Disable MoMs Temporary for CTS Test

Doc No: DS6000-D1A-DMT-V1.4EN
Version: V1.0
Release date: 2017-03-20
Classification: Internal

Keywords

MoMs, CTS test

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	2017-03-20	Kelly Zhang	Disable MoMs temporary for CTS test

Table of Contents

Document Revision History **3**
Table of Contents **4**
1 Disable MoMs Temporary for CTS Test **5**
1.1 MoMS 5
1.2 Purpose 5
1.3 Disable MoMS SOP 5
2 Android M Runtime Permission **7**
2.1 Runtime Permission Introduction 7
2.2 User Scenario 7
2.2.1 App Installation 7
2.2.2 Ask Permissions 8
2.2.3 Revoke Permission 9
2.3 Example 9
2.4 Runtime Permission List 10
2.5 Impacts to App 11
3 Mobile Management Service(MoMS) **12**
3.1 CTA 12
3.2 MoMS Scenario 12
4 Comparison **13**
4.1 App Permission Architecture 13
4.2 MoMS Architecture 14
4.3 Difference between App Permission and MoMS architecture 14
4.4 Current Solution When CTA Option is Enabled 15
4.5 Commit info 15

1 Disable MoMs Temporary for CTS Test

1.1 MoMS

MoMS is the abbreviation of Mobile Manager Service.
Ministry of Industry and Information Technology(MIIT) YDT 2407-2013 required that intelligent terminal(IT) must pass the authentication of CTA (Chia-Type-Approval) than the IT can be sold in mainland China.
MoMs is MTK's in-house solution for CTA:

Figure 1-1. The security sign of mobile IT.

1.2 Purpose

The version of Android M put forward a feature named "Runtime permission feature". It's behavior is like MoMS. But the design idea is complete different, so they can not merge together perfectly.
The policy is designed after Check with the chief:

Project for China market : enable MoMS, disable Runtime Permission;

Project for World-wide(non-China) market : enable MoMS, disable Runtime Permission;

Whether the load support CTA MoMS feature is decided with feature option when build time.

1.3 Disable MoMS SOP

Because of the CTS has relevant test cases for runtime permission. And if enable MoMS will lead to CTS test fail. Now, put forward a set of SOP to make sure CTS test can process smoothly. The SOP is let QA disable MoMS feature temporary before CTS test.
The detail is below:
Only switch enable/disable MoMS on engineering mode without burning new load.
Actually, if the load will do not sold in mainland China or your company have your own solution, you can close MoMS feature option in build config directly.

1 Disable MoMs Temporary for CTS Test

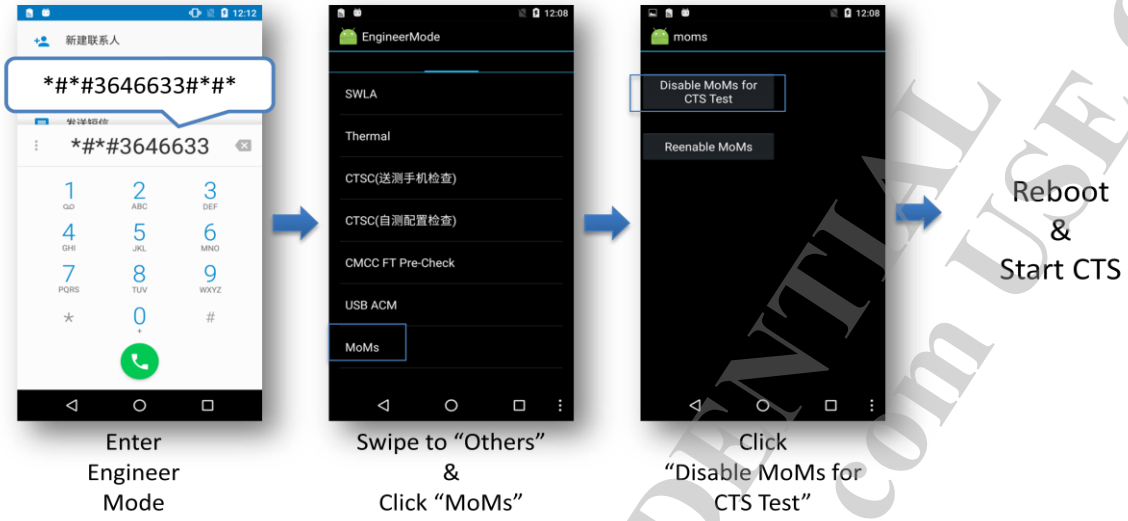

Figure 1-2. Enable or disable MoMS in engineering mode.

The SOP is for CTS test, if you load do not sold in mainland China, please close CTA function directly by feature option.

MTK_CTA_SET
MTK_MOBILE_MANAGERMENT
MTK_PERMISSION_CONTROL, etc

2 Android M Runtime Permission

2.1 Runtime Permission Introduction

If an app on M supports this new permissions model, users do not have to grant any permissions when they install or upgrade the app.
The app requests permissions as needed.
Users may also alter these settings later in the Settings -> Apps menu by selecting an app and then clicking on Permissions.

2.2 User Scenario

2.2.1 App Installation

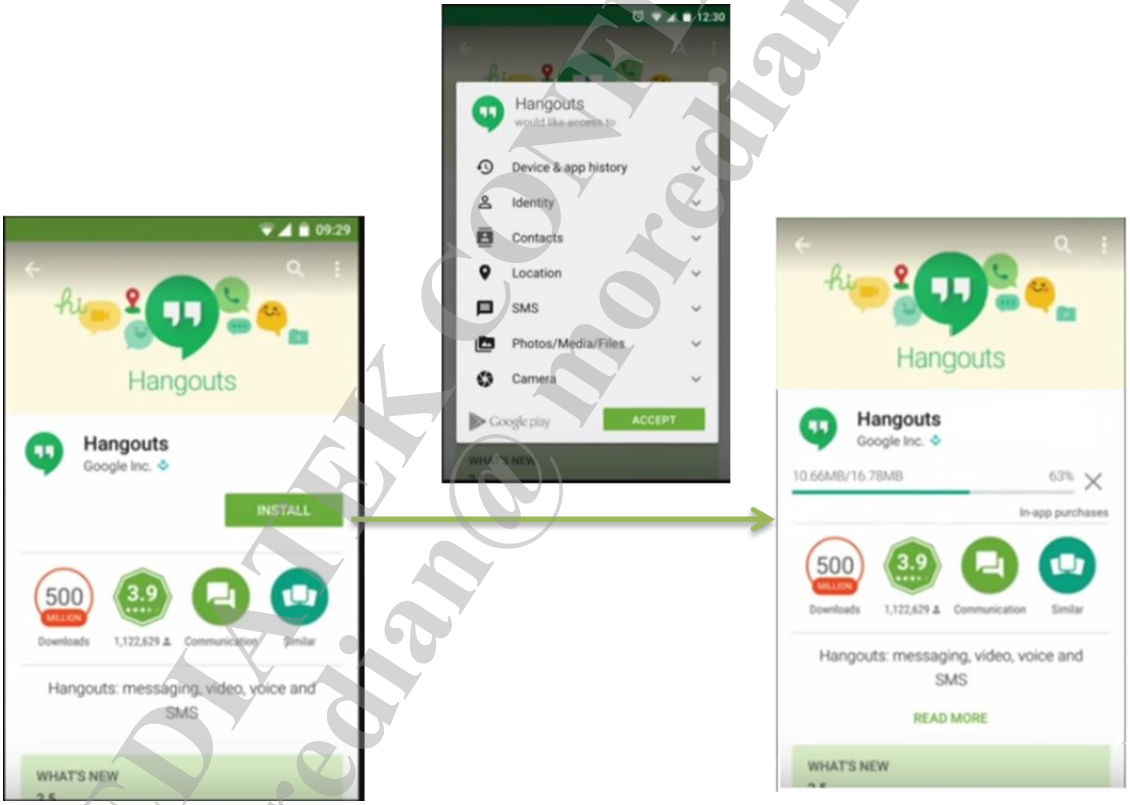

Figure 2-1. No need to grant permissions on installing an app target on M.

2.2.2 Ask Permissions

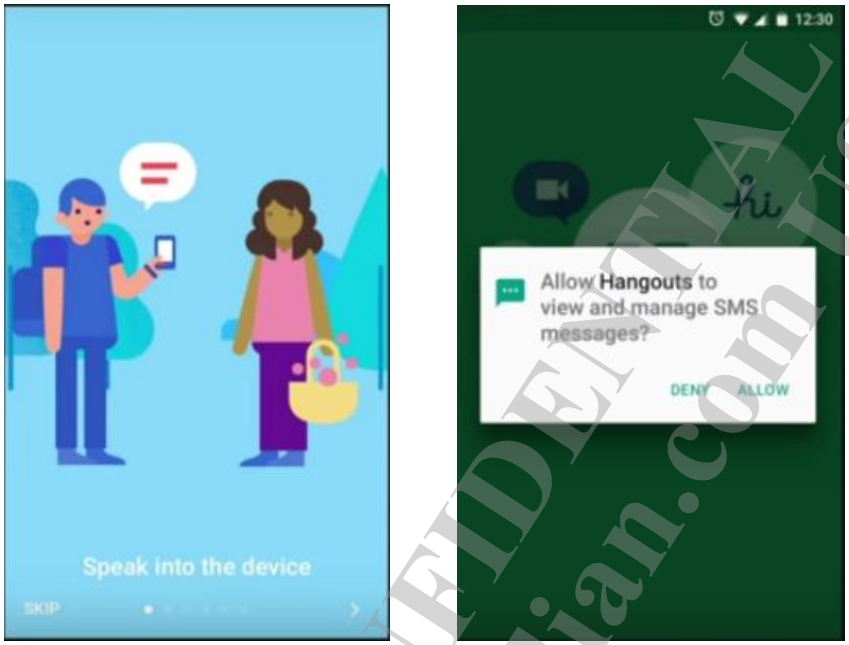

Figure 2-2. Request critical permissions at first launch.

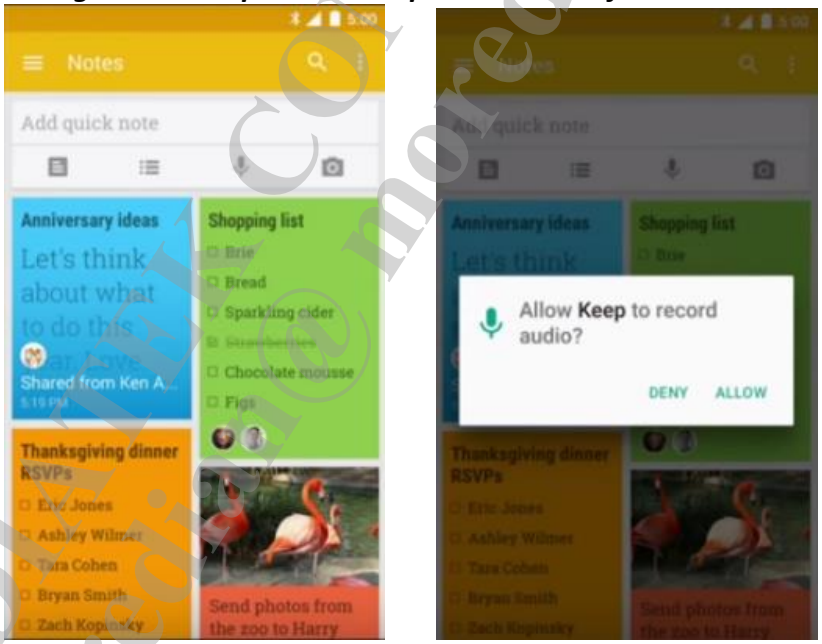

Figure 2-3. Request permission when a feature is invoked.

2.2.3 Revoke Permission

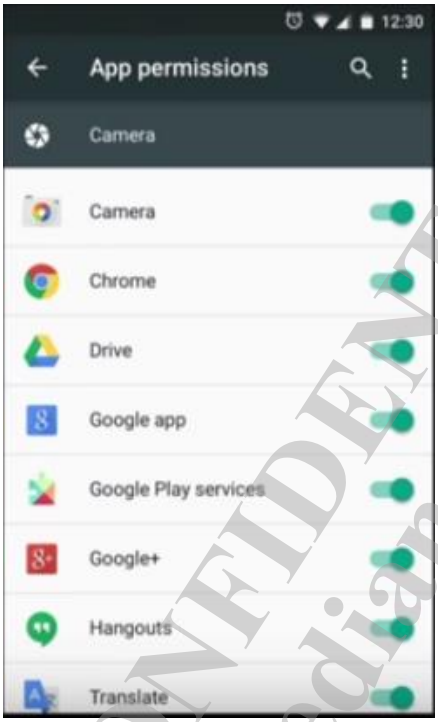

Figure 2-4. Runtime permission setting for one app.

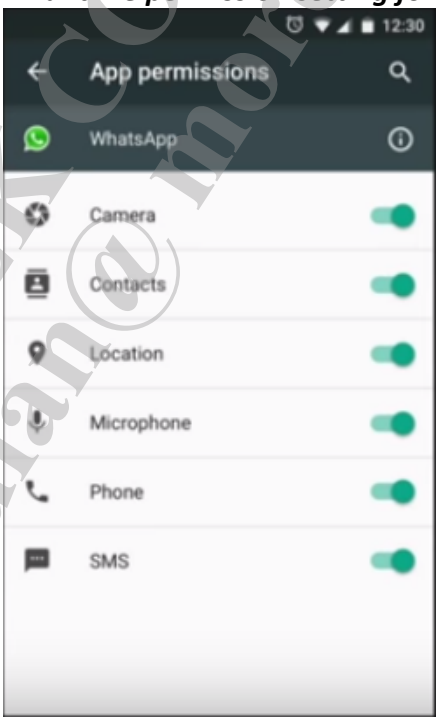

Figure 2-5. Runtime permission setting for a permission group.

2.3 Example

Critical runtime permission default on. (only for system core apps)

When turned off

Ask most of permissions when entered if critical permission is turned off.

Exit app if critical permission is not granted. (even some permissions were granted)

Exit app immediately if never ask again is checked.

Other permissions are requested when required.

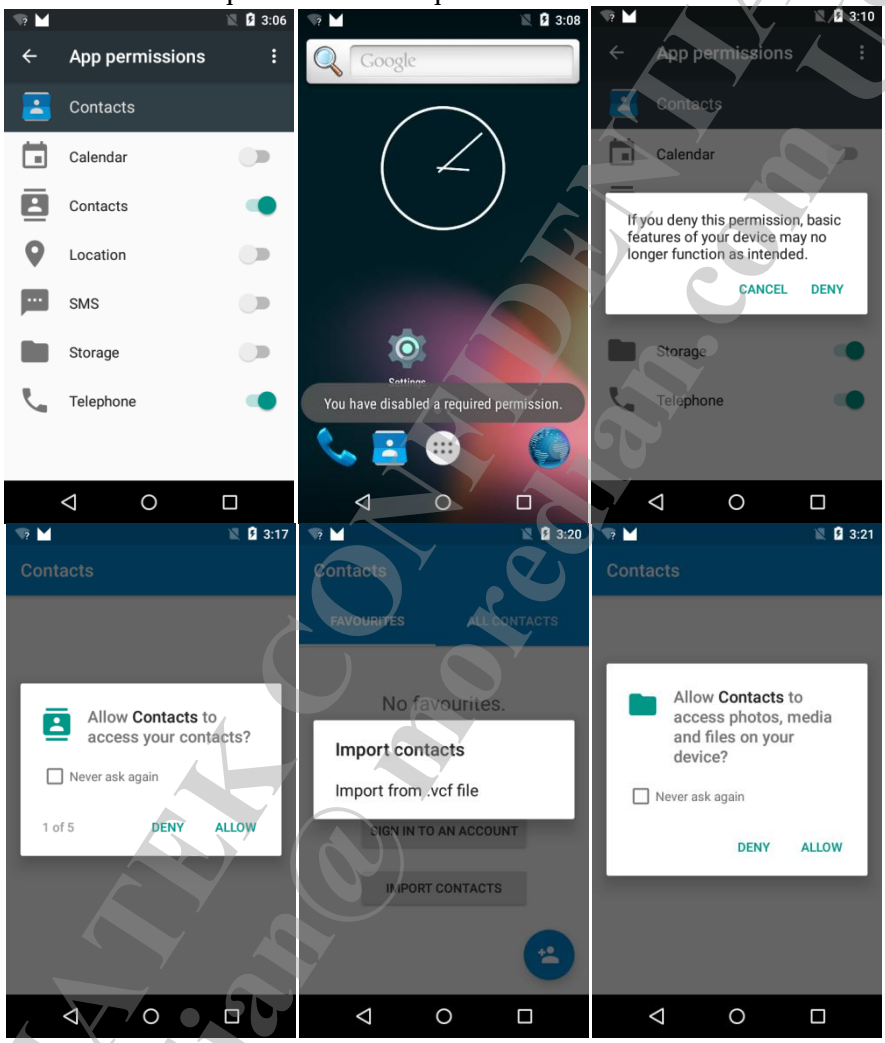

Figure 2-6. Detail oprations of example.

2.4 Runtime Permission List

There are 9 groups and total 25 dangerous permissions:

Permission Group	Permissions
android.permission-group.CALENDAR	• android.permission.READ_CALENDAR • android.permission.WRITE_CALENDAR
android.permission-group.CAMERA	• android.permission.CAMERA
android.permission-group.CONTACTS	• android.permission.READ_CONTACTS • android.permission.WRITE_CONTACTS • android.permission.GET_ACCOUNTS
android.permission-group.LOCATION	• android.permission.ACCESS_FINE_LOCATION • android.permission.ACCESS_COARSE_LOCATION
android.permission-group.MICROPHONE	• android.permission.RECORD_AUDIO
android.permission-group.PHONE	• android.permission.READ_PHONE_STATE • android.permission.CALL_PHONE • android.permission.READ_CALL_LOG • android.permission.WRITE_CALL_LOG • com.android.voicemail.permission.ADD_VOICEMAIL • android.permission.USE_SIP • android.permission.PROCESS_OUTGOING_CALLS
android.permission-group.SENSORS	• android.permission.BODY_SENSORS
android.permission-group.SMS	• android.permission.SEND_SMS • android.permission.RECEIVE_SMS • android.permission.READ_SMS • android.permission.RECEIVE_WAP_PUSH • android.permission.RECEIVE_MMS • android.permission.READ_CELL_BROADCASTS
android.permission-group.STORAGE	• android.permission.READ_EXTERNAL_STORAGE • android.permission.WRITE_EXTERNAL_STORAGE

Figure 2-7. Dangerous permissions and groups.

2.5 Impacts to App

App needs to handle situations that some permissions may be revoked at runtime.

To handle such changes:

UI behavior may need to be redesigned.Code modifications to check and request runtime permissions.There are 42 MTK apps that have to do relevant changes.

3 Mobile Management Service(MoMS)

3.1 CTA

Level 1 focuses on user confirmation

Level 1 is mandatory for CTA certification

Level1~5 define permission(s) to monitor

Total 21 permissions

The key point of CTA identification:
User confirmation
Check permissions one by one
Apply to all 3rd party apps

Table 3-1. CTA Level and Key Feature

CTA Level	Key Feature
Level 1 ~ 5	App Permission Request Record
Level 3	Auto-boot Control Mobile Security

3.2 MoMS Scenario

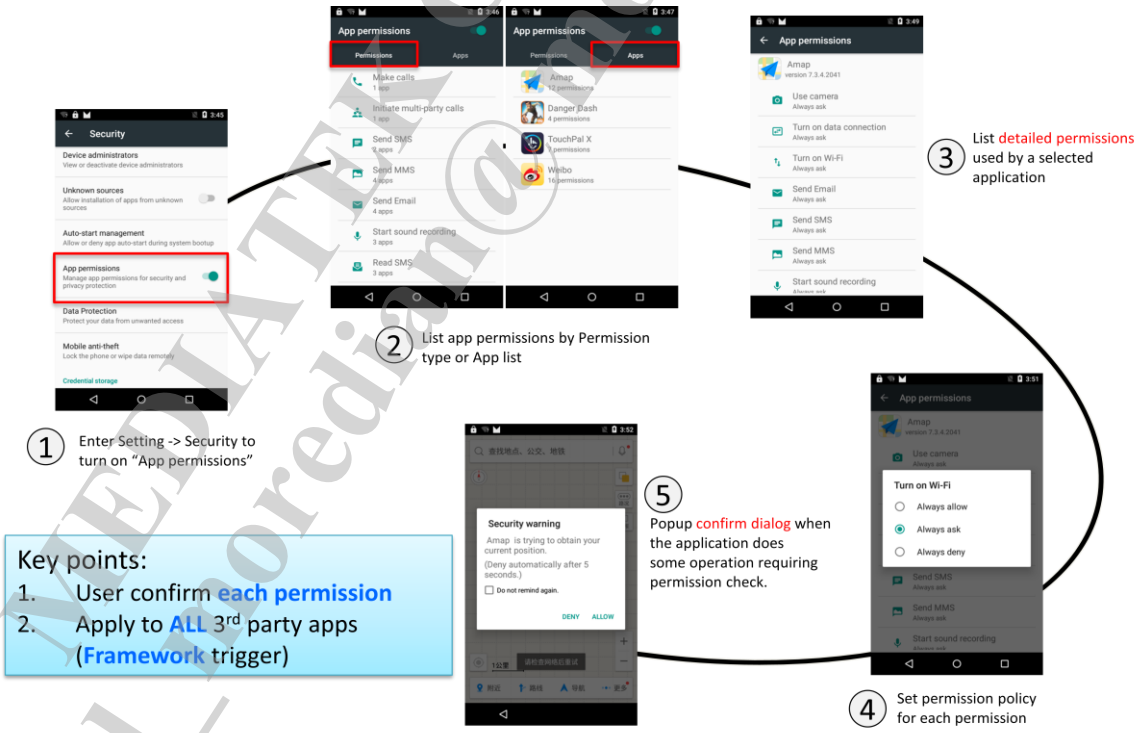

Figure 3-1. MoMS Use Scenario.

4 Comparison

4.1 App Permission Architecture

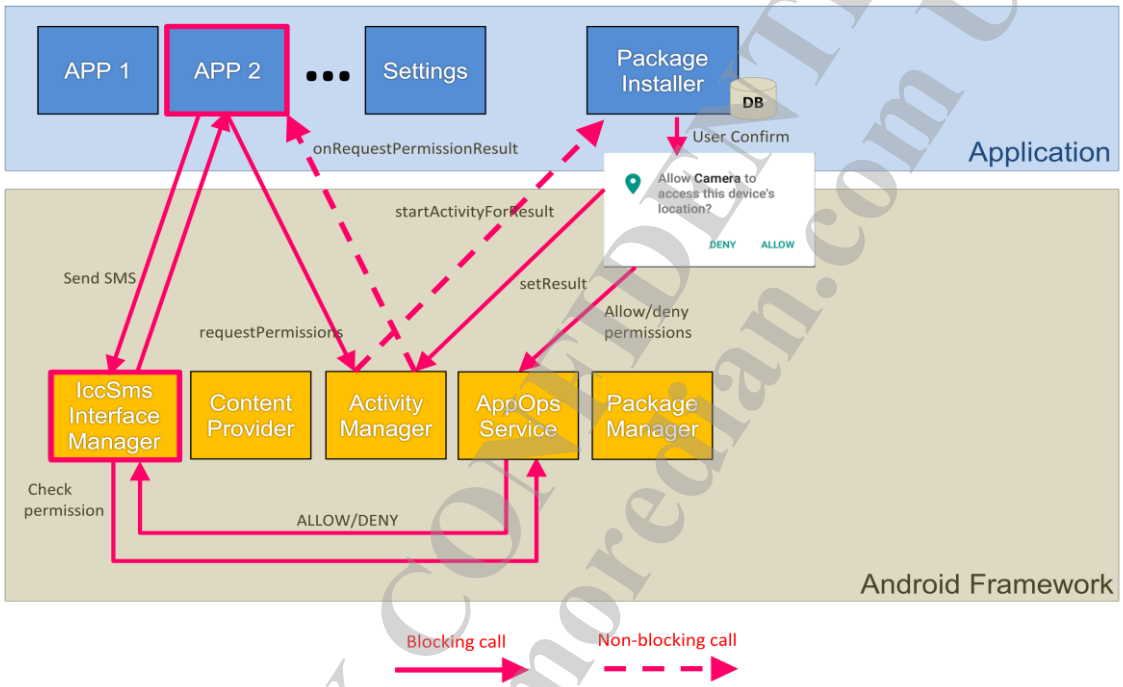

Figure 4-1. App Permission Architecture.

4.2 MoMS Architecture

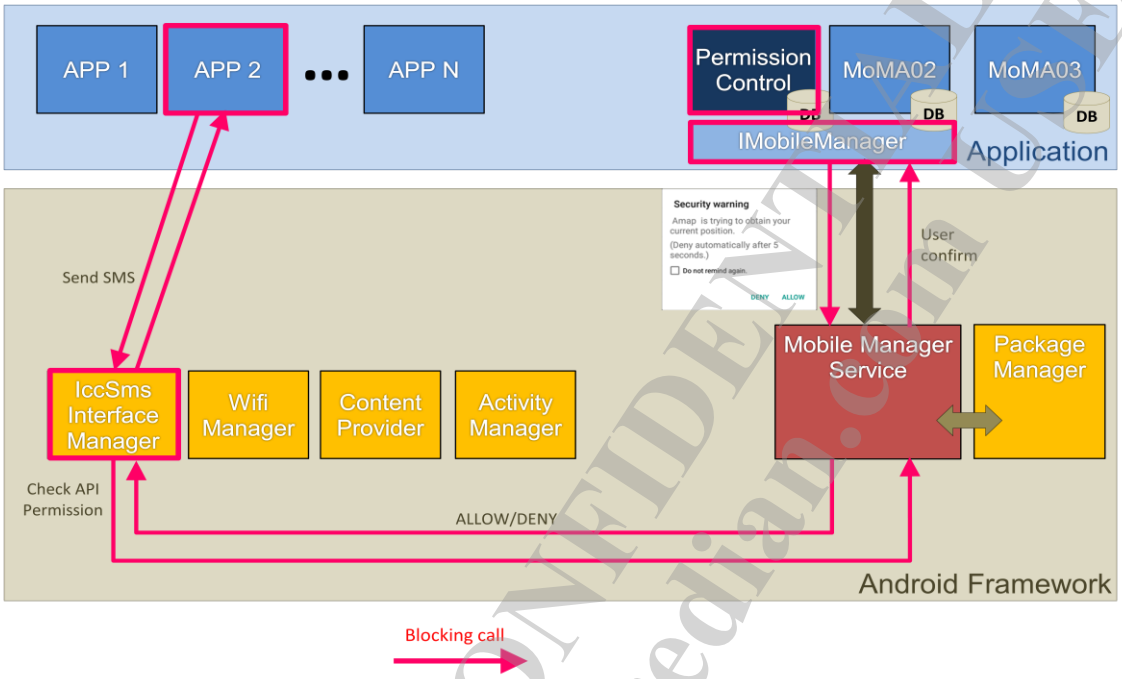

Figure 4-2.MoMS Architecture.

4.3 Difference between App Permission and MoMS architecture

Table 4-1. Contrast between App Permission and MoMS

		M App Permission	MoMS
UE	Permission Control	9 permission groups	21 permission items
	Settings	By permission group By App	By permission type By app list
Design	Popup confirm dialog	App trigger: App should request permission(s) explicitly	Framework trigger: App does not need to modify
	Permission handling	App should have error handling if a permission is denied	FW should have error handing if a permission is denied
CTA Requirements	User confirmation	Compliance: Partial App designed for M : Partial Legacy app : No	Compliance: Yes App designed for M : Yes Legacy app : Yes
	Check permission one by one	Compliance : No	Compliance : Yes
	Apply to all 3rd party apps	Compliance: No App designed for M : Partial Legacy app : No	Compliance : Yes

4.4 Current Solution When CTA Option is Enabled

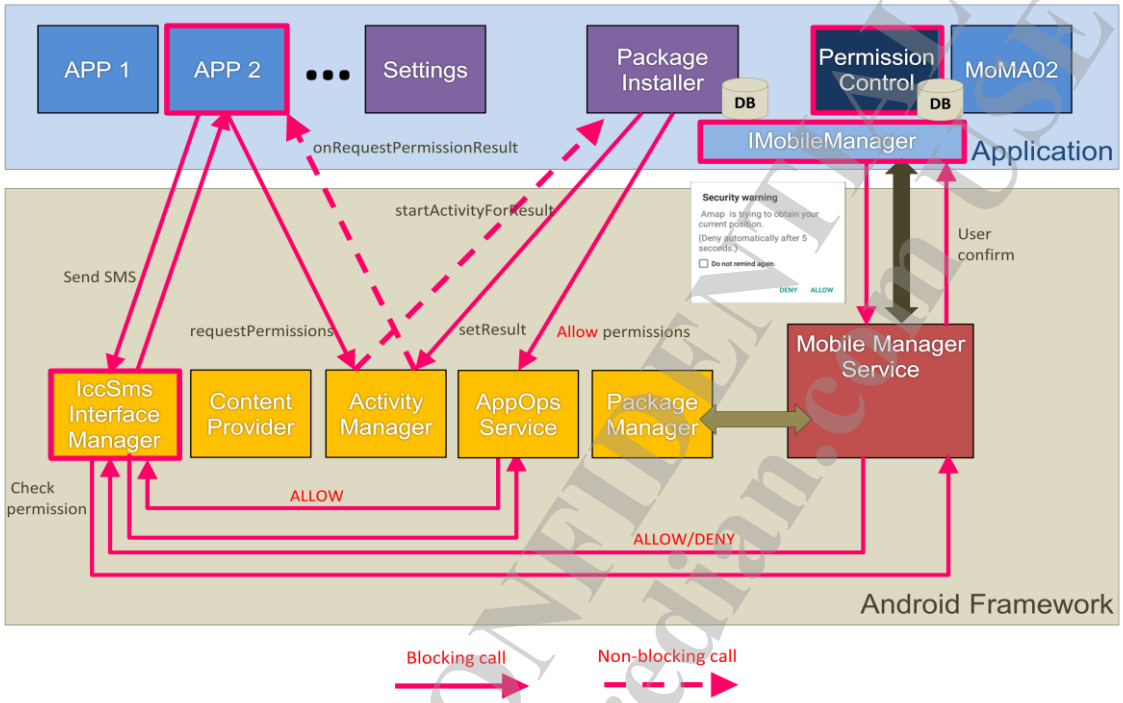

Figure 4-2.Current Solution for CTA Permission Feature.

4.5 Commit info

Included info

[Change-Id] I525d3861b47346fd9dfa01d45bfb10e155e950e7