ICS 33.050
M 30

团 体 标 准

T/TAF 076-2020

移动终端权限申请目的说明实施指南

Mobile intelligent terminal permission application purpose description implementation guide

2020－11－26 发布　　2020－11－26 实施

电信终端产业协会 发布

目　　次

前言 II
引言 III
1 范围 1
2 术语、定义和缩略语 1
2.1 术语和定义 1
3 权限申请目的告知具体要求 1
3.1 权限申请目的展示时机和方式 1
3.2 实现方式 2
3.3 权限申请目的内容要求 2
3.4 安卓系统展示申请目的的敏感权限及权限组对照关系 2
3.5 适配要求 3
附录 A（资料性附录）权限申请目的说明示例 5
附录 B（资料性附录）安卓危险权限权限申请目的告知实现示例 8
附录 C（资料性附录）应用自定义危险权限权限申请目的告知实现示例 9
附录 D（资料性附录）permission_reason_policy 的取值范围 10

前　言

本标准按照 GB/T 1.1-2020 给出的规则起草。

本标准中的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院、华为技术有限公司、OPPO广东移动通信有限公司、维沃移动通信有限公司。

本标准主要起草人：衣强、李腾、贾科、宁华、杜云、胡月、王艳红、李京典、周飞。

引　　言

移动智能终端的普及、以及移动互联网的发展使得移动终端成为日常生活不可获取的部分，这其中涉及大量的个人信息，移动终端上基于权限的管控措施是用户管理个人信息的重要手段，国家对用户个人信息保护高度重视，工信部24号令等多个法律法规、标准规范中明确规定收集使用个人信息时，应明确告知用户收集、使用个人信息的目的，而当前用户终端权限种类多，各应用软件使用目的多种多样，用户很难直接了解权限申请目的，易给用户造成困扰，本规范旨在实现通过操作系统机制申请权限同时告知用户权限申请目的，为移动终端厂商和移动应用软件开发者实现权限申请目的告知提供依据。

移动终端权限申请目的说明实施指南

1 范围

本标准规定了移动终端及其上运行的应用软件基于操作系统机制实现权限申请目的说明的要求和实施指南。

本标准适用于带有操作系统的移动智能终端、运行在移动终端上的应用软件。

2 术语、定义和缩略语

2.1 术语和定义

下列术语和定义适用于本标准。

2.1.1

移动智能终端 smart mobile terminal

移动智能终端是指接入公众移动通信网络、具有操作系统、可由用户自行安装和卸载应用软件的移动终端产品。

2.1.2

移动智能终端应用软件 mobile application

移动智能终端应用软件（以下简称“应用软件”）是指移动智能终端预置以及通过网站、应用商店、扫二维码、应用自身、其他线上线下平台或渠道下载、安装、升级、卸载的应用软件。

2.1.3

敏感权限 sensitive permission

敏感权限对应的数据或资源，涉及下列范围：个人信息或个人敏感信息，一旦泄露、非法提供或滥用可能危害人身和财产安全；对用户存储的数据或其他应用的操作产生影响，可能干扰系统正常运行或实施恶意行为。

3 权限申请目的告知具体要求

应用软件在移动终端上申请敏感权限的情况下，需告知用户其权限申请目的，敏感权限包括涉及到日历、通讯录、通话记录、短信、电话、位置、拍照、录音、传感器、存储、身体活动等个人数据或敏感能力操作的权限。

3.1 权限申请目的展示时机和方式

a） 应用软件运行时申请权限授权的权限申请界面，以文字方式向用户呈现权限申请目的。

b） 应用软件安装完成后的安装器界面，宜以文字方式向用户呈现应用软件的权限申请目的。

c） 移动终端中应用软件的权限管理界面，该界面用于向用户展示权限授权情况和提供授权状态修改选项，在权限管理界面以文字方式向用户呈现应用软件权限申请目的。

3.2 实现方式

若移动终端操作系统支持权限申请目的告知，则应用软件开发者按照操作系统定义的方式下输入权限及权限对应的申请目的。

若移动终端操作系统不支持权限申请目的告知，如安卓系统，应用软件开发者在清单文件中的应用<application>标签下新增自定义元素<meta-data>，在<meta-data>中输入权限及权限申请目的，<meta-data>标签包括name和resource两个属性，其中，name属性为权限名称，resource属性为权限申请目的引用的字符串资源，为避免应用开发者多次适配，name的命名规则统一为“permission.reason.+ 危险权限的权限组名”，resource属性中字符串id不限。

注1：本标准适配安卓API版本号为29及其以上版本。

注2：实现方式示例参考附录B。

3.3 权限申请目的内容要求

3.3.1 对终端厂商的要求

终端厂商提供的权限申请目的展示遵从以下要求：

- 对于安卓系统，在应用软件的权限相关界面，包括权限申请界面界面、安装器界面、或权限管理界面，终端以权限组为粒度展示权限组申请目的。
- 终端默认设置的中文字符情况下，每条权限申请目的字数建议限制为72个字符，支持两行展示；

3.3.2 对应用软件厂商的要求

应用软件厂商在提供权限申请目的时遵从以下要求：

- 所提供的权限申请目的字数符合4.3.1中的要求；
- 基于安卓操作系统开发的应用软件，以权限组粒度展示权限申请目的，即应用软件按照4.2节的实现方式说明每个权限组的申请目的，并说明权限组涉及的子权限。

注1：安卓系统展示申请目的的敏感权限及分组见4.5节。

- 应用自定义危险权限的情况时，若自定义危险权限未指定权限组，则展示权限对应的申请目的；若指定存在的权限组，则展示权限组对应的申请目的；若指定不存在的权限组，则无法展示任何权限申请目的。

注2：应用自定义危险权限的权限申请目的展示示例参考附录C。

- 应用软件申请多个权限或权限组申请应逐一说明每个权限或权限组的申请目的。
- 应用软件申请设备信息权限（安卓系统的READ_PHONE_STATE权限）时，单独呈现申请设备信息的使用目的；

注3：设备信息权限包括读取通话状态、移动网络信息，安卓系统API版本号29之后将不再返回设备标识信息，当系统设置设备信息权限独立于电话权限申请或管理时，则应单独呈现申请设备信息的目的。

- 权限申请目的不应呈现链接；
- 权限申请目的不应呈现虚假目的、以及夸大使用目的、表述不清的描述。
- 应用软件开发者不应在权限申请过程中，通过权限申请目的内容发布广告信息。

3.4 安卓系统展示申请目的的敏感权限及权限组对照关系

权限组	Name属性中的权限组名	子权限
存储权限	android.permission-group.ST	• 读取外部存储内容

	ORAGE	• 修改外部存储内容 • 从媒体收藏中读取位置信息
设备信息权限	android.permission.READ_PHONE_STATE	访问设备信息权限（通话状态和移动网络信息）
拨打电话和管理通话权限	android.permission-group.PHONE	• 打电话 • 继续进行来自其它应用的通话 • 添加语音邮件 • 拨打/接听互联网通话 • 读取电话号码 • 接听来电 • 呼叫转移
位置权限	android.permission-group.LOCATION	• 粗略位置 • 精准位置 • 后台访问位置
相机权限	android.permission-group.CAMERA	使用相机
麦克风权限	android.permission-group.MICROPHONE	使用麦克风
健身运动识别权限	android.permission-group.ACTIVITY_RECOGNITION	健身运动识别
通讯录权限	android.permission-group.CONTACTS	• 读通讯录 • 修改通讯录 • 查找设备上的账户
短信息权限	android.permission-group.SMS	• 发短信 • 接收短信 • 读取短信 • 接收 WAP 信息 • 接收彩信 • 发送彩信 • 读取小区广播消息
通话记录权限	android.permission-group.CALL_LOG	• 读通话记录 • 写通话记录 • 重新设置呼出路径
日历权限	android.permission-group.CALENDAR	• 读日历 • 修改日历
身体传感器权限	android.permission-group.SENSORS	身体传感器

3.5 适配要求

实现权限申请目的展示需所运行的系统支持，因此，应用软件应先判断所运行的系统是否允许其展示权限申请目的，为避免应用软件适配多个接口，终端宜提供统一接口供应用软件调用，以判断所运行的系统是否允许权限申请目的展示，如使用安卓接口Settings.Secure.getString，定义

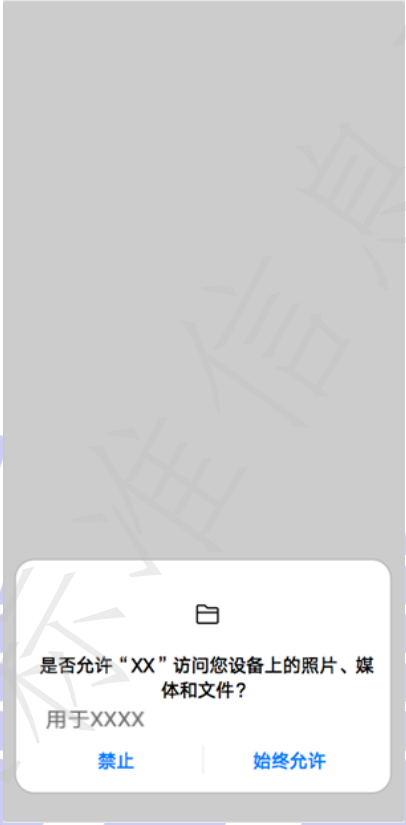
permission_reason_policy名称，permission_reason_policy取值表示系统是否允许应用软件展示权限申请目的，建议包含三种取值，分别是系统对权限申请目的展示没有限制、系统不支持权限申请目的展示、系统支持权限目的展示、但需对权限申请目的内容进一步验证。当系统允许则应用可使用权限申请目的展示，否则应用可使用其它方式实现权限申请目的展示。

在系统允许的情况下，建议应用软件优先使用系统支持的权限申请目的说明方式，避免多次弹框，给用户造成困扰。

注：permission_reason_policy的取值参考附录D。

附 录 A
（资料性附录）
权限申请目的说明示例

图A.1展示了权限动态弹框界面申请目的。



图A.1 权限动态弹框界面申请目的

应用运行时，通过弹框申请权限，在弹框界面除说明需申请的权限外，还应说明权限申请的目的，本示例中，权限申请目的的的描述方式为“用于XXXX”。

图A.2展示了安装器界面权限申请目的。

图A.2 安装器界面权限申请目的

应用安全成功后的安装器界面包括本应用涉及的权限，相应的可在权限名称下说明权限申请目的，本示例中，权限申请目的的描述方式为：以便“XX应用”提供XX服务。

图A.3展示了移动终端应用软件权限管理界面权限申请目的。

图A.3 移动终端应用软件权限管理界面权限申请目的

移动应用软件中通常为用户提供权限管理界面，权限管理界面为用户提供终端上应用软件的权限权限授权情况，包括已允许的权限和已禁止的权限，且用户还可以进一步修改权限授权状态，在权限管理界面上为用户提供管理权限操作时应为用户展示应用申请某一权限的目的，上图中是在为用户提供修改权限授权状态界面为用户提供目的展示的示例。

附 录 B
（资料性附录）
安卓危险权限权限申请目的告知实现示例

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
  <manifest xmlns:android="http://schemas.android.com/apk/res/android"
      package="com.example.permissionreasontest">

      <application
          android:allowBackup="true"
          android:icon="@mipmap/ic_launcher"
          android:label="@string/app_name"
          android:roundIcon="@mipmap/ic_launcher_round"
          android:supportsRtl="true"
          android:theme="@style/AppTheme">

          <!-- ... -->

          <meta-data
              android:name="permission.reason.android.permission-group.LOCATION"
              android:resource="@string/permission_reason_location" />

          <meta-data
              android:name="permission.reason.android.permission-group.STORAGE"
              android:resource="@string/my_permission_reason_storage" />

          <!-- ... -->
      </application>
  </manifest>

<resources>
      <!-- ... -->
      <string name="permission_reason_location">Used for people nearby!</string>
      <string name="my_permission_reason_storage">Used for message persist!</string>
      <!-- ... -->
  </resources>
```

附 录 C
（资料性附录）
应用自定义危险权限权限申请目的告知实现示例

A.1 自定义危险权限未指定权限组

```
<permission android:name="com.test.cust1" android:protectionLevel="dangerous"
    android:description="@string/permission_des"/>

<uses-permission android:name="com.test.cust1"/>

...

    <meta-data
        android:name="permission.reason.com.test.cust1"
        android:resource="@string/permission_reason_cust1" />

...
```

A.2 自定义危险权限指定权限组

```
<permission-group android:name="com.test.cust-group2"
android:description="@string/permission_reason_cust_group"/>

<permission android:name="com.test.cust2"
android:protectionLevel="dangerous"
    android:description="@string/permission_des"
    android:permissionGroup="com.test.cust-group2"/>

<uses-permission android:name="com.test.cust2"/>

...

    <meta-data
        android:name="permission.reason.com.test.cust-group2"
        android:resource="@string/permission_reason_cust_group" />

...
```

附 录 D
（资料性附录）
permission_reason_policy 的取值范围

permission_reason_policy的取值范围包括：

- “NO_RESTRICTED”：表示系统对应用使用权限申请目的展示没有限制；
- “SUPPORTED;com.package1;com.package2;...”：表示系统支持，但需要对应用软件权限申请目的内容进一步验证，package包含系统支持的应用列表；
- “FORCED_RESTRICTED”：表示系统不支持权限申请目的展示。

电信终端产业协会团体标准

移动终端权限申请目的说明实施指南

T/TAF 076-2020
*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn