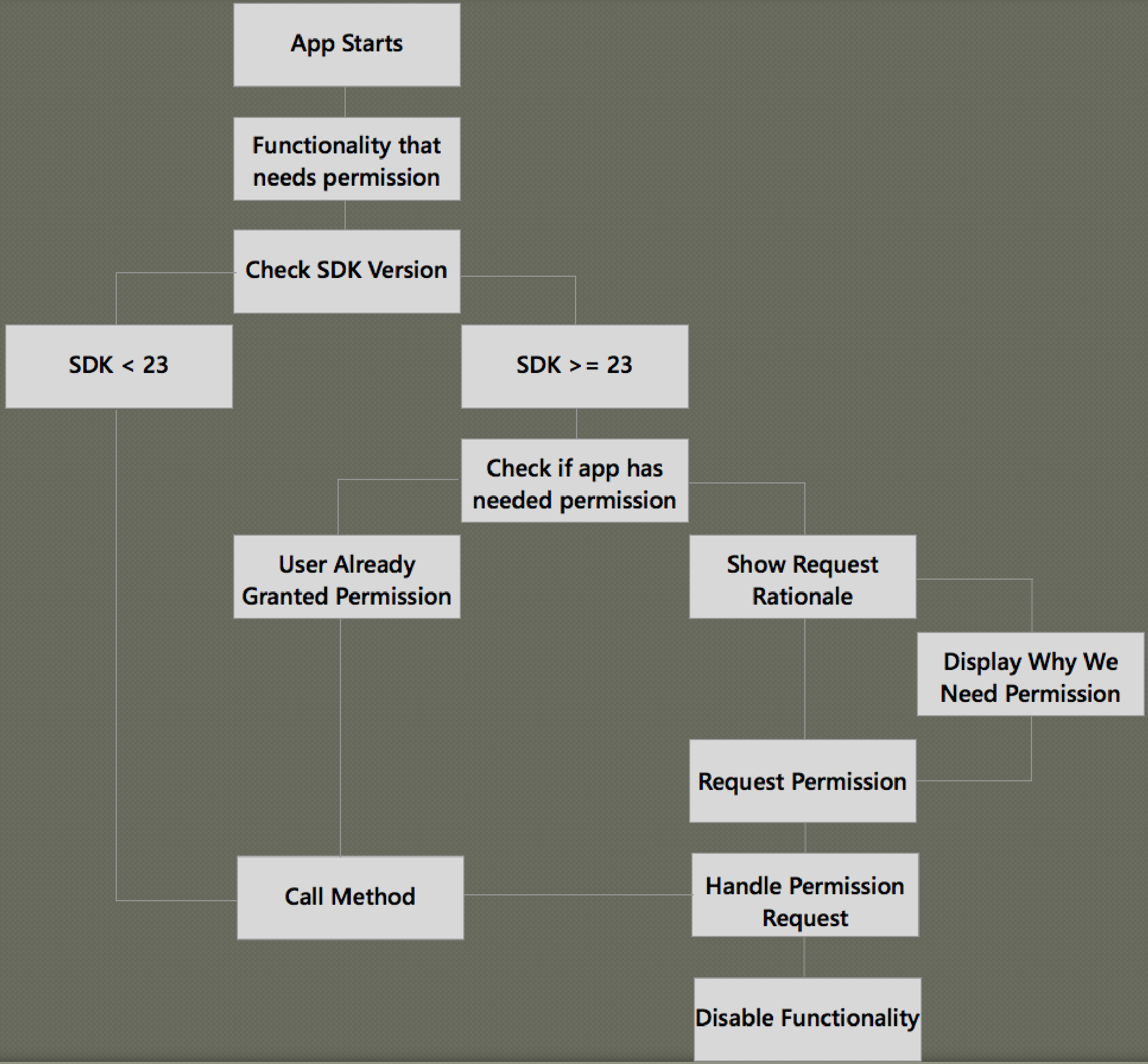
Android >=M Runtime Permissions



App Starts

Functionality that needs permission

Check SDK Version

SDK < 23

SDK >= 23

Check if app has needed permission

User Already Granted Permission

Show Request Rationale

Display Why We Need Permission

Request Permission

Call Method

Handle Permission Request

Disable Functionality

Key methods

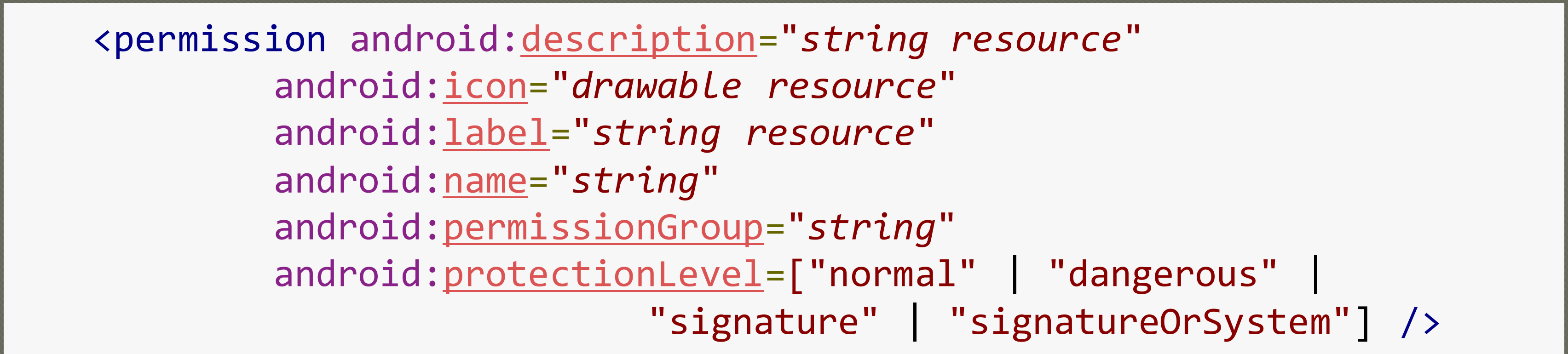
- checkSelfPermission
- requestPermissions
- onRequestPermissionsResult

Permissions

- If an app requests a dangerous permission listed in its manifest, and the app already has another dangerous permission in the same permission group, the system immediately grants the permission without any interaction with the user.
- For example, if an app had previously requested and been granted the READ_CONTACTS permission, and it then requests WRITE_CONTACTS, the system immediately grants that permission.

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

<permission>



```
    <permission android:description="string resource"
            android:icon="drawable resource"
            android:label="string resource"
            android:name="string"
            android:permissionGroup="string"
            android:protectionLevel=["normal" | "dangerous" |
                              "signature" | "signatureOrSystem"] />
```

android:protectionLevel = normal

- The default value. A lower-risk permission that gives requesting applications access to isolated application-level features, with minimal risk to other applications, the system, or the user. The system automatically grants this type of permission to a requesting application at installation, without asking for the user's explicit approval (though the user always has the option to review these permissions before installing).

android:protectionLevel = dangerous

- A higher-risk permission that would give a requesting application access to private user data or control over the device that can negatively impact the user. Because this type of permission introduces potential risk, the system may not automatically grant it to the requesting application. For example, any dangerous permissions requested by an application may be displayed to the user and require confirmation before proceeding, or some other approach may be taken to avoid the user automatically allowing the use of such facilities.

android:protectionLevel = signature

- A permission that the system grants only if the requesting application is signed with the same certificate as the application that declared the permission. If the certificates match, the system automatically grants the permission without notifying the user or asking for the user's explicit approval.

android:protectionLevel = signatureOrSystem

- A permission that the system grants only to applications that are in the Android system image *or* that are signed with the same certificate as the application that declared the permission. Please avoid using this option, as the signature protection level should be sufficient for most needs and works regardless of exactly where applications are installed. The "signatureOrSystem" permission is used for certain special situations where multiple vendors have applications built into a system image and need to share specific features explicitly because they are being built together.