



SIM8500_XX系列 Secureboot应用文档

模组

芯讯通无线科技(上海)有限公司

上海市长宁区临虹路289号3号楼芯讯通总部大楼

电话: 86-21-31575100

技术支持邮箱: support@simcom.com

官网: www.simcom.com

名称:	SIM8500_XX系列Secureboot应用文档
版本:	1.00
日期:	2022.3.10
状态:	已发布

版权声明

本手册包含芯讯通无线科技（上海）有限公司（简称：芯讯通）的技术信息。除非经芯讯通书面许可，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播，违反者将被追究法律责任。对技术信息涉及的专利、实用新型或者外观设计等知识产权，芯讯通保留一切权利。芯讯通有权在不通知的情况下随时更新本手册的具体内容。

本手册版权属于芯讯通，任何人未经我公司书面同意进行复制、引用或者修改本手册都将承担法律责任。

芯讯通无线科技(上海)有限公司

上海市长宁区临虹路289号3号楼芯讯通总部大楼

电话：86-21-31575100

邮箱：simcom@simcom.com

官网：www.simcom.com

了解更多资料，请点击以下链接：

<http://cn.simcom.com/download/list-230-cn.html>

技术支持，请点击以下链接：

<http://cn.simcom.com/ask/index-cn.html> 或发送邮件至 support@simcom.com

版权所有 © 芯讯通无线科技(上海)有限公司 2021，保留一切权利。

关于文档

版本历史

版本	日期	作者	备注
1.00	2022.3.10	满存金	第一版

适用范围

本文档适用于 SIMCom SIM8500XX 系列。

目录

关于文档.....	3
版本历史.....	3
适用范围.....	3
目录.....	4
介绍.....	5
本文目的.....	5
使用工具.....	5
参考文档.....	5
1. 镜像签名.....	6
1.1 镜像签名介绍.....	6
1.2 安全相关的配置.....	6
1.3 生成签名密钥对.....	7
1.3.1 Bsp 签名的密钥.....	7
1.4 签名.....	7
2.ROTPK 部署.....	7
2.1 配置 SecurityServer 写 ROTPK	8
2.2 产线 Client 部署 ROTPK.....	8
2.2.1 加载 WriteX.seq 文件.....	8
2.2.2 与 SecurityServer 建立连接.....	8
2.2.3 产线部署.....	9
2.3 检查 SecureBoot 标志位.....	9
2.3.1. 加载 CheckX.seq 文件.....	9
2.3.2 测试.....	9
3.校验测试.....	10

介绍

本文目的

详细介绍了开启 secureboot 的流程，指导客户开启 Secureboot 功能。

参考此应用文档，开发者可以很快理解并快速开发相关业务。

开启 secureboot 流程：镜像签名-ROTPK 部署-测试

使用工具

1. SecurityServer
2. Simba

这两工具是用来做 ROTPK 部署的，Secureboot 的开启不仅需要硬件上做 ROTPK 部署还需要软件签名。

参考文档

[1] 29660_Android10.0Secureboot 使用指南 V1.2

1. 镜像签名

针对需要保护镜像的特点，采取不同的签名和验证方案。原理是相似的，不同之处在于基于加载阶段的不同，签名方案的算法及用来验证签名的元数据的组织方式不一样。

1.1 镜像签名介绍

在引导阶段加载启动的镜像，采用展锐特有的签名验签方案。这些镜像有 fdl1.bin、fdl2.bin、u-boot-spl16k.bin、sml.bin、tos.bin u-boot.bin。这些镜像的执行处于系统早期的引导阶段，一般都运行在安全级别较高的模式。

Uboot 启动后，会逐步加载和校验内核及 android 系统和 modem 系统镜像，这些系统镜像均采用 Avb2.0 方案进行签名和验证。对仅读取一次的小分区（例如 boot、dtbo、recovery 和 modem bins）通常是通过将整个内容计算哈希并签名；对于内存装不下的较大分区（如文件系统 system, vendor, product 和 socko 及 odmko 分区）可以使用哈希树的方式签名；启动时，验证流程会在将数据加载到内存时持续进行。

1.2 安全相关的配置

开启安全启动，首先需要在 Android 板级配置中打开如下的配置：

```
device\sprd\sharkle\sl8541e_1h10_32b\sl8541e_1h10_32b_Natv.mk
```

```
BOARD_SECUREBOOT_CONFIG := true    (我们的代码中默认打开的为 true)    //false will close
```

同时在 BSP 板级配置中同步导出如下的配置：

```
bsp\device\sharkle\androidq\sl8541e_1h10_32b\sl8541e_1h10_32b_Natv\common.cfg
```

```
--- a/androidq\sl8541e_1h10_32b\sl8541e_1h10_32b_Natv\common.cfg
```

```
+++b/androidq\sl8541e_1h10_32b\sl8541e_1h10_32b_Natv\common.cfg
```

```
@@ -1,3 +1,14 @@
```

```
#DTS
```

```
export BSP_DTB="sl8541e-1h10_32b"
```

```
export BSP_DTBO="sl8541e-1h10_32b-overlay"
```

```
+#secure boot config: SPRD|NONE
```

```
+export BSP_PRODUCT_SECURE_BOOT="SPRD"
```

```
+export BSP_PRODUCT_VBOOT="V2"
```

```
+#firmware
```

```
+export BSP_CONFIG_TEE_FIREWALL="true"
```

```
+#sml+tos
```

```
+export BSP_BOARD_TEE_CONFIG="trusty"
```

```
+export BSP_BOARD_ATF_CONFIG="true"
```

```
+export BSP_BOARD_ATF_BOOT_TOS_CONFIG="true"
```

1.3 生成签名密钥对

安全启动方案需要配置如下的密钥来完成所有系统镜像的签名和校验

1.3.1 Bsp 签名的密钥

BSP 相关的镜像签名密钥位置在以下目录：

bsp/build/packimage_scripts/configs/

主要有以下几对：

rsa2048_0.pem 和 rsa2048_0_pub.pem

rsa2048_1.pem 和 rsa2048_1_pub.pem

rsa4096_vbmeta.pem & Rsa4096_vbmeta.pem

可以通过下面的命令生成密钥对：

生成 rsa 私钥

```
$ openssl genrsa -out rsa2048_0.pem 2048
```

```
Generating RSA private key, 2048 bit long modulus
```

```
.....+++
```

```
.....+++
```

```
e is 65537 (0x10001)
```

生成 rsa 公钥

```
$ openssl rsa -in rsa2048_0.pem -pubout -out rsa2048_0_pub.pem
```

```
writing RSA key
```

```
$ls -al *.pem
```

```
-rw-r--r-- 1 user group 1679 Feb 26 20:46 rsa2048_0.pem
```

```
-rw-r--r-- 1 user group 451 Feb 26 20:48 rsa2048_0_pub.pem
```

Bsp 签名是在对 chipram, bootloader 及 trusty 等目标进行编译过程中自动进行的。负责签名的脚本将会在编译目标成功更新后触发：

其中 rsa2048_0 公钥对是用来对 chipram 部分(fdl1.bin & u-boot-spl-16k.bin)签名。rsa2048_1*.pem 用来对 sml.bin, tos.bin 和 u-boot.bin 进行签名。

注意：密钥一点要妥善保存好。

1.4 签名

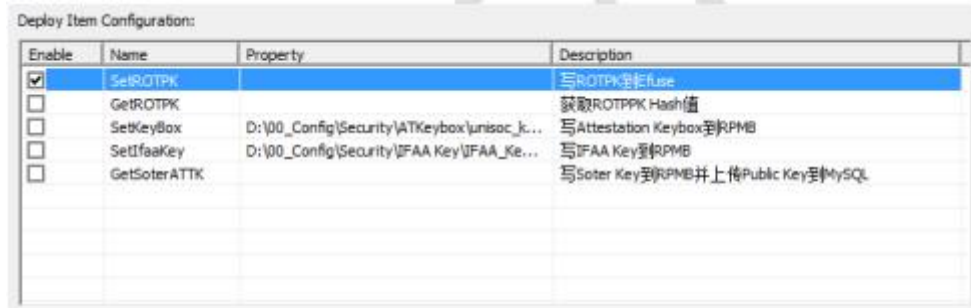
签名是目标编译过程中自动进行的。

2.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 Efuse 中，写 ROTPK 成功后即开启 SecureBoot 功能，支持 TEE 环境则采用安全部署写 ROTPK 的方式开启 SecureBoot 功能；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。

2.1 配置 SecurityServer 写 ROTPK

在 SecurityServer 端配置安全部署需要执行的操作: 双击任务栏 Server 的图标或者右键选择 Setting 项, 进入设置界面, SetROTPK 选项 (其他测项按照实际需求进行勾选), 如下图所示:



然后点击 Ok 保存并启动 Server, 并确保 Server 正常运行。

说明: 1. Server Port 一般不需要修改, 在客户端配置一样的 Port 即可;

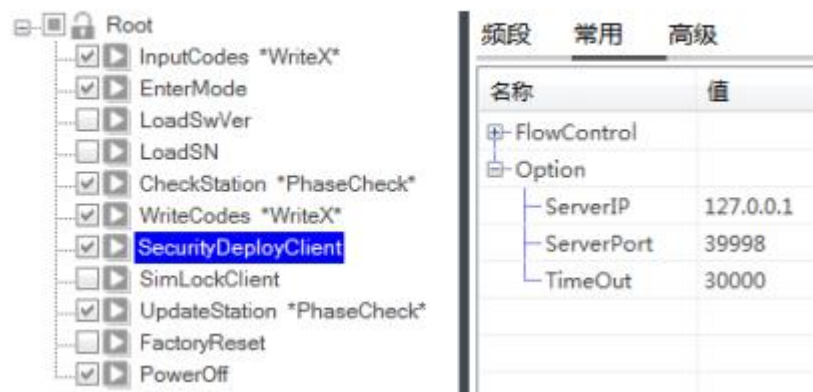
2. 可新建或者修改现有 Project, 点击 OK 按钮保存并启动 Server。

2.2 产线 Client 部署 ROTPK

按照上一节说明, 配置好 SecurityServer 并正常启动后, 配置客户端与 Server 端建立连接, 使用客户端工具进行部署:

2.2.1 加载 WriteX.seq 文件

打开 Simba 工具, 点击打开加载\Bin\Project\Provision\WriteX.seq 文件, 勾选 EnterMode、SecurityDeployClient 等选项:





2.2.2 与 SecurityServer 建立连接

在 SecurityDeployClient 常用页面设置 Server IP 和 Server Port, 如下所示:

Server IP=127.0.0.1 //设置 SecurityServer 的 IP 地址，127.0.0.1 表示本机
Server Port=39998 //与 SecurityServer 中 port 设置一致，默认不需要修改

2.2.3 产线部署

点击工具开始按钮，进行测试，测试成功界面如下图所示：

全部开始(S)						 	
状态	全部通过						
结果	通过						
耗时	00:00:26						
通过率(%)	(1/1)100.00%						

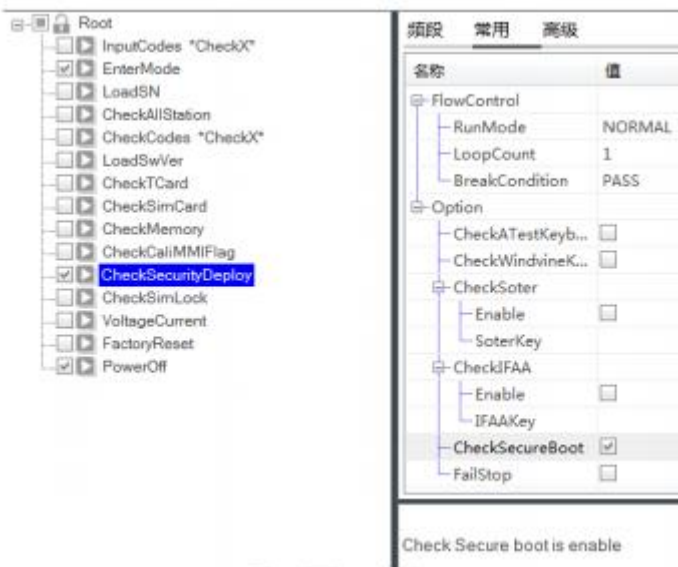
	测试项	条件	下限	数据	上限	单位	状态
▶ 1	Port Plugged In	SPRD U2S Diag (COM5)	-	1.00	-	-	pass
2	Port Plugged Out	SPRD U2S Diag (COM5)	-	1.00	-	-	pass
3	Port Plugged In	SPRD U2S Diag (COM5)	-	1.00	-	-	pass
4	EnterMode	Mode = Gd81	1.00	1.00	1.00	-	pass
5	Security Deploy Client		1.00	1.00	1.00	-	pass

2.3 检查 SecureBoot 标志位

部署结束后可使用 Simba 工具检查 SecreuBoot 标志位，确认部署是否 Pass：

2.3.1. 加载 CheckX.seq 文件

打开 Simba 工具，点击打开加载\Bin\Project\Provision\CheckX.seq 文件，勾选 Enter Mode\CheckSecurityDeploy 等选项，CheckSecurityDeploy 常用页面中勾选 CheckSecureBoot 选项：



2.3.2 测试

返回到测试页面，点击工具开始按钮进行测试，测试 Pass 界面如下图所示：

全部开始(S)									
状态	全部通过								
结果	通过								
耗时	00:00:24								
通过率 (%)	(2/2) 100.00%								
	测试项	条件	下限	数据	上限	单位	状态		
1	Port Plugged In	SPRD U2S Diag (COM5)	-	1.00	-	-	pass		
2	Port Plugged Out	SPRD U2S Diag (COM5)	-	1.00	-	-	pass		
3	Port Plugged In	SPRD U2S Diag (COM5)	-	1.00	-	-	pass		
4	EnterMode	Mode = 0x81	1.00	1.00	1.00	-	pass		
5	SecureBoot is enabled		1.00	1.00	1.00	-	pass		
6	Port Plugged Out	SPRD U2S Diag (COM5)	-	1.00	-	-	pass		
7	PowerOff		1.00	1.00	1.00	-	pass		

注意：步骤是，手机关机，simba 点开始，连接 usb 线，不用按什么键，每次部署手机都要下电一次，确保手机在关机状态下。开关键拨到开的状态。

3.校验测试

具体测试操作步骤如下：

1. 签过名的镜像文件下载到设备中
2. ROTPK 部署到设备，就可以开启成功

模块开启 secureboot 成功，下载未签名的镜像文件，会下载失败。

注意：ROTPK 部署和软件签名，都需要操作，两者缺一不可。