Simlock 介绍

Document Number:		**Document Version:**	
Owner:		**Date:**	
Document Type:			
NOTE:	ALL MATERIALS INCLUDED HEREIN ARE COPYRIGHTED AND CONFIDENTIAL UNLESS OTHERWISE INDICATED. The information is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination, or other use of or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. This document is subject to change without notice. Please verify that your company has the most recent specification. Copyright © 2013 Spreadtrum Communications Inc.		

SPREADTRUM®

www.spreadtrum.com

目录

1. Simlock 简介 3
2. 相关知识介绍 3
2.1. IMSI 3
2.2. MCC MNC 3
2.3. Network subset 3
2.4. GID1 3
2.5. GID2 4
3. 基础 simlock 类型 4
3.1. Network lock 5
3.2. Network Subset lock 5
3.3. SP lock 5
3.4. Corporate lock 5
3.5. User lock 5
4. 扩展 simlock 类型 6
4.1. One simlock 6
4.2. 卡槽依赖 1 6
4.3. 卡槽依赖 2 6
4.4. 卡槽 2 网络锁黑名单锁定 6
4.5. 过期卡+one simlock 6
4.6. 过期卡+卡槽依赖 1 7
4.7. 过期卡+卡槽依赖 2 7
5. AP 侧基础 simlock 功能实现 7
5.1. simlock 状态监听与消息通知时序图 8
5.2. simlock 解锁时序图 9
5.3. simlock 解锁流程图 10
6. 参考引用 10

1. Simlock 简介

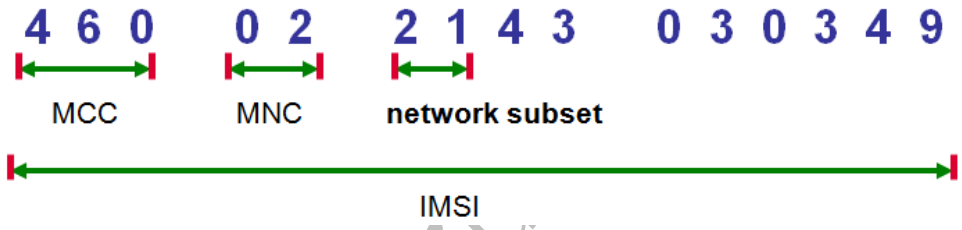
Simlock 通常是运营商用于竞争的一种手段，通过低价销售手机，并将该手机绑定特定 SIM 卡限制与 SIM 卡相关的通信业务而赢取市场。

当 simlock 锁卡功能开启后，在开机的过程中，系统会去检验 SIM 卡的对应信息是否匹配（如 MCC，MNC 等），如果匹配则正常开机，如果被锁则需通过密码解锁后才能使用手机所有功能，否则手机的与 SIM 卡相关的通信业务不可用。

2. 相关知识介绍

2.1. IMSI

IMSI：International Mobile Subscriber Identification Number，即国际移动用户识别码，是一种存储于 SIM 卡中的标识码，是识别唯一移动用户的标志。可以使用 AT+CIMI 获取 IMSI 值。



2.2. MCC MNC

MCC：移动国家码，3 位数字，IMSI 的前 3 位。

MNC：移动网号，2 位或 3 位数字，IMSI 的第 4-5 或 4-6 位。

2.3. Network subset

固定为 IMSI 的第 6，7 位，由运营商规定，代表某一时间运营商发行的某一类型卡。

2.4. GID1

Group Identifier Level 1：SIM 卡的基本文件中包含的用于关联特定 SIM 卡和移动设备的标识符，它可用于识别用于特定应用的一组 SIM 卡。

取值范围：0-255

Identifier: '6F3E'	Structure: transparent	Optional
File size: n bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to n	USIM group identifier(s)	O	n bytes

2.5. GID2

Group Identifier Level 2：GID2 和 GID1 的文件结构是完全相同的，都是用于网络运营商取决于应用而实现不同的安全级别。

Identifier: '6F3F'	Structure: transparent	Optional
File size: n bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to n	USIM group identifier(s)	O	n bytes

3. 基础 simlock 类型

Simlock 支持 5 种基础锁类型，这 5 种类型的锁定项各不相同，可以单独或组合使用。

Code	Network (MCC, MNC)	Network Subset (IMSI digits 6 and 7)	SP	Corporate	SIM/USIM (IMSI digits 8 to 15)
Personalisation category					
Network	✓				
Network subset	✓	✓			
SP	✓		✓		
Corporate	✓		✓	✓	
SIM/USIM	✓	✓			✓

3.1. Network lock

网络锁，该业务允许网络运营商个性化移动终端，限制其只能使用特定网络运营商的(U)SIMs。

锁定项：MCC, MNC

3.2. Network Subset lock

网络子集锁，该业务是对网络锁做进一步的限制，使移动终端只能用于网络锁(U)SIMs 的一个子集。

锁定项：MCC, MNC,Network subset

3.3. SP lock

服务供应商锁，该业务允许服务提供商个性化移动终端，限制其只能使用特定服务供应商的(U)SIMs，只针对 GID1。

锁定项：MCC, MNC, sp

3.4. Corporate lock

集团业务锁，该业务允许集团对其提供给雇员和客户的移动终端进行个性化，限制其只能使用该公司自己的(U)SIMs，针对 GID1 和 GID2。

锁定项：MCC, MNC, sp, corporate

3.5. User lock

用户锁，该业务限制手机只能用于特定的(U)SIMs，即某张特定 IMSI 的 SIM 卡。

锁定项：imsi_len, imsi_val[0]-[7]

4. 扩展 simlock 类型

4.1. One simlock

任意一个卡槽插入符合配置的白名单 SIM 卡，两张卡都可以用。目前只针对网络锁。

4.2. 卡槽依赖 1

当卡槽 1 插入白名单的 SIM 卡时，卡槽 2 插入任意卡都可用；

当卡槽 1 不插卡或插入黑名单的 SIM 卡时，卡槽 2 插入任意卡都不可用。

目前该功能只针对网络锁。

4.3. 卡槽依赖 2

当卡槽 1 插入白名单的 SIM 卡时，卡槽 2 插入任意卡都可用；

当卡槽 1 不插卡或插入黑名单的 SIM 卡时，卡槽 2 插入白名单的 SIM 卡时卡 2 可用，插入黑名单的 SIM 卡时不可用。

目前该功能只针对网络锁。

4.4. 卡槽 2 网络锁黑名单锁定

只针对卡槽 2 配置网络锁黑名单，卡槽 1 可仍配置普通白名单的网络锁，当卡槽 2 插入 nv 中配置的黑名单 SIM 卡时，该卡不可用。

4.5. 过期卡+one simlock

在 one simlock 的基础上，增加对过期卡的限制，即不同于白名单的有效 SIM 卡，白名单的过期卡无解锁卡槽的功能。

譬如：卡槽 1 插入黑名单 SIM 卡，卡槽 2 插入白名单过期卡，两张卡均不可用。

4.6. 过期卡+卡槽依赖 1

在卡槽依赖 1 的基础上，增加对过期卡的限制，即不同于白名单的有效 SIM 卡，卡槽 1 的白名单过期卡没有解锁卡槽 2 的能力。

譬如：卡槽 1 插入白名单过期卡，卡槽 2 插入白名单 SIM 卡，两张卡均不可用。

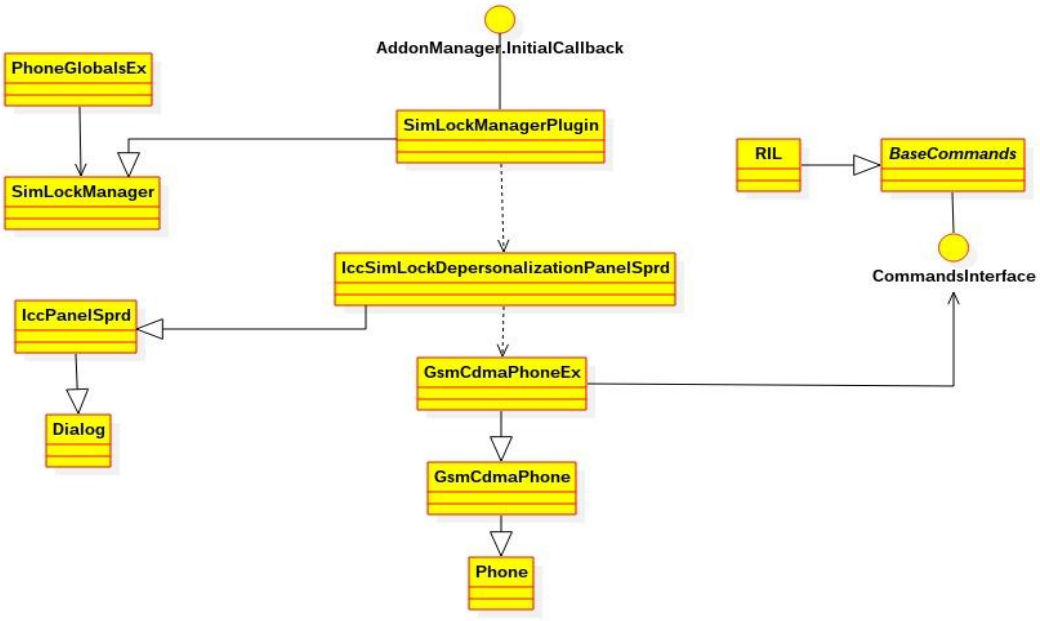
4.7. 过期卡+卡槽依赖 2

在卡槽依赖 2 的基础上，增加对过期卡的限制，即不同于白名单的有效 SIM 卡，卡槽 1 的白名单过期卡没有解锁卡槽 2 的能力。

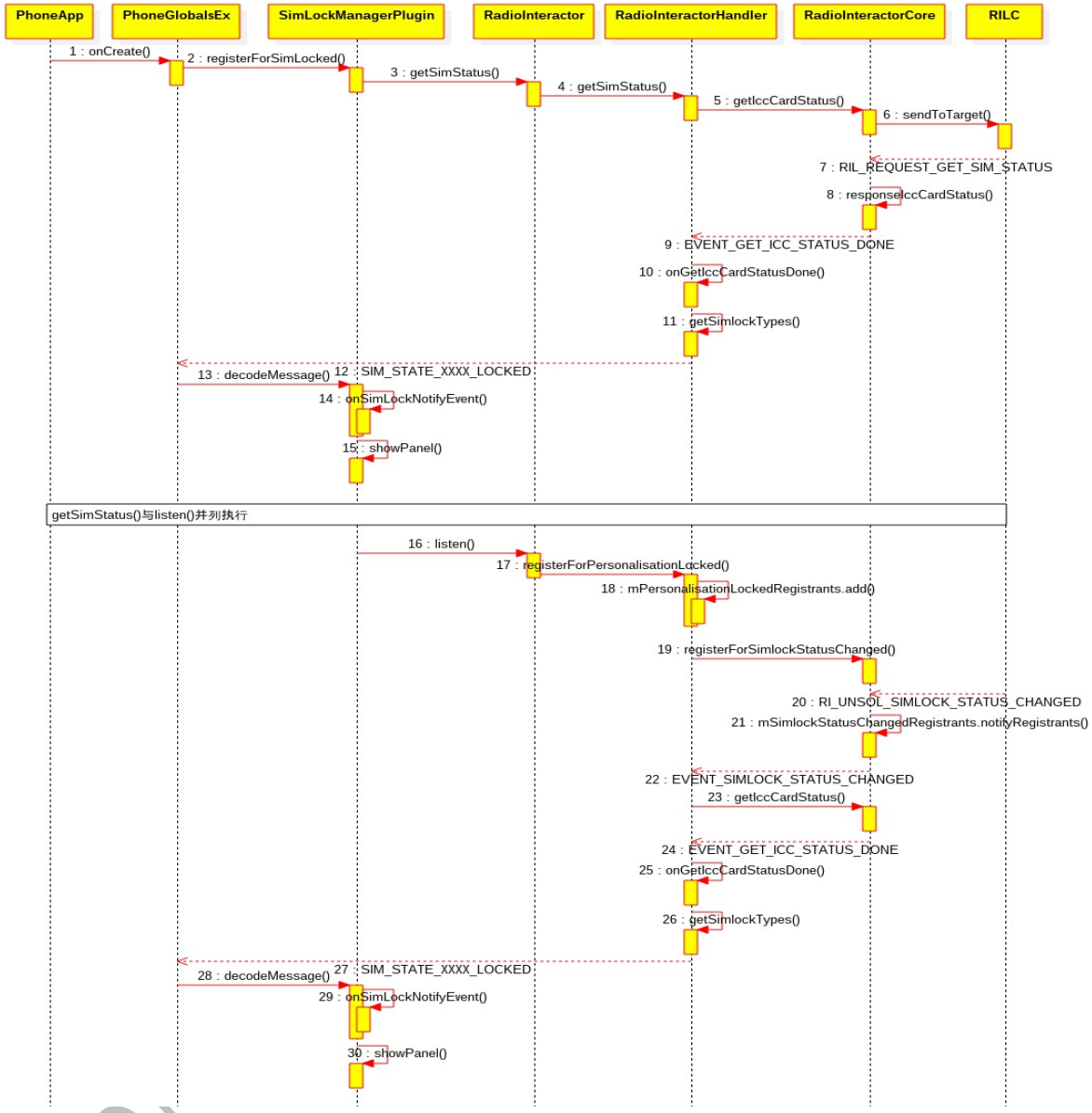
譬如：卡槽 1 插入白名单过期卡，卡槽 2 插入非白名单 SIM 卡，两张卡均不可用；卡槽 1 插入白名单过期卡，卡槽 2 插入白名单 SIM 卡，卡 2 可用。

5. AP 侧基础 simlock 功能实现

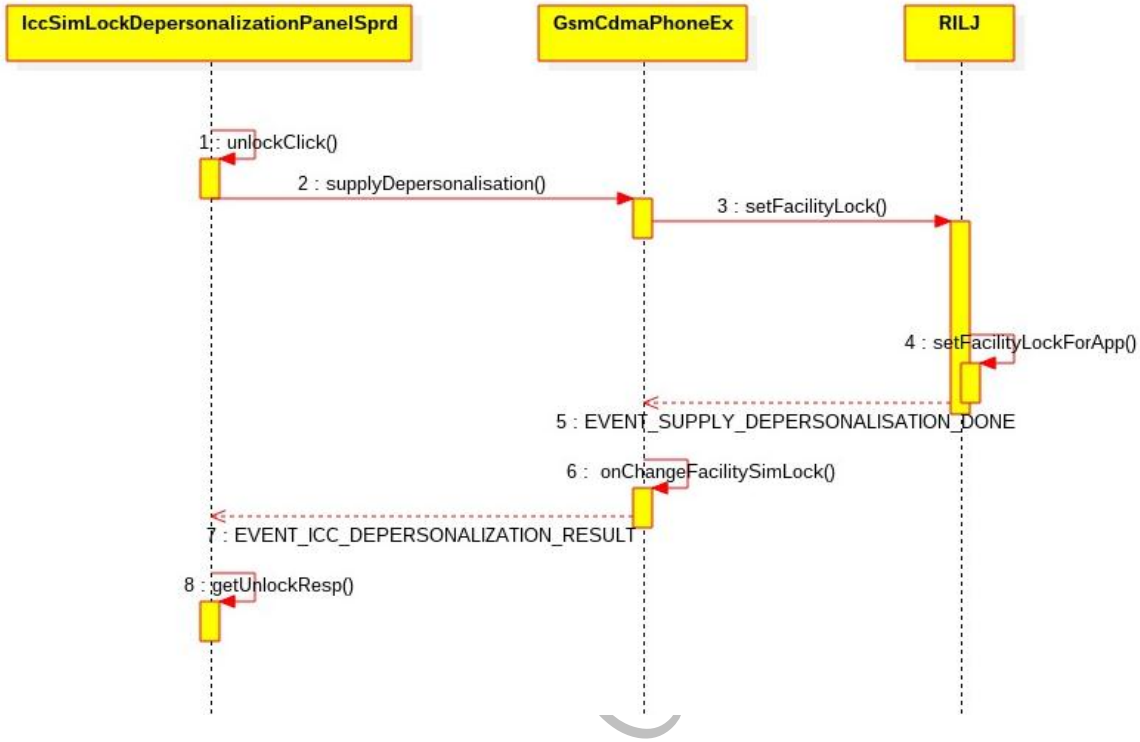
在 simlock 基础功能中，AP 侧主要是负责 simlock 状态的监听和处理，包括解锁界面的显示、交互，modem 负责锁卡的逻辑和功能，AP 与 modem 通过 AT 进行交互。



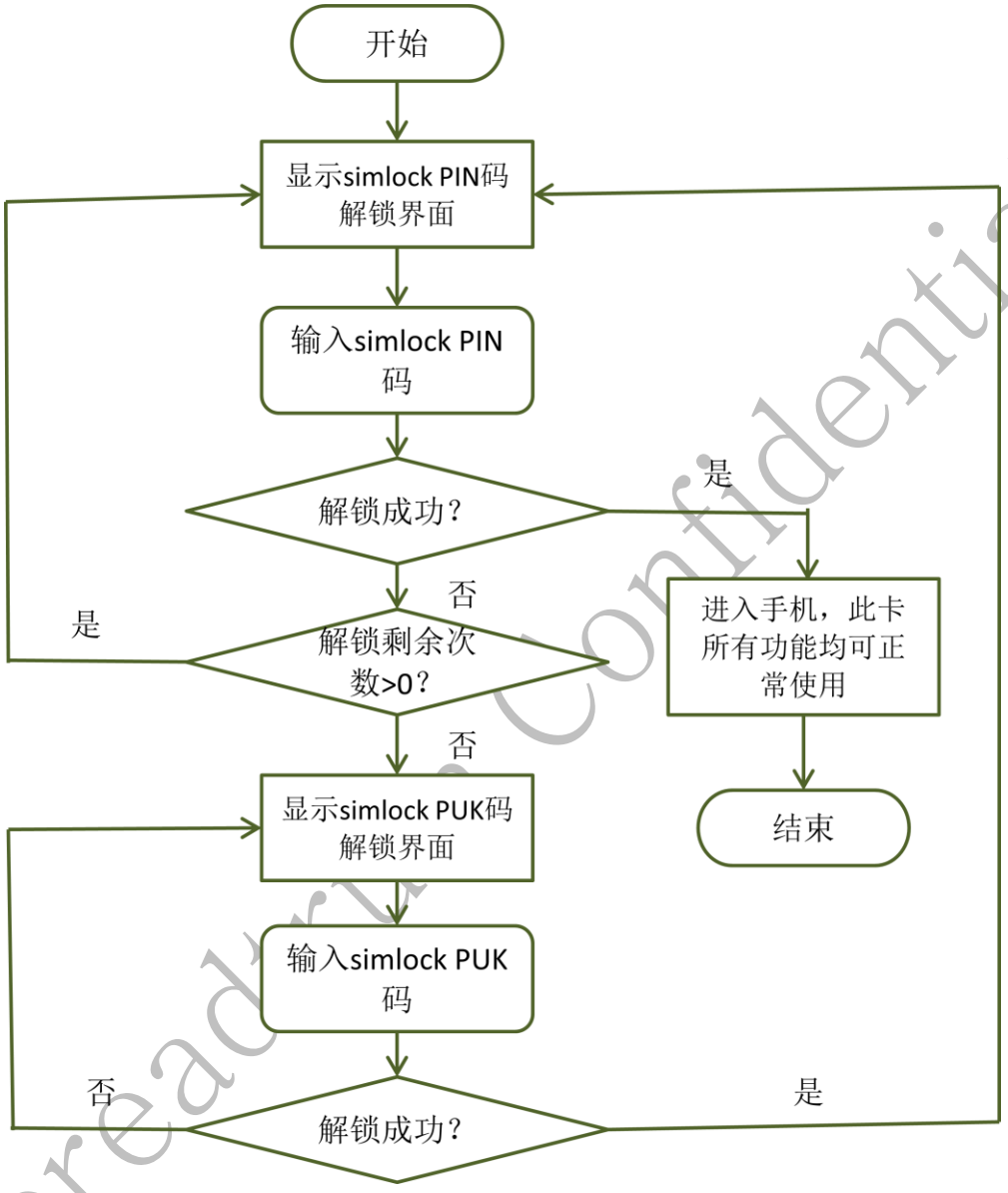
5.1. simlock 状态监听与消息通知时序图



5.2. simlock 解锁时序图



5.3. simlock 解锁流程图



6. 参考引用

3GPP TS 22.022
3GPP TS 31.102