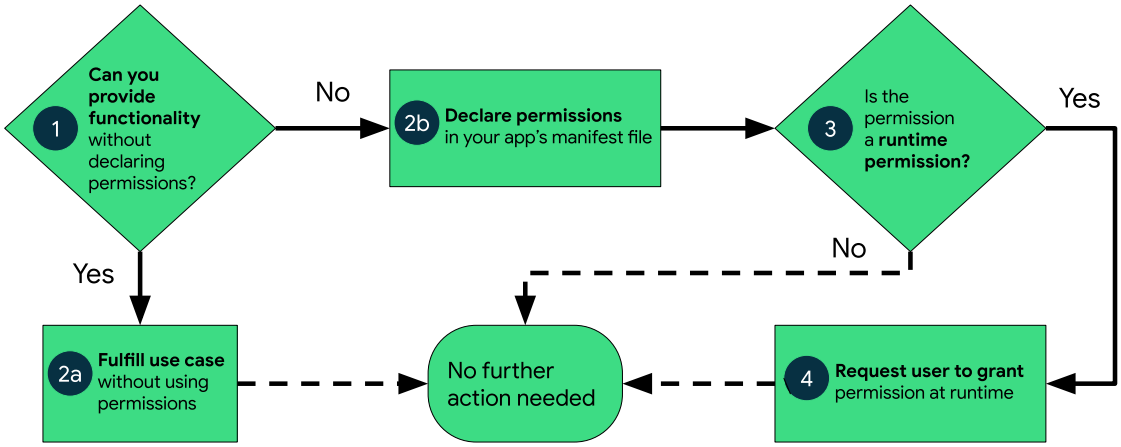
Android权限介绍

应用权限有助于保护对以下数据的访问和对以下操作的执行，从而为保护用户隐私提供支持：

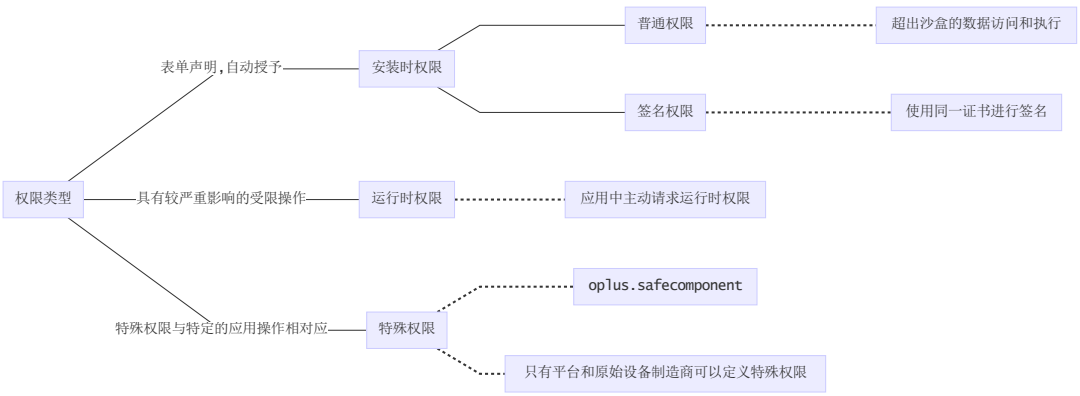
- **受限数据**，例如系统状态和用户的联系信息。
- **受限操作**，例如连接到已配对的设备并录制音频。



在 Android 中使用权限的概要工作流示意图。

组件服务运行在Android Runtime(沙箱)中, 其访问Android的数据范围或是执行操作范围是受限制的.

Android 将权限分为不同的类型，包括安装时权限、运行时权限和特殊权限。每种权限类型都指明了当系统授予应用该权限后，应用可以访问的受限数据范围以及应用可以执行的受限操作范围。



权限不仅仅用于请求获取系统功能的使用权。您还可以限制其他应用与您的应用组件交互的方式。

限制与应用的服务的交互

使用 `android:permission` 属性应用于清单中 `` 标记的权限可限制谁能启动或绑定到关联的 `Service`。系统会在 `Context.startService()`、`Context.stopService()` 和 `Context.bindService()` 期间检查该权限。如果调用方没有所需的权限，将会发生 `SecurityException`。

检查权限：

- 在调用某项服务期间，将权限字符串传入 `Context.checkCallingPermission()`。此方法会返回一个整数，指示当前调用进程是否已获授权限。请注意，仅在执行从另一个进程传入的调用（通常是通过从服务发布的 IDL 接口或提供给另一进程的某种其他方式来实现）时，才可使用此方法。
- 如需检查另一进程是否已获得特定权限，请将该进程 (PID) 传入 `Context.checkPermission()`。
- 如需检查另一软件包是否已获得特定权限，请将该软件包的名称传入 `PackageManager.checkPermission()`。