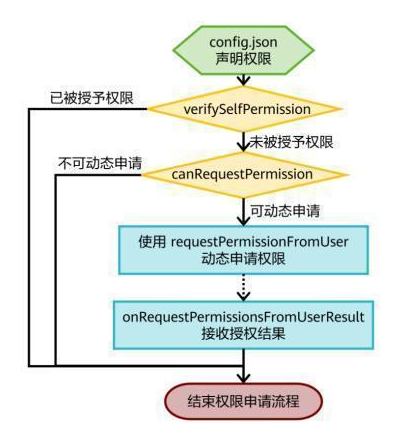
* HarmonyOS 中所有的应用均在应用沙盒内运行。默认情况下，应用只能访问有限的系统资源，系统负责管理应用对资源的访问权限
* 应用权限管理是由接口提供方 (Ability) 、接口使用方（应用）、系统（包括云侧和端侧）以及用户等多方共同参与的整个流程，保证受限接口是在约定好的规则下被正常使用，避免接口被滥用而导致用户、应用和设备受损
* 权限使用原则：
  + 权限申请最小化：
    - 不申请跟用户提供的功能无关的权限
    - 尽量采用无需权限的操作来实现相应功能
  + 权限申请完整：应用所需权限都要逐个在应用config.json配置文件中按格式声明
  + 满足用户可知：应用申请敏感权限的目的需要告知客户
  + 权限就近申请：应用在用户触发相关业务功能时，就近提示用户授予实现此功能所需的权限
  + 权限不扩散：在用户未授权的情况下，不允许提供给其他应用使用
  + 应用自定义权限防止重名：建议以包名为前缀来命名，防止跟系统定义的权限重名
* 权限声明
  + 应用在config.json中使用“reqPermissions”属于对需要的权限逐个进行声明
  + 若使用到第三方库也涉及权限使用，也需统一在应用的config.json中逐个声明
  + 没有在config.json中声明的权限，应用无法获得此权限的授权
* 敏感权限-动态申请
  + 敏感权限基于用户可知可控的原则，需要应用在运行时主动调用系统动态申请权限的接口，系统弹窗由用户授权
  + 敏感权限需要应用动态申请，通过运行时发送弹窗的方式请求用户授权，该类权限的授权方式为用户授权（user\_grant）
  + 即使用户向应用授予了请求的权限，应用在调用受此权限管控的接口前，也应该先检查自己有无此权限，而不能把之前授予的状态持久化，因为用户在动态授予后还可以通过设置取消应用的权限
  + 敏感权限的申请需要按照动态申请流程向用户申请授权，常用的敏感权限包括：
    - 位置
    - 相机
    - 麦克风
    - 日历
    - 健身运动
    - 健康
    - 分布式数据管理
    - 媒体
  + 通讯录属于受限权限，在动态申请前，还需申请权限证书
  + 敏感权限的申请流程如下图



* 非敏感权限
  + 已在config.json文件中声明的非敏感权限，会在应用安装时自动授予，该类权限的授权方式为系统授权（system\_grant）
  + 非敏感权限需要在config.json文件中的“reqPermissions”字段中声明
  + 访问网络需要申请 ohos.permission.INTERNET 权限，该权限非敏感权限，不需要动态申请
* 自定义权限
  + 自定义权限需要在config.json文件中的“defPermissions”字段中自定义所需的权限
    - {
    - "module":{
    - "defPermissions":[
    - {
    - "name":"com.myability.permission.MYPERMISSION",
    - "grantMode":"system\_grant",
    - "availableScope":["signature"]
    - },{
    - …
    - }
    - ]
    - }
    - }
  + HarmonyOS 为了保证应用对外提供的接口不被恶意调用，需要对调用接口的调用者进行鉴权
  + 大多情况下，系统已定义的权限满足了应用的基本需要，若有特殊的访问控制需要，应用可在 config.json 中以"defPermissions": []属性来定义新的权限，并通过 availableScope 和grantMode 两个属性分别确定权限的开放范围和授权方式，使得权限定义更加灵活且易于理解
  + 为了避免应用自定义新权限出现重名的情况，建议应用对新权限的命名以包名的前两个字段开头，这样可以防止不同开发者的应用间出现自定义权限重名的情况
* 权限保护方法
  + 保护 Ability
    - 通过在 config.json 里对应的 Ability 中配置"permissions": ["权限名"]属性，即可实现保护整个 Ability 的目的，无指定权限的应用不能访问此 Ability
  + 保护 API
    - 若 Ability 对外提供的数据或能力有多种，且开放范围或保护级别也不同，可以针对不同的数据或能力在接口代码实现中通过 verifyPermission(String permissionName, int pid, int uid)来对 uid 标识的调用者进行鉴权
* 使用verifySelfPermission()方法可以判断当前应用是否已获得特定权限授权