PersistentDataBlockManager

# TODO

<https://cfig.github.io/2017/12/20/Android-Factory-Reset-Protection-FRP/>

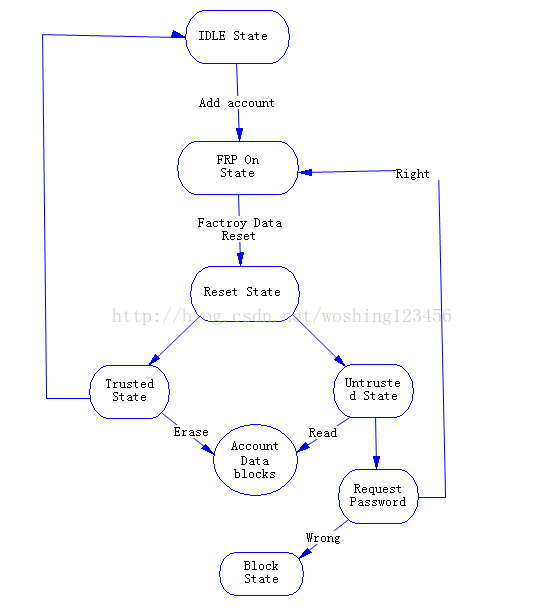
<https://www.smwenku.com/a/5b8085dd2b71772165a81bf6/zh-cn/>

# 简介

在Android 5.0 以后以后的设备默认开启恢复出厂设置保护功能，主要是为了减少用户在丢失手机的带来的损失，比如手机上的一些照片和其他一些重要资料被偷盗者非法利用。此功能可以让用户可以通过谷歌账号登陆Google Play Service远程重置手机或者更改屏幕解锁密码或者锁定屏幕。

       这个和苹果设备的苹果ID是一样的，不同的是苹果设备是强制要求有苹果ID的，而Android设备不是强制的，你可以不添加谷歌账号到设备上，那么这个功能也就不会开启。

让我们看看它的实现方式。让我们看看它的实现方式。



        上图是我用PowerDesign画的一个简单状态图，其中Account Data Blocks是这个机制的关键地方，一个独立存储分区。

首先我们要有一块独立的存储分区，这块分区在恢复出厂设置的时候是不能进入的。这块分区大小为500KB，设置系统Property值ro.frp.pst来指定这个分区的路径。读写这个分区是通过系统的API android.service.persistentdata.PersistentDataBlockManager来操作的，对第三方应用是隐藏的。同时这个API也是为了设备厂商定制SetupWizard而提供的。

       当你创建在你的设备上创建一个谷歌账号时，FRP就会把创建一个重置标志和key保存在这个block。当然，你可以创建多个账号到你的设备上，任何一个账号都可以起到相同的作用。在你的设备丢失后，你可以在其他的Android设备通过Android设备管理器登陆你的Google账号来定位你的设备，同时也可以清空数据或者锁定。

       如果你的设备被偷了，那么你可以远程让自己的手机恢复出厂设置，那么设备就会认为这是不可信任的恢复出厂设置。在进入SetupWizard的时候设备就会读出存储在PersistentDataBlock的数据，提示输入账号密码，那么此时小偷进行不下去，手机在手里废了。

       设备唯一信任的恢复出厂设置是通过Settings来手动操作的恢复出厂设置，这时设备会把PersistentDataBlockde 数据擦除。完了就是一部全新的手机。这不就便宜了小偷了吗，所以最好上个屏幕锁，在小偷破解你的密码之前你先来个不可信任的恢复出厂设置。不过即使小偷顺利的完成了这个操作，你的相片什么的也会被擦除了，不用担心什么艳照门，使你的损失降到最低。

       如果小偷是个高手，想通过刷机来使用手机。那么我们有个安全机制，就是OEM Unlock state. 这个标志位存放在独立分区的最后一位，只能通过PersistentDataBlockManager这个API来更改。手机出厂后是要disable OEM Unlock的，即这个值为0. 如果OEM Unlock是disable的，是不容许刷 bootloader的，因此这个方法也不行。

      那么我们如何把这个功能集成到Android系统中呢？

         1.添加一个独立的存储块并且在恢复出厂设置的时候不会进入和擦除这个分区。

         2.这个block的大小在500KB左右，最大不要超过2M，否则会影响手机性能。

         3.设置这个block的拥有者是系统。

         4.设置系统Property  ro.frp.pst值来指定这个block的路径。

         5.添加一个物理内存块（如eMMC）的入口并指定路径。

         6.如果你要授权一个Service来读写这个block来存取我们账号的标志，只要更改config\_persistentDataPackageName为Service的名字，如果用到默认的谷歌解决方案，则这个值被设置为Google Play Service Package。在国内的网络是无法登陆Google账号的，设备厂商就可以提供自己的用户账号服务来定制这个功能。

        7.添加Factory Reset Protection的SElinux的权限，即在sepolicy配置文件来添加上下文环境。

     为了避免在集成时引入一些安全风险，有以下注意事项。

        1.所有的在添加账号生成的标志必须保存在我们这块独立的存储分区。

        2.JTag接口必须被锁住，即JTag不能进入这个物理存储块。

        3.在硬件开发时不要破坏安全机制，反对添加物理装置（如特殊按键）来自动实施可信任恢复出厂设置。

        4.添加到设备的任何一个Google账号都可以通过验证。

        5.不要在出厂前在设备上添加任何虚拟的账号，用户不知道密码可能被锁死。

        6.用户可以登录Google网站来更改密码，新的密码才能在设备上通过认证而不是报错。

        7.但是当你登录Google网站更改Google账号密码，设备要等72小时后才能使用新密码解锁，在此期间用户可以使用就密码解锁，目的是防止用户的手机和账号同时丢失的情况，被人重置密码破解。

        8.这个功能建立在2015年1月之后版本的Google Play Service上，设备厂商必须预装最新的Google Play Service来开启这个功能。

      Android L之后这个功能就默认打开了，以后再也不用担心Android手机丢了，当然前提是你要在你的手机上注册一个Google account或者设备厂商定制实现类似机制的服务账号。

# PersistentDataBlockManager

# 参考

Android L集成新特性之恢复出厂设置保护之如何实现，类似苹果ID的远程控制功能

https://blog.csdn.net/woshing123456/article/details/44524051