKeyBox
5=SystemClose
6=DeployEnd
```

说明：

1. KeyBox 是写到 EMMC 的 RPMB 分区，在写 Keybox Key 之前需要先初始化 RPMB 分区，这一步是在 SystemInit 进行的，所以 SetKeyBox 必须在 SystemInit 之后。
 2. 根据谷歌的要求，一个硬件对应一个 Keybox，故 Keybox 写成功后，会将已写过的 Keybox 从当前 db 文件中删除。另外根据谷歌要求，Keybox 只能写一次，不能重新。
-

4.5 产线部署 Attestation KeyBox

按照上一节介绍方法配置好 SecuritySever，开启 SecuritySever 并选项相应的 Project。

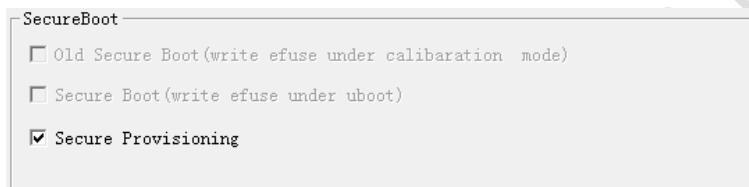
1. 配置 Client 与 SecurityServer 的连接：打开 WriteIMEI.ini 配置文件，配置 Server 端的 IP

[SECURE DEPLOYMENT]

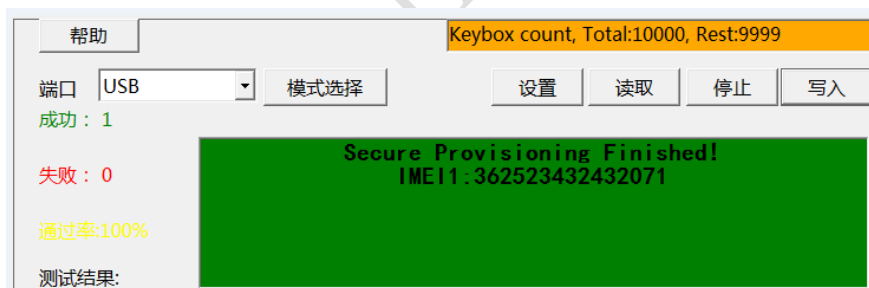
Server IP=127.0.0.1 //设置 SecurityServer IP 地址

Server Port=39998 //设置 SecurityServer Port 口，默认不需要修改

2. 打开 WriteIMEI 工具，设置界面勾选安全部署测项，如下所示：



3. 产线部署：点击工具“写入”按钮，进行测试，测试成功界面如下图所示：



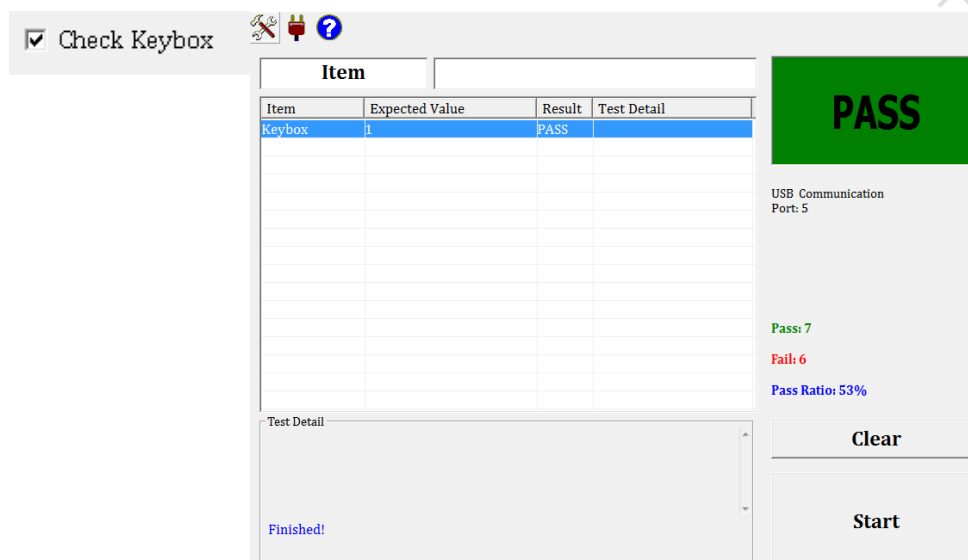
说明：

Keybox 部署 Pass 后，WriteIMEI 工具的右上角会显示 Keybox 总数量及剩余可用数量

4.6 检查 Attestation KeyBox 标志位

部署结束后使用 CheckX 工具检查 Attestation KeyBox 标志位是否 Pass:

进入工具设置界面，勾选 **Check Keybox** 选项，然后进行测试。



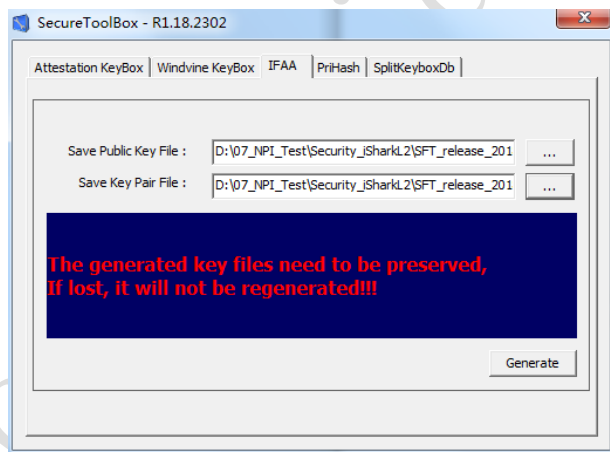
第5章 IFAA 部署

互联网金融身份认证联盟(IFAA)、是阿里主导的一种移动支付身份认证方式，基于公钥校验体系，能够强有力的防范恶意攻击行为。如果需要接入 IFAA 平台，则需要进行 IFAA 认证及产线部署。

5.1 接入 IFAA 平台

访问 IFAA 官网：<http://ifaa.org.cn>/获取加入 IFAA 的流程说明，也可参阅相《IFAA 终端厂商接入流程.docx》。

首先使用 SecurityServer 中 ToolBox 目录下的 SecureToolBox.exe 工具生成设备密钥，如下图所示：



然后将 Public Key 上传至 IFAA 服务器 <http://ifaa.org.cn/>。

说明：

1. SecureToolBox 生成的 IFAA Public Key 上传至 IFAA 服务器、IFAA Key Pair 用于产线部署；
2. SecureToolBox 每次生成的密钥对文件都不相同，生成的公钥及密钥对文件需要妥善保管。
3. IFAA 采用一型一密，相同型号的产品只需要生成一次密钥对文件就可以了。

5.2 IFAA 部署配置 SecurityServer

产线 IFAA 部署时将指定的 IFAA Key Pair 文件写入到手机的 RPMB 分区，在 Server 的 SecureCenter.ini 配置文件中指定 IFAA Key Pair 的文件路径，并在 SecureOperations.ini 配置文件中添加相应步骤。

1. 设置 IFAA Key Pair 文件的路径：

在 SecurityServer 的配置文件 SecureCenter.ini 中添加密钥对文件的路径（需要指定完整文件名及后缀），如下：

```
[IFAA]
```

```
;please configure the ifaa rsa file
```

```
Key=D:\keypair\Demo\IFAA_Key_Pair.pem //注意：前面不能有分号
```



说明：

IFAA Key Pair 即由 SecureToolBox 工具生成的 IFAA Key Pair 文件

2. 添加 SetIFAAKey 步骤：在 SecurityServer 配置文件文件 SecureOperations.ini 中添加 SetIfaaKey，可参考如下配置：

```
[IFAA]
```

```
1=GetUID
```

```
2=SystemInit
```

```
3=SetIfaaKey
```

```
4=SystemClose
```

```
5=DeployEnd
```



说明：

IFAA Key 是写到 EMMC 的 RPMB 分区，在写 IFAA Key 之前需要先初始化 RPMB 分区，这一步是在 SystemInit 进行的，所以 SetIfaaKey 必须在 SystemInit 之后。

5.3 产线部署 IFAA

按照上一节介绍方法配置好 SecuritySever，开启 SecuritySever 并选项相应的 Project。

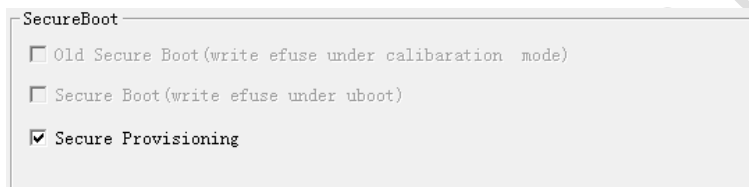
1. 配置 Client 与 SecurityServer 的连接：打开 WriteIMEI.ini 配置文件，配置 Server 端的 IP

[SECURE DEPLOYMENT]

Server IP=127.0.0.1 //设置 SecurityServer IP 地址

Server Port=39998 //设置 SecurityServer Port 口，默认不需要修改

2. 打开 WriteIMEI 工具，设置界面勾选安全部署测项，如下所示：



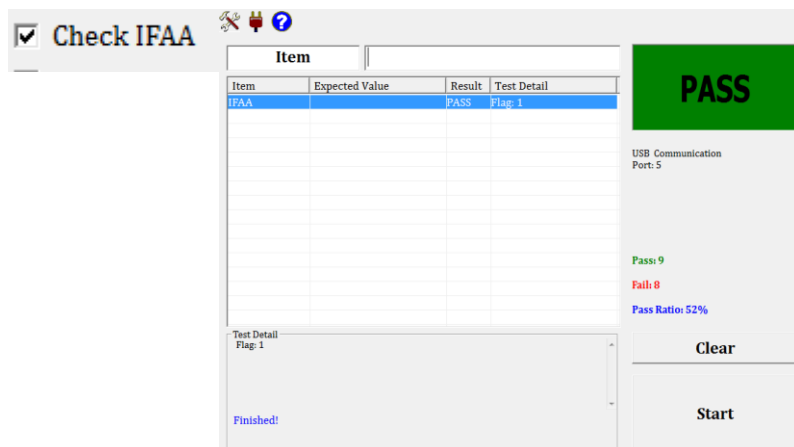
3. 产线部署：点击工具“写入”按钮，进行测试，测试成功界面如下图所示：



5.4 检查 IFAA 标志位及 Key Hash

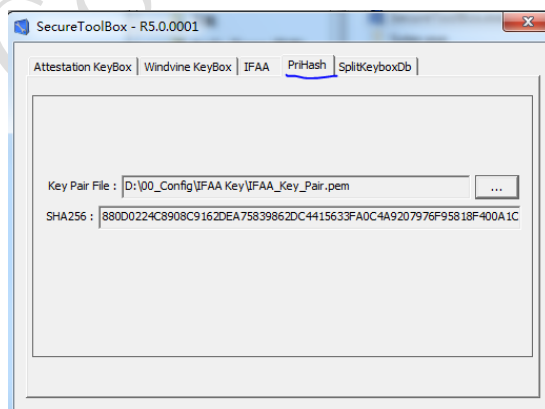
部署结束后使用 CheckX 工具检查 Attestation KeyBox 标志位是否 Pass:

进入工具设置界面，勾选 Check IFAA 选项，然后进行测试。



另外还支持检查 IFAA Key 的 Hash 值是否正确:

1. 使用 SecurityServer 中\Bin\ToolBox\SecureToolBox.exe 工具可读取 IFAA Key 的 Hash 值: 切换到 PriHash 页面，导入密钥文件计算获得，如下图所示:



2. 在 CheckX 工具的配置文件 CheckX.ini 中设置上一步查询出的 IFAA Key Hash 信息:

IFAA Key=880D0224C8908C9162DEA75839862DC4415633FA0C4A9207976F95818F400A1C

然后打开 CheckX 工具，进入工具设置界面，勾选 Check IFAA 选项进行测试，会在检查标志位的同时检查写入到手机中的 IFAA Key Hash 信息与设置的是否一致。

第6章 SOTER 部署

SOTER，即腾讯生物认证平台，如需接入 SOTER 平台进行 TENcent SOTER 认证，则需要进行 SOTER 产线部署。先访问 SOTER 合作官网：wecooper.weixin.qq.com，按平台指引注册账号。关于 SOTER 开发及接入详细流程请参阅《SOTER 开发接入流程.docx》及《SOTER 终端厂商接入流程.docx》

产线 SOTER 部署采用一机一密，部署时由手机硬件生成一对公私钥，将私钥写入手机 RPMB 分区，公钥上传至 MySQL 数据库，部署完之后再将 MySQL 数据库的内容上传到 SOTER 服务器。

说明：

1. 产线部署采用的是 C/S 架构，OEM 应该将独立部署服务器（数据库信息配置在服务器端），产线站位客户端机器通过 socket 与服务器进行交互，**不应将服务器应用跟客户端应用放在同一台 PC 上运行的方式**
 2. 关于数据加固部分，ODM 产线运维可以**定期对数据库内容进行备份**，防止数据丢失。
-

6.1 MySQL 数据库的使用

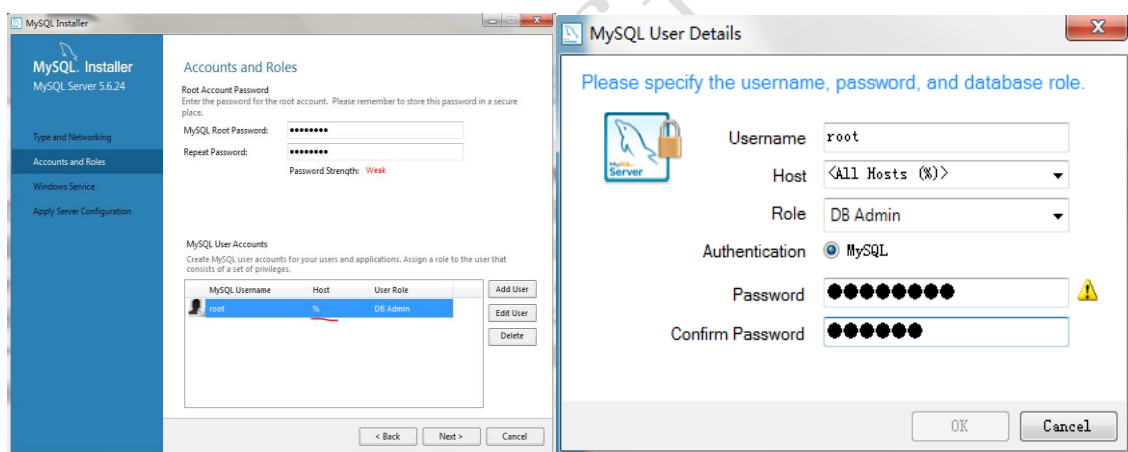
SOTER 部署必须要使用 MySQL 数据库外用来储存硬件生成的 Key，并将上传至微信服务器。

6.1.1 安装 MySQL 数据库

推荐 MySQL 版本：5.6.24.0 以上版本

运行 MYSQL 安装文件，安装 MySQL 数据库，安装过程中注意以下事项：

- 电脑设置为管理员权限
- 需启用 TCP/IP 连接（Enable TCP/IP Networking, Port Number:3306）
- 设置 MySQL Root 密码
- 点击 Add User，建立 MySQL 账号（Host 栏位选择”All Host (%)”项）

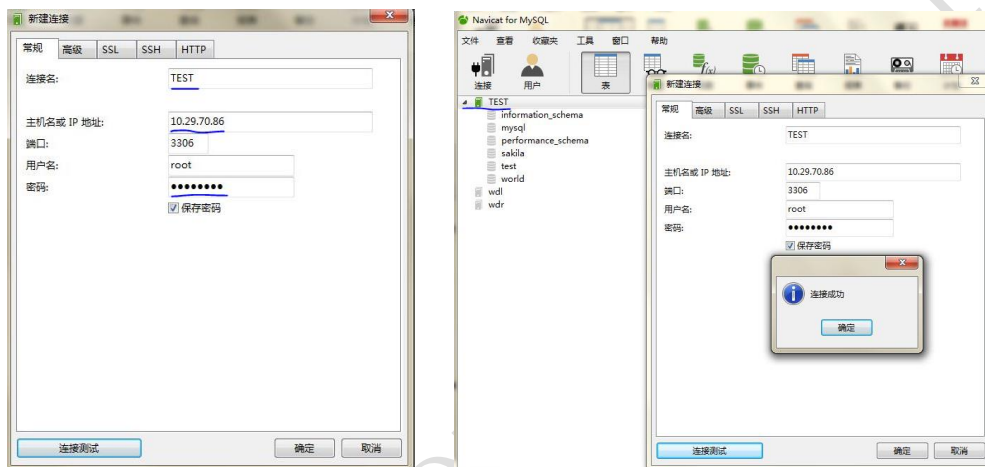


6.1.2 导入 SQL 表文件

MySQL 安装完之后，需要建立数据库，并导入指定的数据库表结构文件（即 SQL 文件，在 SecurityServer 目录\Bin\ToolBox\SQL 下的 **itrust.sql** 文件）。

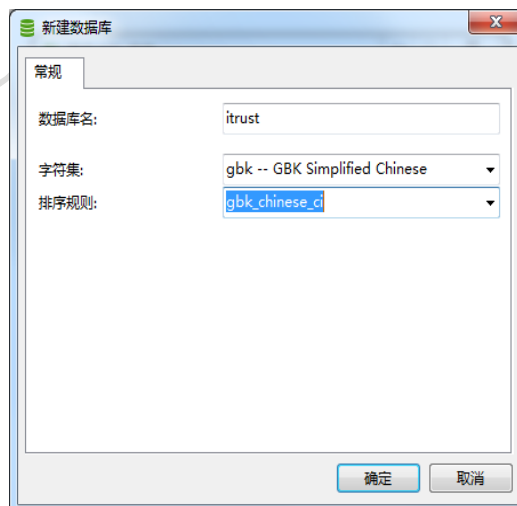
可以使用 MySQL 自带的 MySQL Workbench 数据库管理工具，或者 Navicat 工具管理数据库。下面以 Navicat 工具示例如何导入 SQL 表结构文件：

1. 打开 Navicat 工具，新建连接，输入连接名、主机 IP（本机可直接输入 localhost）、用户名及密码（MySQL 服务端设置的用户名及密码），完成后进行连接测试，连接成功后点击确定

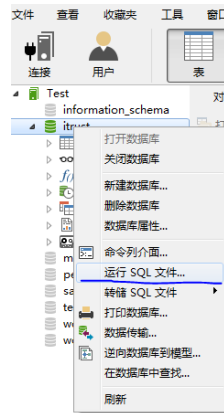


2. 新建数据库，并导入 SQL 文件：

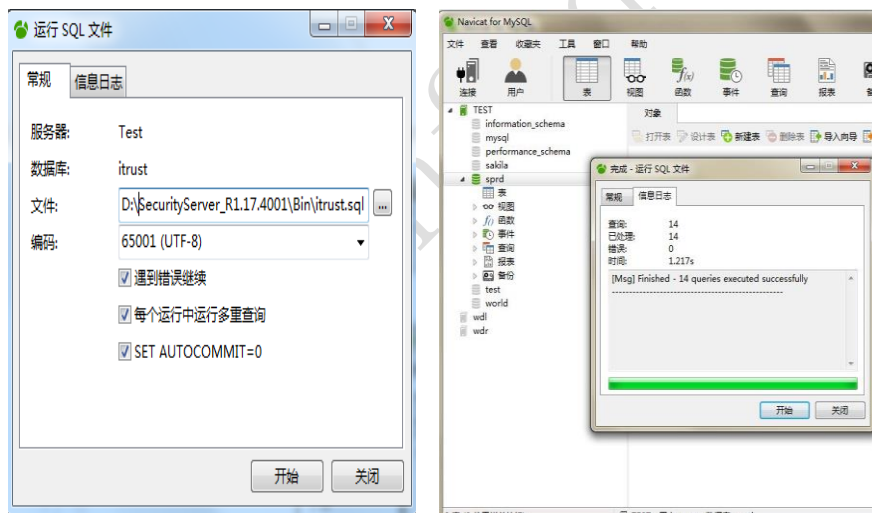
➤ 新建数据库：右键上一步建立的连接，点击“新建数据库”，数据库名称为 **itrust**



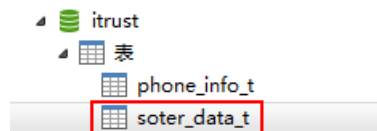
- 运行 SQL 文件：右键上一步新建的数据库，选择“运行 SQL 文件”



- 导入 SQL 文件：在运行 SQL 文件页面“常规/文件”中加载“itrust.sql”文件



3. 检查数据库中是否包含表 phone_info_t 和表 soter_data_t，如下图所示。如未包含表 soter_data_t，在 itrust 数据库中导入“soter_data_t.sql”数据表：



6.2 SecurityServer 与 MySQL 建立连接

SOTER 部署需要连接 MySQL 数据库，MySQL 数据库用于保存部署时手机硬件生成一对公私钥，并将该公私钥上传至 SOTER 服务器。

在部署前，需按照 6.1 节介绍安装 MySQL、导入 SQL 表文件，然后在 SecurityServer 的配置文件 SecureCenter.ini 中设置与 MySQL 数据库建立连接，如下所示：

```
[DataBase]
IP=127.0.0.1           //MySQL 服务 IP
Port = 3306            //MySQL 设置 Port
UserName=root          //MySQL 数据库用户名
PassWord=12345678      //MySQL 数据库密码
DataBase=itrust        //MySQL 数据库文件名称
```

6.3 SOTER 部署配置 SecurityServer

MySQL 配置好之后，需要在 SecureOperations.ini 配置文件中添加 GetSoterATTK，然后开启 Server 并选择对应的 Project，可参考如下配置：

```
[Demo]
1=GetUID
2=SystemInit
3=GetSoterATTK
4=SystemClose
5=DeployEnd
```



说明：

SOTER Key 是写到 EMMC 的 RPMB 分区，在写 SOTER Key 之前需要先初始化 RPMB 分区，这一步是在 SystemInit 进行的，所以 GetSoterATTK 必须在 SystemInit 之后。

6.4 产线部署 SOTER

按照上一节介绍方法配置好 SecuritySever，开启 SecuritySever 并选项相应的 Project。

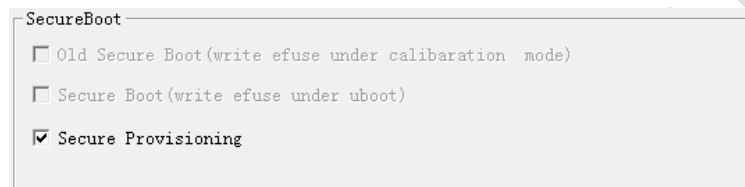
1. 配置 Client 与 SecurityServer 的连接：打开 WriteIMEI.ini 配置文件，配置 Server 端的 IP

[SECURE DEPLOYMENT]

Server IP=127.0.0.1 //设置 SecurityServer IP 地址

Server Port=39998 //设置 SecurityServer Port 口，默认不需要修改

2. 打开 WriteIMEI 工具，设置界面勾选安全部署测项，如下所示：



3. 产线部署：点击工具“写入”按钮，进行测试，测试成功界面如下图所示：



6.5 上传注册设备信息至微信服务器

产线 SOTER 部署完成后,需将传至 MySQL 数据库的公钥信息上传至微信服务器,未上传将会导致 SOTER 认证失败。

可使用 SecurityServer 中 Bin\ToolBox 目录下的 Soter.exe 工具将注册设备信息(传至 MySQL 数据库中信息)上传至微信服务器,步骤如下:

1. 在上传前需要在 SoterConfig.ini 文件中配置 MySQL 相关信息及上传方式,各项配置说明如下:

[Settings]

AutoMode = 0 //0: 将数据库中没有提交的设备注册完成后退出;
 //1: 提交完设备信息后不退出, 等待 Interval 中设置间隔后继续
 查找未注册的设备上传微信服务器。该配置项程序会动态查询,
 再次设置为 0 时自动退出
Interval = 600 //单位为秒, AutoMode 为 1 时有效

[DataBase]

ip = 10.29.70.27 //安全部署 MySQL 数据库 IP
port = 3306 //安全部署 MySQL 数据库端口
username = root //安全部署 MySQL 数据库用户名
password = 12345678 //安全部署 MySQL 数据库密码
database = itrust //安全部署 MySQL 数据库名称

2. 在命令行界面运行 SecurityServer 中 Bin\ToolBox 目录下的 Soter.exe 工具(在部署前需要配置 MySQL 数据库 IP 相关信息), 如下图所示:

```
D:\SecurityServer Bin\ToolBox>Soter.exe -b SPRD -i  
wxalxxxxxxxxxxxxxx -s XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

-b: 设备 brand 信息, 上图 brand 为 SPRD

-i/-s: 分别为 appid 及 appsecret 信息 (需要从微信公众号中申请获得)



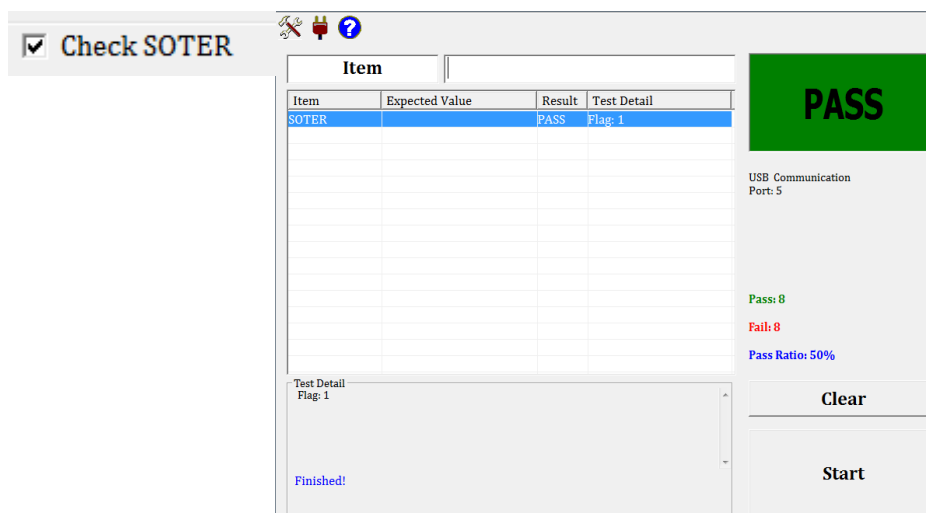
注意:

SOTER 产线部署完成后务必要上传注册设备信息到微信服务器。

6.6 检查 SOTER 标志位

部署结束后使用 CheckX 工具检查 SOTER 标志位是否 Pass:

进入工具设置界面，勾选 Check SOTER 选项，然后进行测试。



第7章 FAQ

7.1 安装 MySQL 的常见问题

1. 安装前需要确保已经安装过 netFramework 4.0
2. Window Server 系统需要安装补丁和补丁 KB2999226-X64.msu

7.2 芯片未写 HUK，进行安全部署会有什么问题？

芯片未写 HUK，在 System Init 阶段会报错，部署失败。

可以查看工具 PhoneCommand Log，Log 中会打印 production not write HUK 信息，如下所示

[2018-06-25 13:21:12:003] apSecurityScheme:

[2018-06-25 13:21:12:003] --> 43(0x0000002b) Bytes

00000000h: 7E 03 00 00 00 29 00 62 00 1D 00 1D 00 00 00 00 ; ~....).b.....

00000010h: 19 00 02 80 10 25 9F A6 D6 4D 11 E6 91 8B 3B 2C ;%...M....,

00000020h: 3A BE 2B 31 10 00 00 02 00 63 7E ; :+1....c~

[2018-06-25 13:21:12:006] <<- 53(0x00000035) Bytes

00000000h: 7E 03 00 00 00 33 00 62 00 01 00 27 00 23 00 00 ; ~....3.b...'#..

00000010h: 00 02 80 00 03 00 00 00 70 72 6F 64 75 63 74 69 ;producti

00000020h: 6F 6E 20 6E 6F 74 20 77 72 69 74 65 20 48 55 4B ; on not write HUK

00000030h: 20 21 0A D4 7E ; !..~

7.3 芯片 Secure Bit 未置位，进行安全部署会有什么问题？

如果 Secure Bit 未置位，安全部署可以 Pass，但是使用 CheckX 工具检查 Secure Boot Enable 标志位会显示失败，下载非签名的 Pac 也是可以的，即安全部署功能未生效。

7.4 安全部署是否可以重复部署？

除 Keybox 外，部署 Pass 的手机，可以再次部署，但是 Efuse 只写一次，如果已经写过了，这一步就直接 By Pass 了。

7.5 IFAA/SOTER/Keybox 写在那里，是否可以重复写入？

IFAA/SOTER/Keybox 写入手机 EMMC 的 RPMB 分区，写 IFAA/SOTER/Keybox 需要初始化 RPMB 分区，初始化 RPMB 分区是在 System Init 阶段去做的，所以 IFAA/SOTER/Keybox 在 SystemInit 之后。

IFAA 部署采用一型一密，IFAA Key 会写入手机 EMMC RPMB 分区，可以重复写的，即可以使用新的 IFAA Key 覆盖原有的 Key。

SOTER 部署是一机一密，SOTER Key 由手机根据手机硬件 ID 生成，并写入 EMMC RPMB 分区，且只会生成一次，再次部署，会将之前写入 RPMB 分区的 Key 读出上传到 MySQL 数据库。SOTER 部署 Pass 后需要上传设备信息到微信服务器。

Keybox 是按照 Devices ID 进行申请的，每个硬件对应唯一的 Keybox，不能重写。

7.6 维修更换 EMMC/BB 芯片，是否需要重新部署？

1. 如需使用安全部署提供的相关功能：

更换 BB 芯片，EMMC 芯片需要同时更换，并需重新进行安全部署，才能正常使用安全部署提供的相关功能

更换 EMMC 芯片，BB 芯片不需要同时更换，但需重新进行安全部署，才能正常使用安全部署提供的相关功能

2. 如不需使用安全部署提供的相关功能：

更换 BB 芯片，如果没有更换 EMMC 芯片，则无法再进行安全部署（因安全部署会初始化 EMMC 的 RPMB 分区，仅能执行一次，相当于 BB 芯片与 EMMC 芯片绑定了），仅影响安全部署提供的相关功能。

更换 EMMC 芯片，BB 芯片不需要更换。

7.7 更换指纹模组是否需要重新进行部署

不需要。IFAA/SOTER/KeyBox 写入 EMMC 的 RPMB 分区, 与硬件相关, 而与指纹模组不相关, 更换指纹模组不会影响 IFAA/SOTER/KeyBox 相关功能的使用。

7.8 重新下载是否需要重新进行部署

不需要。重新下载不会擦除 EMMC 的 RPMB 分区, 故不需要重新进行部署。

7.9 常见 Error Code

1. Attestation Keybox 重复部署: 当前手机已成功部署过 Attestation Keybox, 则不允许再次部署

```
Attestation keybox has already been deployed
IMEI1:362523432432220
```

2. Attestation Keybox 中的 DeviceID 字段与版本预设不匹配

```
Attestation keybox is mismatching the format of
this project
IMEI1:362523432432238
```

3. Db 文件中无可用的 Attestation Keybox (可能是 keybox 已用完)

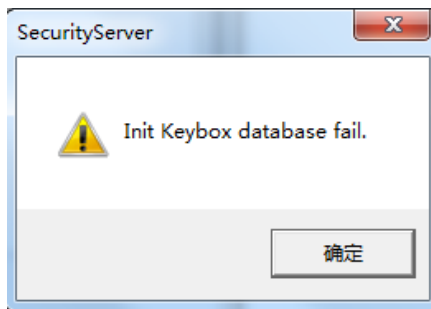
```
Not find attestation keybox file
IMEI1:362523432432246
```

7.10 Keybox db 文件新旧版本转换

SecurityServer_R5.0.0001 新增了统计 keybox 使用状态的功能，keybox 的表结构升级到 v2 版本。

使用该版本下的 SecureToolBox.exe 工具生成的 db 文件与之前工具（如 R4.18.2101，生成 v1 版本的表结构）生成的 db 文件版本数据结构不一致，无法兼容。

R5.0.0001 版本工具使用 v1 版本的 db 文件，打开 Server 出现以下提示：



为了解决升级 SecurityServer，之前使用旧版本 SecureToolBox.exe 工具生成的 db 文件无法使用的问题，可使用 db_transfer.exe 命令行工具，将旧版本的 db 文件转换成新的数据结构 db 文件，使用方法如下：

在命令行运行该应用程序，并给出 db 文件的全路径，如下所示：

```
D:\00_Config>db_transfer.exe "d:\00_Config\2010.db"  
start transfer...  
transfer db to v2.0 successful
```



说明：

1. 可以将该工具放到待转换的 db 目录下，避免输入路径
2. 升级到 v2 版本的 db 文件前，请先做好备份

7.11 安全部署各 Command ID 对应的操作

安全部署报错，更具界面上提示的错误命令 ID，对应的操作说明如下：

```
BSL_RCV_SYSTEM_READY = 0x0001, /* Received the system ready command from client */
BSL_CMD_SYSTEM_INIT = 0x0002,    /* System init */
BSL_CMD_GET_UID = 0x0003,        /* Get chip UID */
BSL_CMD_SET_RTC = 0x0004,        /* Set RTC */
BSL_CMD_SET_ROTPK = 0x0005,      /* Set ROTPK */
BSL_CMD_GET_ROTPK = 0x0006,      /* Get ROTPK */
BSL_CMD_SYSTEM_CLOSE = 0x0009,   /* System close */
BSL_CMD_SET_KEYBOX = 0x000A,     /* Set Keybox */
BSL_CMD_SET_IFAAKEY = 0x000B,    /* Set IFAA RSA Key */
BSL_CMD_GET_DEVICE_ID = 0x000C,  /* Get Device ID */
BSL_CMD_GET_WECHAT_CA = 0x000D,  /* Get Wechat Certificate */
```

附录 Revision History

Version	Date	Owner	Notes
1.0	2017/11/28	HWE-NPI	Created
2.0	2018/04/01	HWE-NPI	Updated
3.0	2018/06/20	HWE-NPI	<ol style="list-style-type: none">1. 新增部署时显示当前 Keybox 使用状态2. 支持分割 Keybox db 功能3. 除 SOTER 部署外，不再依赖 MySQL4. 支持 Keybox 防重写、防错写