System Low-Level Design Document

System Low-Level Design Document

Analysis & Design

MT6000

Doc No:	AD6000-T5-SLD-V1.0EN_Permission_control_N
Version:	V1.0
Release date:	2016-08-28
Classification:	Internal

Specifications are subject to change without notice.

Keywords

System Low-Level Design Document

MediaTek Inc.

Postal address

No. 1, Dusing 1st Rd. , Hsinchu Science Park, Hsinchu City, Taiwan 30078

MTK support office address

No. 1, Dusing 1st Rd. , Hsinchu Science Park, Hsinchu City, Taiwan 30078

Internet

http://www.mediatek.com/

Document Revision History

Revision	Date	Author	Description
V1.0	2016-12-20	Zhengyu Zhan	Initial Release from DS6000-D4A-DMT-V1.0EN

Contents

Document Revision History **4**
Table of Contents ..... Error! Bookmark not defined.
Lists of Tables ..... Error! Bookmark not defined.
Lists of Figures ..... Error! Bookmark not defined.
1 Introduction **7**
1.1 Purpose 7
1.2 Scope 7
1.3 Who Should Read This Document 7
1.4 How to Use This Manual 8
2 References **9**
3 Overview **10**
3.1 Logical Architecture 10
3.2 Auto boot control 10
3.3 Permission request records 11
3.3.1 PermissionTriggerHistoryActivity & AppToPermissionActivity 11
3.3.2 TriggerTimeDialog 12
3.4 Cellular data control 12
3.4.1 CellularDataControlActivity 12
3.4.2 CellularDataCheckActivity & CellularDataCheckActivityTwo 13
4 Activities **14**
4.1 Auto boot control 14
4.1.1 Type 14
4.1.2 Purpose 14
4.1.3 Subordinates 15
4.1.4 Dependencies 15
4.1.5 Processing 15
4.1.6 Data 16
4.2 Permission request records 17
4.2.1 Type 17
4.2.2 Purpose 17

4.2.3 Dependencies 17
4.2.4 Processing 18
4.3 Cellular data control 18
4.3.1 Type 19
4.3.2 Purpose 19
4.3.3 Dependencies 19
4.3.4 Processing 20
4.3.5 Data 21

1 Introduction

1.1 Purpose

In CTA spec "Technical requirements for security capability of smart mobile terminal" indicate the smart phone must satisfy the security level 1 defined in spec. There are five levels defined in spec since only level 1 can pass CTA test. MTK In House permission will cover the level 5 security range defined in spec.

The level 5 security on software side requires the device should give a way for user to control some application's behavior.

1. 3rd application's permissions such as read your contacts, this part has been done by Android N.
2. Whether 3rd application can auto boot.
3. Whether 3rd application can use cellular data.
4. Record all application's permission request.

Under this background the permission control feature are required to do and pass CTA test for security issues.

1.2 Scope

The In House PermissionControl is base on the Android system requirements specification. And will be only enabled on internal devices.

These document relate only to Android N and later Version, For Android M Version, please refer to AD6000-T5-SLD-V1.0EN_Permission_control_M.doc

1.3 Who Should Read This Document

This document is primarily intended for:

- Engineers with technical knowledge of the android app
- Customers who integrate the permission control with user-defined applications

1.4 How to Use This Manual

This segment explains how information is distributed in this document, and presents some cues and examples to simplify finding and understanding information in this document. Table 1-1 presents an overview of the chapters and appendices in this document.

Table 1-1. Chapter Overview

#	Chapter	Contents
1	Introduction	Describes the scope and layout of this document.

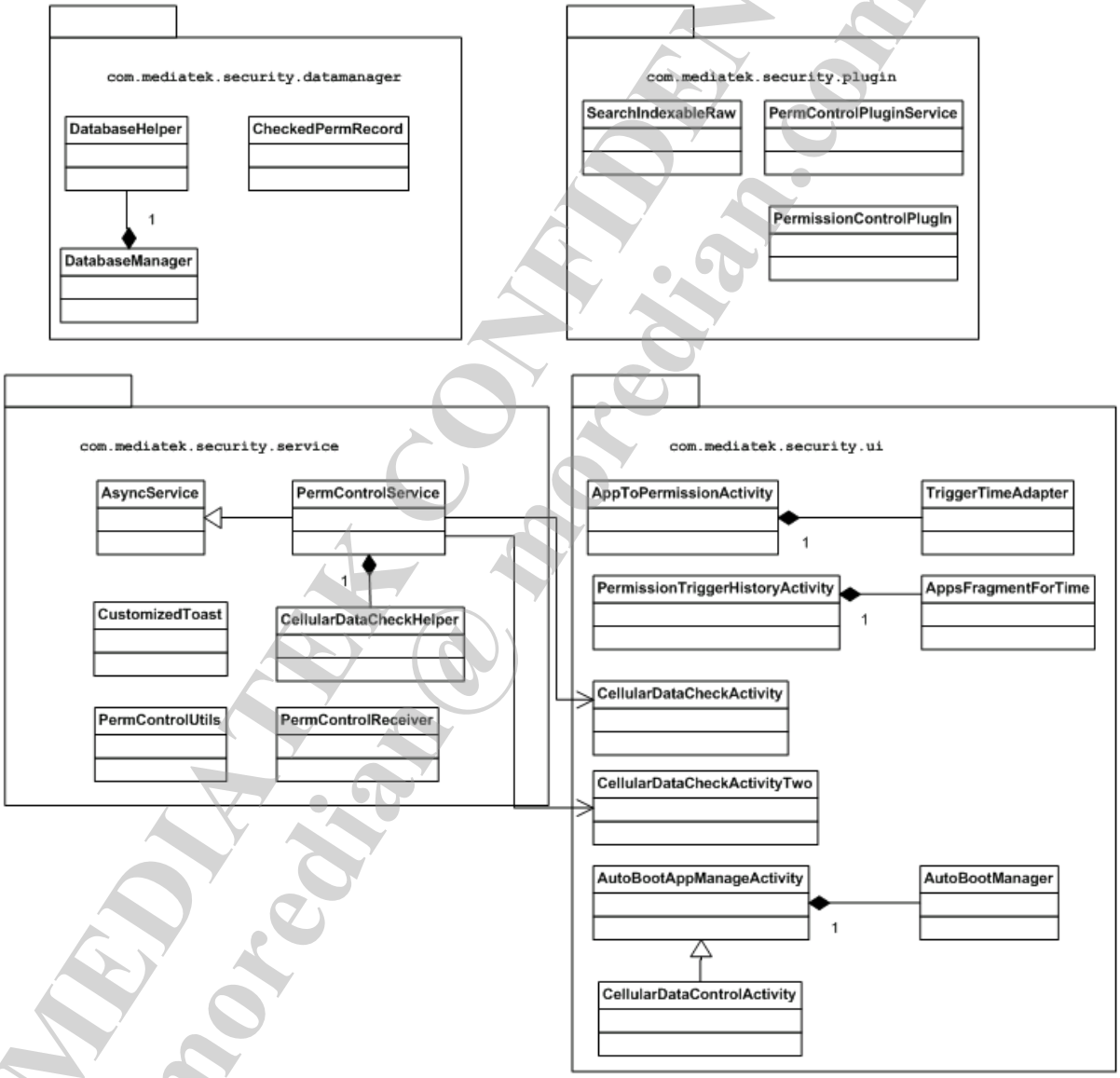
2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

1. CTA mobile security spec v0 96.pdf
2. YDT 2407-2013 移动智能终端安全能力技术要求.pdf
3. YDT 2408-2013 移动智能终端安全能力测试方法.pdf

3 Overview

3.1 Logical Architecture



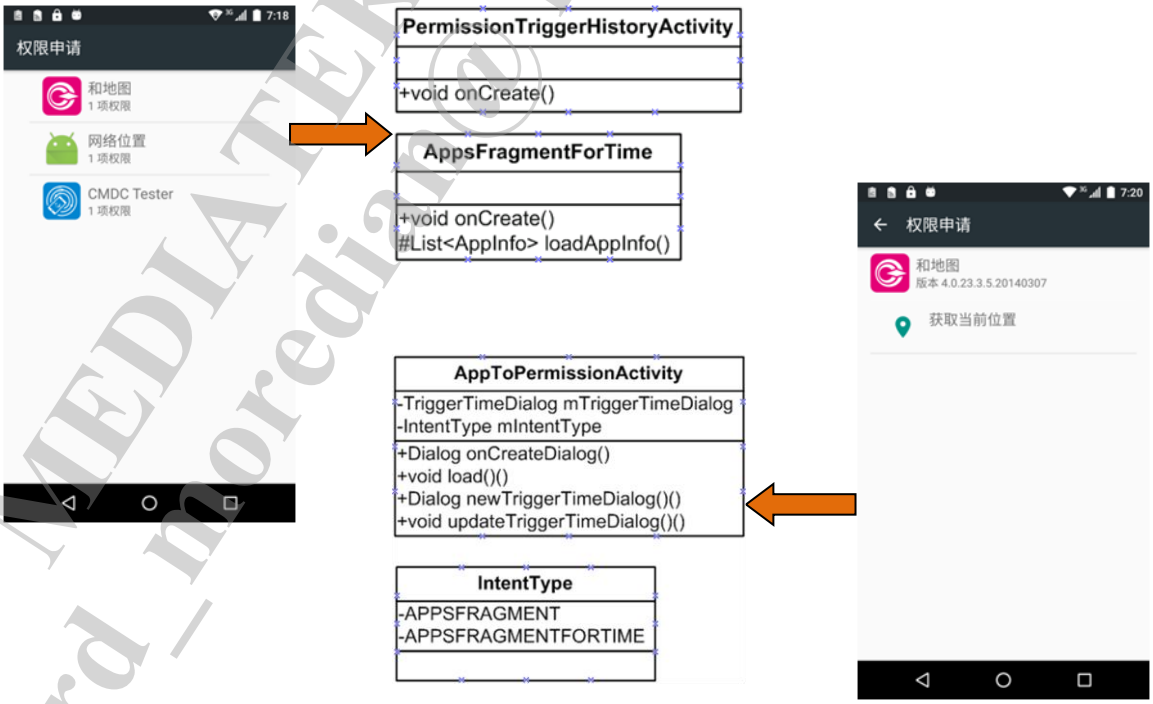
3.2 Auto boot control

This activity shows which 3th party apps needs auto boot. Through the switch to enable/disable whether the app can auto boot.

3.3 Permission request records

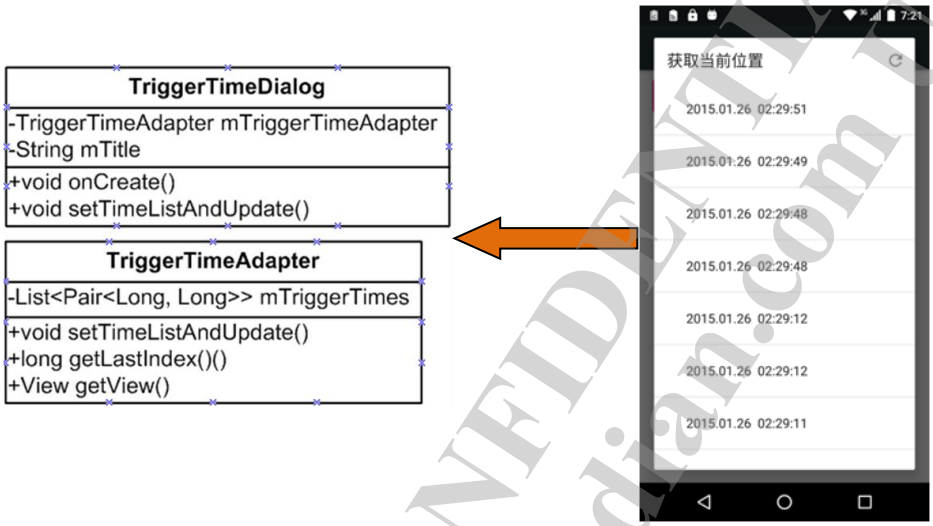
3.3.1 PermissionTriggerHistoryActivity & AppToPermissionActivity

Since permission request' s activity is similar with permission control' s. PermissionTriggerHistoryActivity include AppsFragmentForTime which is extends from AppsFragment. ApptoPermissionActivity use a member variable mIntentType to distinguish which feature is using this activity and do difference performance.



3.3.2 TriggerTimeDialog

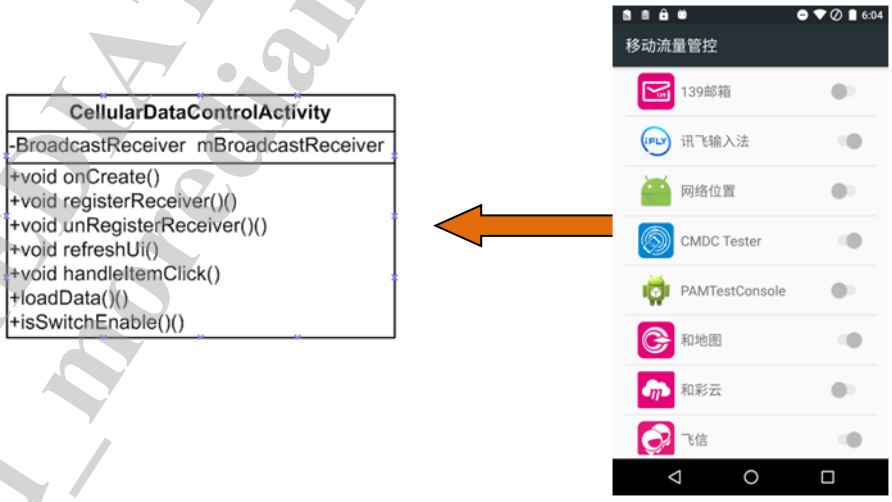
This dialog shows the selected app' s permission request history. It will update data when its parent activity' s onResume function has been called or the refresh button has been pressed.



3.4 Cellular data control

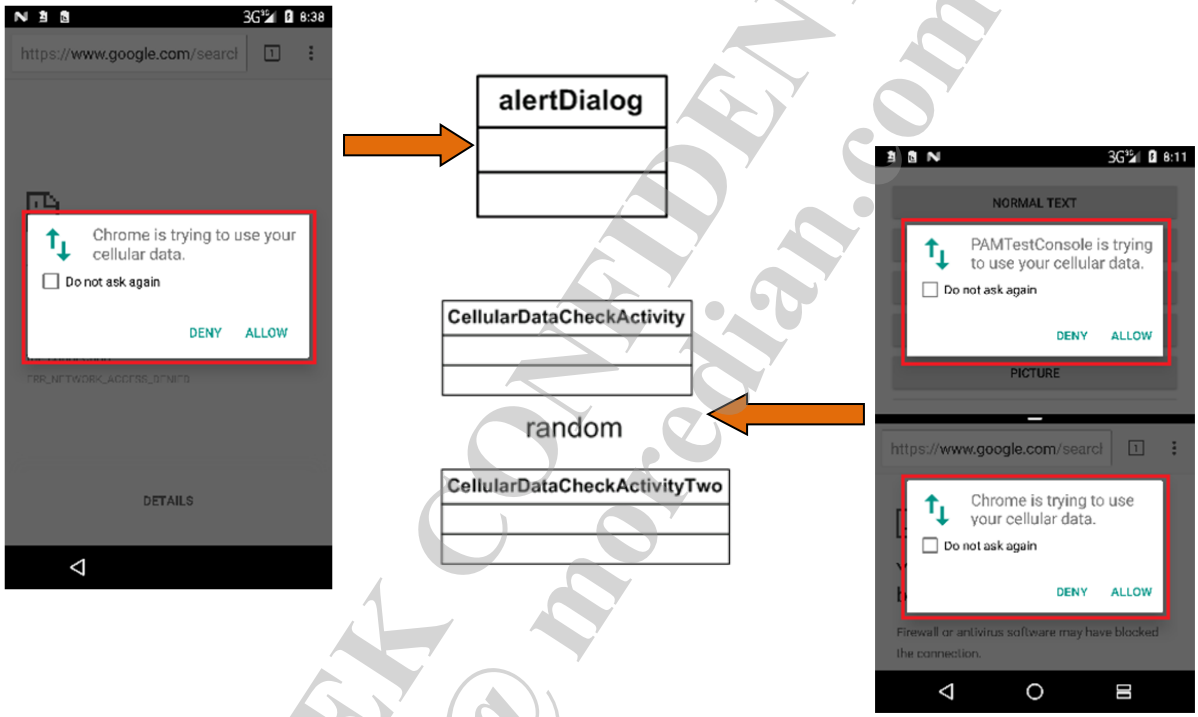
3.4.1 CellularDataControlActivity

This activity extends from AutoBootAppManagerActivity. It shows which 3th party apps use cellular data. Through the switch to enable/disable whether the app can use cellular data.



3.4.2 CellularDataCheckActivity & CellularDataCheckActivityTwo

These two activities are for Android N multi-window. When permission control show an alert dialog in multi-window mode, the dialog will lay on top of two activities. So permission control need to start a dialog style activity and use FLAG_ACTIVITY_LAUNCH_ADJACENT to decide window will show this activity.



4 Activities

4.1 Auto boot control

This feature manager which 3th party apps can auto boot.

4.1.1 Type

An activity of permission control.

4.1.2 Purpose

Manager which 3th party apps can auto boot.

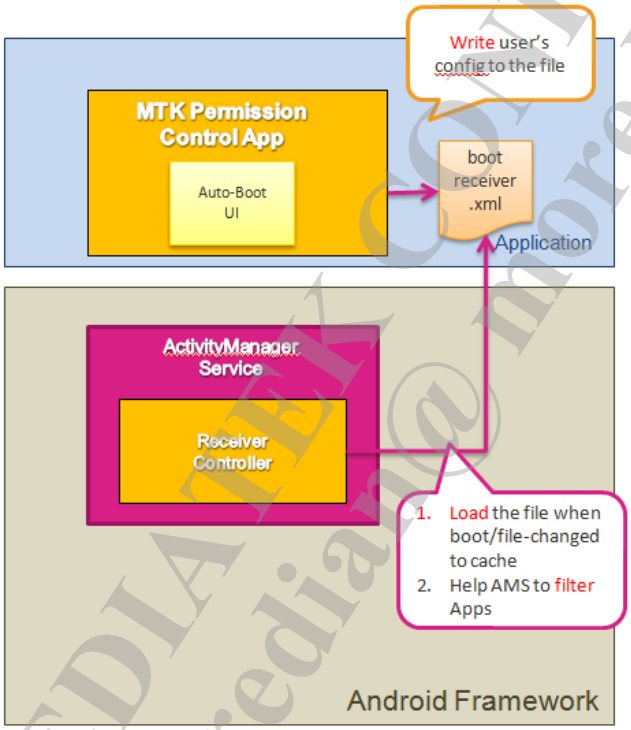
4.1.3 Subordinates

Directly call by settings through plug-in.

4.1.4 Dependencies

AutoBootManager, an class help AutoBootActivity to manager bootreceiver.xml

4.1.5 Processing



1. When boot, ReceiverController will start to load the configurations from bootreceiver.xml
2. ReceiverController will send intents to apps except the 3rd party apps recorded in the config-file .
3. User can control the 3rd party apps to auto-boot or not in the UI.
4. AutoBoot app will write the configuration to the bootreceiver.xml.

5. AutoBoot app is completely independent from the service part.

There are 2 important files in this architecture :

1. /data/system/bootreceiver.xml
   - save packages' Auto Boot Control settings
   - if there is not any package that has been denied to receive intent, this file will not exist.
2. config.xml
   - **path :** vendor/mediatek/proprietary/frameworks/base /res/res/values/
   - **Purpose :**
     - ➢ To customers, let them can customize the monitored intent list
     - ➢ To AutoBoot modules, we will ask PMS "which 3rd party apps we want to control" , so we need this intent list.

```
 <!-- Intent names which are controlled by AutoBootControl for CTA spec.  -->
<string-array name="config_auto_boot_policy_intent_list" translatable="false">
    <item>android.intent.action.BOOT_COMPLETED</item>
    <item>android.intent.action.ACTION_BOOT_IPO</item>
</string-array>
```

   - **Usage :**

```
String[] intentList = mContext.getResources().getStringArray(
                com.mediatek.internal.R.array.config_auto_boot_policy_intent_list);
```

4.1.6 Data

data/data/com.mediatek.security/bootreceiver.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<boot-receiver>
  <pkg u="0" n="com.whty.wicity.china" e="false" />
</boot-receiver>
```

- u : user id
- **n :** package name
- **e** : allowed to receive boot intent or not

4.2 Permission request records

This feature shows permission request history of all apps(include system apps).

4.2.1 Type

Multiple activites

4.2.2 Purpose

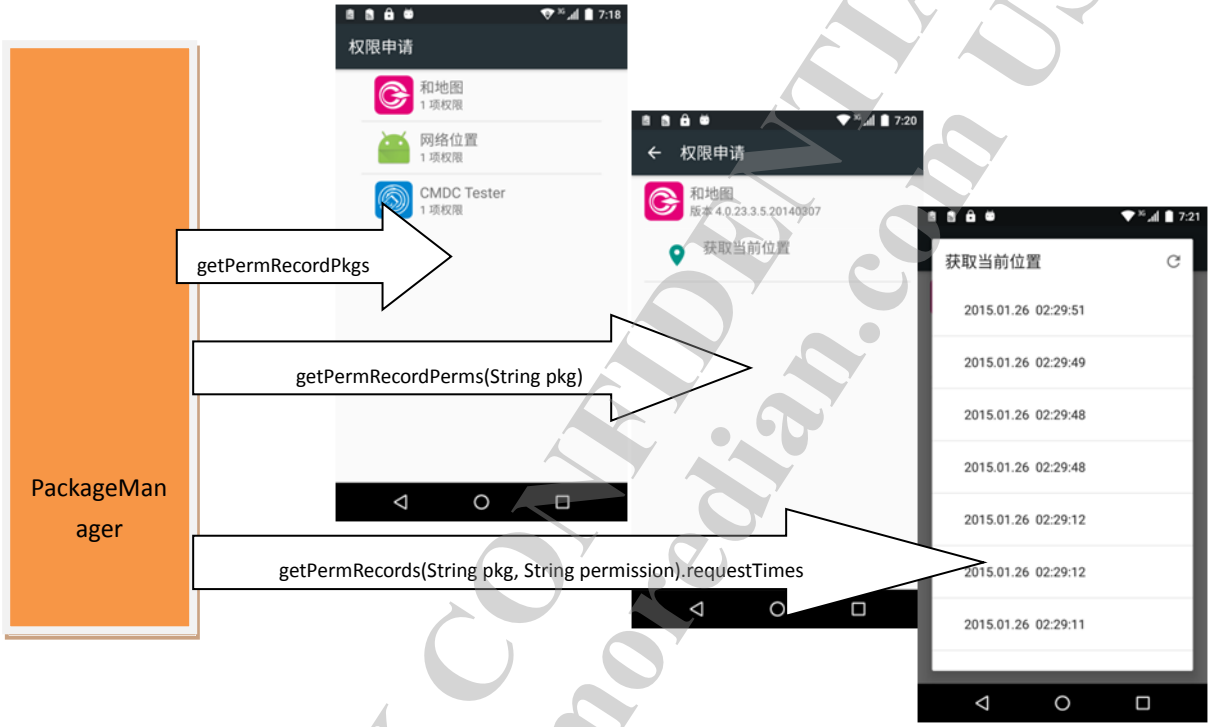
To view permission called records of apps.

4.2.3 Dependencies

PackageManager, the activity will obtain records data from PackageManager.

4.2.4 Processing

- Get these directly from PackageManager



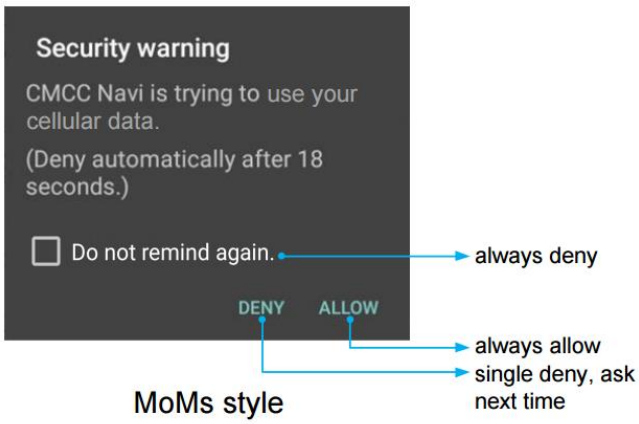
4.3 Cellular data control

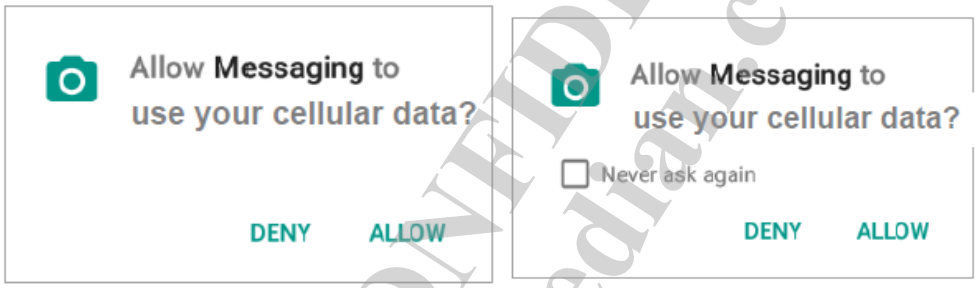
This feature manager which 3th party apps can use cellular data.

1. Add a new entrance in “More” menu in Data usage page for app

Figure 1

Figure 2





Android N style
Use following different style for android N and MoMs.

1st time popup：no checkbox

2nd time popup：with checkbox

4.3.1 Type

Activity, service, database

4.3.2 Purpose

Manager which 3th party apps can use cellular data.

4.3.3 Dependencies

PermControlService

- Init database when boot complete
- Receive cellular data denied broadcast and show dialog to notify user

- Send broadcast to UI when installed packages has been changed

DatabaseHelper

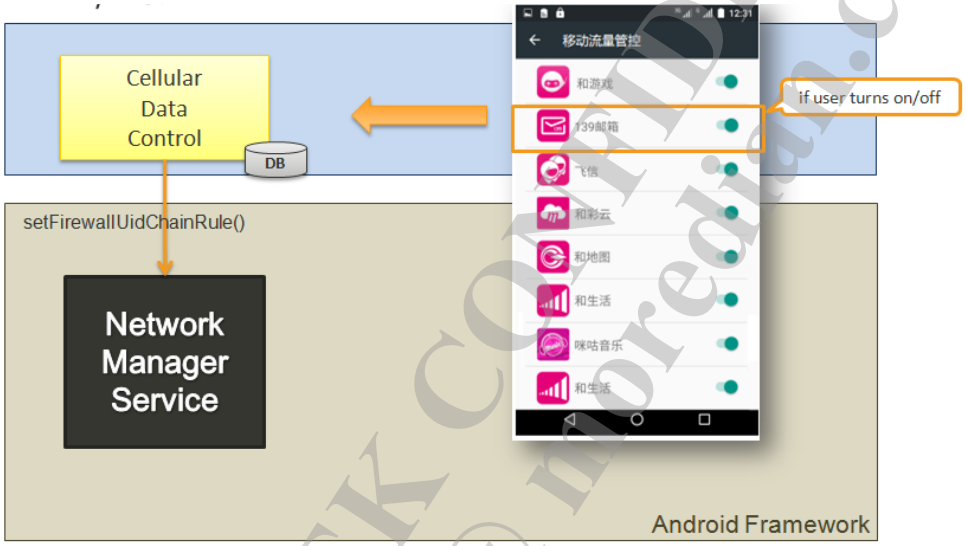
The database saves the application’ s access ability of cellular data.

DatabaseManager

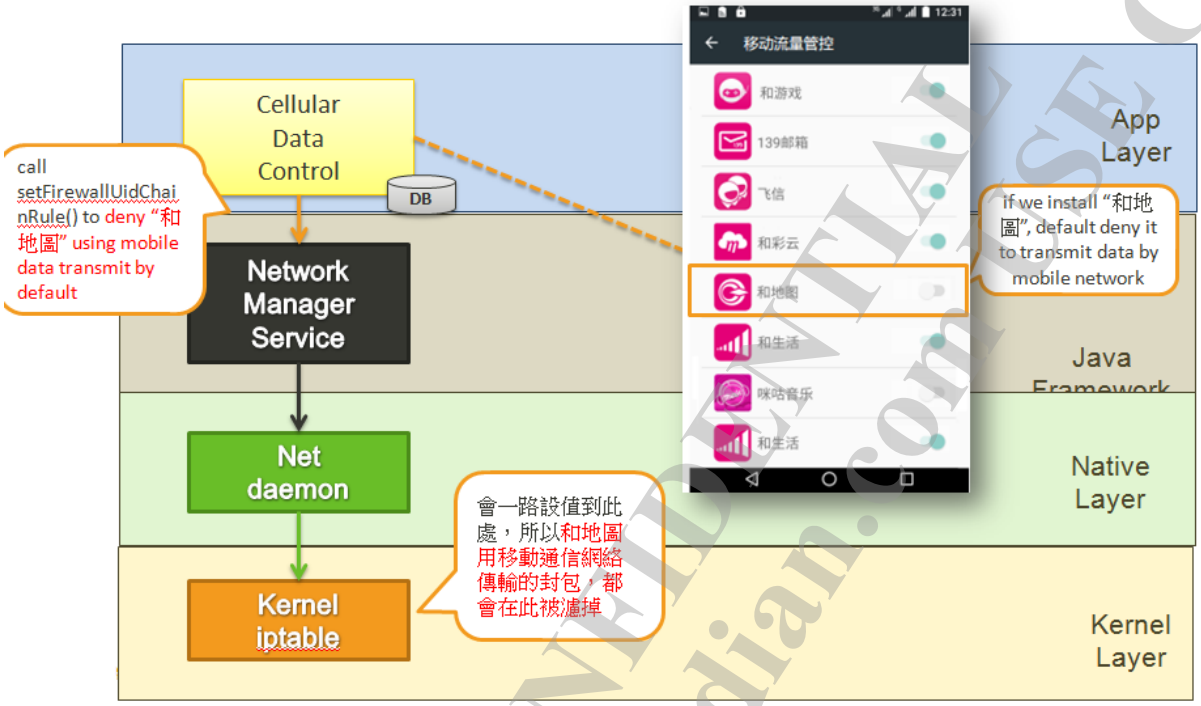
Proxy of DatabassHelper.

4.3.4 Processing

- Save the application’ s ability to access cellular data in database.



- Set ability to framework
  - When first boot up,or install a new app, Cellular Data Control app will set these Apps “cellular data control” to denied as default.



- Receive cellular data denied broadcast
  - When Network manager service received a net daemon that something want to use network，it will notify Cellular Data Control app that "和地圖"'s network access will be denied by send a broadcast，and Cellular Data Control App will pop up a dialog to notify user.
  - When Cellular Data Control App receive the broadcast
    - Check in database about "和地图"'s setting.
    - Found "和地图"'s cellular data has been set to false，and it will failed when try to access network, so pop up a dialog to notify user.

4.3.5 Data

Since directly access the data base is a time consuming process, therefore there will a cache for outside to access the actual cellular data status for different installed applications.

There is one cache designed in which are Map format. The cache map's key is package name. Their values are a list data with CheckedPermRecord data type.

To query the data for a specific package

CheckedPermRecord *record = DatabaseManager.getCellularDataRecord(String pkgName);*

To query all installed package that under permission controlled

List< CheckedPermRecord *> permsList = DatabaseManager.getCellularPerm();*

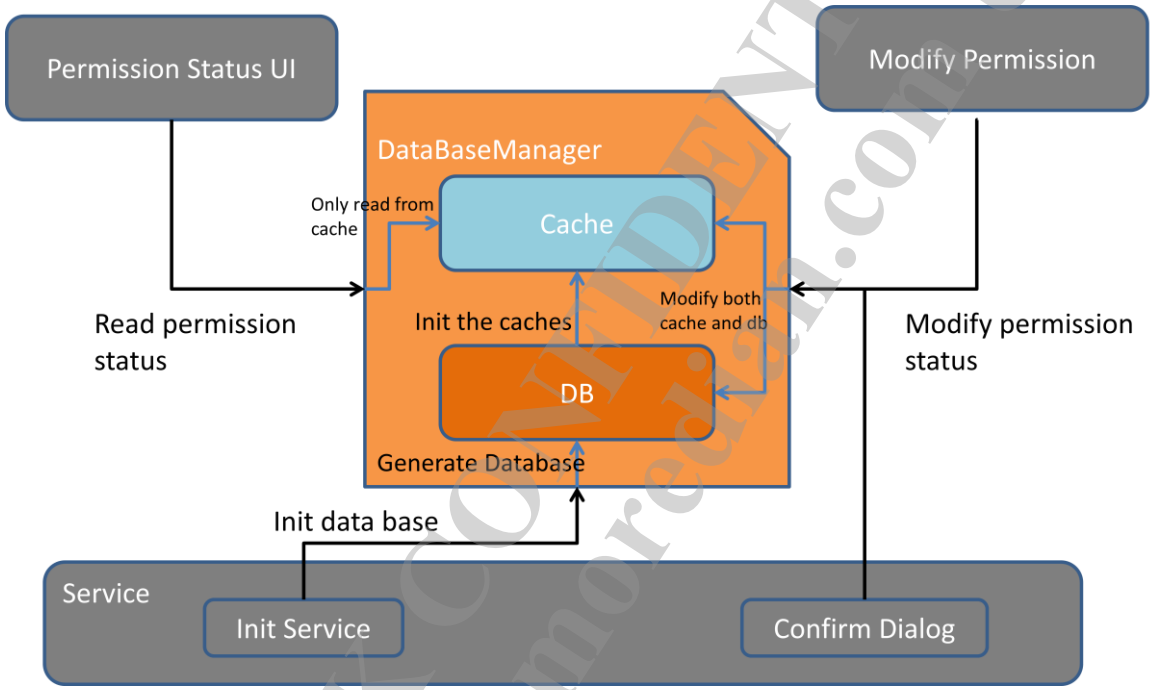


Figure 18 Data Access Process

4.3.5.1 Database design

Database is under folder /data/data/com.mediatek.security/databases/permission_contorl.db, there are three tables in the database. Table package_permission storage 3th app' s use cellular data status, it can be grant, ask or delay.

Package_permission	
_id	long
packages_name	text
cellular_data	int