

ICS 33.030  
CCS M21

# 团体标准

T/TAF 353.7—2026

## 移动互联网应用程序(APP)最小必要申请使用权限要求 第7部分：短信

Mobile Internet application permission application and usage  
minimization and necessity requirements—  
Part 7: SMS

2026-06-17 发布

2026-06-17 实施

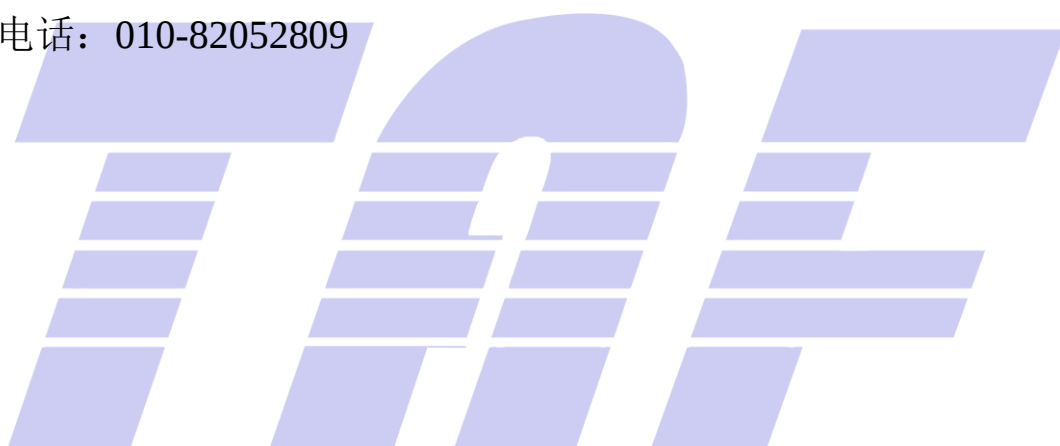
电信终端产业协会 发布

## 版权声明

本文件的版权属于电信终端产业协会，任何单位和个人未经许可，不得进行技术文件的纸质和电子等任何形式的复制、印刷、出版、翻译、传播、发行、合订和宣贯等，也不得未经允许采用其具体内容编制本团体以外各类标准和技术文件。如有以上需要请与本团体联系。

邮箱：tafrb@taf.org.cn

电话：010-82052809



目 次

前言 ..... II

引言 ..... III

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 1

5 基本原则 ..... 1

6 典型场景 ..... 2

7 技术要求 ..... 5

8 评估要求 ..... 6

附录 A（资料性） 短信权限检查与申请代码示例 ..... 7

## 前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是T/TAF 353《移动互联网应用程序（APP）最小必要申请使用权限要求》的第7部分。T/TAF 353已经发布了以下部分：

- 第1部分：总则；
- 第2部分：相册；
- 第3部分：文件；
- 第4部分：联系人；
- 第5部分：通话记录；
- 第6部分：日历；
- 第7部分：短信。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会（TAF）提出并归口。

本文件起草单位：中国信息通信研究院、小米通讯技术有限公司、维沃移动通信有限公司、OPPO广东移动通信有限公司、荣耀终端股份有限公司、华为终端有限公司、卓望数码技术（深圳）有限公司、北京三星通信技术研究有限公司、友盟同欣（北京）科技有限公司、阿里巴巴（北京）软件服务有限公司、玩咖欢聚科技（北京）有限公司、厦门美柚股份有限公司、上海声网科技有限公司。

本文件主要起草人：赵小平、吴越、张丹静雅、任雨、陈鑫爱、王艳红、周飞、常浩伦、武林娜、王淞鹤、杜云、李京典、李可心、姚一楠、贾科、李腾、杨明慧、闫金保、赵晓娜、衣强、张圣迪、杨艺、王彬、贾紫薇、姚栋、刘艾婧、刘伟峰、黄鹏华、钱雷、薛源。

# 引 言

随着移动互联网的快速发展，APP已成为用户获取信息和服务的主要载体，但其过度申请和滥用权限的问题日益突出，严重威胁用户信息安全和合法权益。

T/TAF 353《移动互联网应用程序（APP）最小必要申请使用权限要求》系列标准旨在对APP最小必要的申请使用权限提出要求，由7部分构成。

- 第1部分：总则。目的在于规定APP最小必要申请使用权限的基本原则、基本要求，以及APP开发运营者、移动应用分发平台、移动智能终端、第三方评估机构在最小必要权限管理方面的管理要求。
- 第2部分：相册。目的在于规定移动互联网应用程序（APP）最小必要的申请访问相册的基本原则、典型场景、技术要求和评估要求。
- 第3部分：文件。目的在于规定移动互联网应用程序（APP）最小必要的申请使用文件的基本原则、典型场景、技术要求和评估要求。
- 第4部分：联系人。目的在于规定移动互联网应用程序（APP）最小必要的申请使用终端系统联系人权限的基本原则、典型场景、技术要求和评估要求。
- 第5部分：通话记录。目的在于规定移动互联网应用程序（APP）最小必要的申请使用通话记录权限的基本原则、典型场景、技术要求和评估要求。
- 第6部分：日历。目的在于规定移动互联网应用程序（APP）最小必要的申请使用日历访问权限的基本原则、典型场景、技术要求和评估要求。
- 第7部分：短信。目的在于规定移动互联网应用程序（APP）最小必要的申请使用短信的基本原则、典型场景、技术要求和评估要求。

# 移动互联网应用程序(APP)最小必要申请使用权限要求 第7部分： 短信

## 1 范围

本文件规定了移动互联网应用程序（APP）最小必要的申请使用短信的基本原则、典型场景、技术要求和评估要求。

本文件适用于移动互联网应用程序提供者规范的申请使用短信权限，也适用于主管部门、第三方评估机构、移动应用分发平台、移动智能终端等对APP申请上述权限的行为进行监督、管理和评估。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

T/TAF 353.1—2026 移动互联网应用程序（APP）最小必要申请使用权限要求 第1部分：总则

## 3 术语和定义

T/TAF 353.1—2026界定的以及下列术语和定义适用于本文件。

### 3.1

#### 短信权限 SMS permission

由移动智能终端操作系统提供，允许移动互联网应用程序处理用户短息数据的权限，包括收取、读取和发送短信的权限。

注1：本文件所指权限仅为操作系统定义并开放给APP申请使用的权限。

注2：Android系统中，收取、读取和发送权限分别为android.permission.RECEIVE\_SMS、  
android.permission.READ\_SMS和android.permission.SEND\_SMS。

## 4 缩略语

下列缩略语适用于本文件。

APP：移动互联网应用程序（Mobile Internet Application）

## 5 基本原则

APP申请访问短信的基本原则如下：

- a) 应满足T/TAF 353.1—2026的要求；
- b) 申请短信权限应当具有明确、合理的目的，应为实现面向用户的功能或用途，即若无法接收/读取/发送短信信息，应用就无法使用；

- c) APP提供的业务场景不在第6章列出的范围内时,应用开发者应参考类似功能的场景,满足最小必要要求。

6 典型场景

6.1 APP 可申请使用短信权限场景

- APP(包括嵌入的 SDK)应按照业务功能场景申请使用相关权限,不应过度申请权限。
- a) APP 可申请使用短信权限的典型场景见表 1。
- b) 针对未被表 1 所覆盖的其他场景,应详细评估 APP 功能与权限的相关性,仅在短信权限为 APP 实现功能的不可替代的必要条件时,才可允许申请。
- c) 评估方可通过 APP 的功能描述、截图/视频演示、触发路径描述等辅助材料判断 APP 申请使用短信权限的必要性。

表 1 APP 可申请使用短信权限的典型场景

| 场景                                   | 详细描述                                                                                           | 细分场景举例                                                                      | 可使用权限 |    |    |
|--------------------------------------|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|-------|----|----|
|                                      |                                                                                                |                                                                             | 收取    | 读取 | 发送 |
| 已关联设备的<br>配套应用(可<br>收/发短信)           | 通过此类应用,用户能够将移动设备与已关联设备(例如智能手表、汽车技术、智能家居设备等)连接起来,通常服务于以下场景:<br>1) 设备连接后短信消息提醒<br>2) 拒接场景下自动短信回复 | (收)连接设备:设备连接后提醒,实时查看消息通知提醒,但不会读取短信内容,仅需监控短信到达的瞬间,进行短信提醒,无需读取短信内容。           | √     | —  | —  |
|                                      |                                                                                                | (发)拒接来电后的短信自动回复功能:当使用智能设备拒接来电时,设置短信自动回复功能。                                  | —     | —  | √  |
| 骚扰拦截与风险检测                            | 垃圾内容检测和/或垃圾内容屏蔽                                                                                | —                                                                           | √     | —  | √  |
| 特殊功能场景<br>下短信触达<br>(基于用户目的,即用户需求的通知) | 基于应用核心功能,在特殊或特定场景下,用户明确授权后,应用通过短信触达,完成业务交互                                                     | (读)短信接单:便捷生活品类应用中,通过开启短信接单功能,在网络不佳的情况下使用短信进行交互以顺利完成订单,仅能读取与该业务相关的特定号码发送的短信。 | —     | √  | —  |
|                                      |                                                                                                | (发)短信接单:网络不佳的情况下,根据用户操作向特定号码发送短信指令,实现订单配送信息交互                               | —     | —  | √  |
|                                      |                                                                                                | (发)未接来电后的短信自动回复功能:当拒接、未接到来电后,设置短信自动回复功能。                                    | —     | —  | √  |

表1 APP可申请使用短信权限的典型场景（续）

| 场景                | 详细描述                                                                  | 细分场景举例                                                                                                            | 可使用权限 |    |    |
|-------------------|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-------|----|----|
|                   |                                                                       |                                                                                                                   | 收取    | 读取 | 发送 |
| 人身安全/紧急警报（通过发送短信） | 在发生紧急状况时发送短信，进行行程分享、紧急求助、一键报警、防护提醒等                                   | <b>（发）应用在紧急情况下代用户发送求助短信：</b> 包括但不限于应用中一键求助、一键求救、安全守护、一键报警等紧急求助的场景和功能。                                             | —     | —  | √  |
|                   |                                                                       | <b>（发）行程分享短信同步：</b> 出行用车品类，经用户授权，通过短信将行程信息自动分享给紧急联系人。                                                             |       |    |    |
|                   |                                                                       | <b>（发）家人防护功能提醒：</b> 实用工具品类，经用户授权，通过关联，在家人收到诈骗电话/短信/安装应用时发送短信提醒。                                                   |       |    |    |
| 查询流量、监控流量         | 以便利用户操作为目的，APP帮助用户发送特定短信指令至特定号码，查询相关信息或订阅服务的场景，如流量余额查询或者向运营商发送流量校准短信。 | 原则上限定实用工具品类、电信类APP                                                                                                | —     | —  | √  |
| 数据备份及同步           | 通过读取设备中的短信数据（包括收件箱、发件箱、草稿等），备份短信到用户指定的存储（设备、云盘等）。                     | <b>（读）自动备份服务：</b> 用于备份手机短信数据（需用户授权）。                                                                              | —     | √  | —  |
|                   |                                                                       | <b>（读）一键换机：</b> 接收旧手机的短信数据并传输至新手机（本地传输，不上传服务器）。                                                                   |       |    |    |
| 安全风险              | 如果应用的某个可验证的核心用途涉及金融交易功能，可允许该应用仅出于安全方面的目的而获取“短信相关权限                    | <b>（读）支付保镖：</b> 金融交易场景下的安全风险行为，风险检测行为的一种类型，当通过网址或支付类应用软件进行交易支付时，此功能通常用于保护交易行为和当前手机所处环境的安全；通过读取短信内容，识别短信中是否包含恶意网址。 | —     | √  | —  |

表 1 APP 可申请使用短信权限的典型场景（续）

| 场景         | 详细描述                                                  | 细分场景举例                                                                 | 可使用权限 |    |    |
|------------|-------------------------------------------------------|------------------------------------------------------------------------|-------|----|----|
|            |                                                       |                                                                        | 收取    | 读取 | 发送 |
| 安全风控       | 如果应用的某个可验证的核心用途涉及金融交易功能，可允许该应用仅出于安全方面的目的而获取“短信相关权限    | <b>（读/接收）操作异常提醒：</b> 通过用户常规登录动作及数据，分析应用使用异常时发短信提醒。                     | √     | √  | —  |
|            |                                                       | <b>（读）风控与反欺诈：</b> 基于反欺诈目的读取短信记录（如接发数量、接收时间、短信内容），用于风控模型迭代、资信评估及欺诈行为检测。 | √     | √  | —  |
| 云手机场景下短信发送 | 云手机类应用涉及短信功能，可允许应用获取短信相关权限以调用真机的发短信能力、保障云机短信功能与真机的协同。 | —                                                                      | —     | √  | √  |

6.2 APP 不应申请使用短信权限场景

APP 出现以下情形不应申请使用短信权限：

- a) 短信权限的使用与 APP 的服务场景并没有直接关联；
- b) 仅以服务体验、产品研发、算法推荐、风险控制为由申请权限；
- c) 获取短信是为了将其出售或分享给第三方用于分析或仅用于个性化广告推荐；
- d) 无需短信权限就能完成 APP 的目标任务，实现功能；
- e) 不应申请使用短信权限的典型场景见表 2。

表2 APP不应申请使用短信权限场景

| 功能/场景       | 详细描述                                                                      | 细分场景                                                                                                   |
|-------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| 短信个人信息读取    | 通过读取短信中特定内容，包括但不限于个人信息、行程信息、消费信息等，用于应用中个某项特殊功能使用。                         | —                                                                                                      |
| 分享功能、邀请好友   | 用于分享套餐、智能家居等产品；或基于某些需求背景，通过发送短信邀请通讯录好友。                                   | <b>（发）分享功能：</b> 用于分享套餐、智能家居等产品；                                                                        |
|             |                                                                           | <b>（发）邀请好友：</b> 在用户邀请通讯录好友注册登录使用某应用的场景下，给被邀请用户发送短信。点击邀请之后就会打开手机短信发送页面，点击“发送”按钮后，邀请好友的信息就会以手机短信的形式发送出去。 |
| 获取验证码、验证码读取 | 用户注册、登录账号、身份验证等场景下，用户输入手机号码后，点击获取验证码后，读取短信验证码的行为。<br>系统输入法读取验证码的场景不适用于本条。 | —                                                                                                      |

表 2 APP 不应申请使用短信权限场景（续）

| 功能/场景                                          | 详细描述                                                       | 细分场景                                                                                                                             |
|------------------------------------------------|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 系统短信功能替代                                       | 应用通过申请权限，达到与系统短信功能一致的目的。                                   | <b>短信管理：</b> 与系统短信功能一致，应用完全替代系统短信，进行短信的读取及发送。                                                                                    |
|                                                |                                                            | <b>定时发送：</b> 基于非合理场景下的频繁呼叫、短信发送（合理场景除外）。                                                                                         |
|                                                |                                                            | <b>针对用户手机或其他设备的远程控制：</b> 基于当前应用，针对其他号码下的手机等设备进行短信的读取、发送。                                                                         |
| 短信召回、推广，以及服务信息变更通知<br>（基于开发者目的，用户流失召回、推广信息发送等） | 通过向特定用户群体发送短信，以促使用户重新回到产品或服务中，或基于某些场景、或某个节点进度变更，向用户进行短信发送。 | <b>（发）短信召回：</b> 适用于各类产品或服务，当用户在规定时间内没有使用产品或服务，处于流失状态时，企业会通过短信召回的方式，尝试唤醒他们，吸引他们再次使用。比如游戏公司向长时间未登录游戏的玩家发送短信，告知其游戏的更新内容、新活动等，吸引玩家回流 |
|                                                |                                                            | <b>（发）短信推广：</b> 应用发送活动、产品、商业、优惠等推广营销服务相关信息，用于一般场景下的用户通知、触达。                                                                      |
|                                                |                                                            | <b>（发）产品服务变更通知：</b> 在必需时发出与服务、业务等有关的通知；包括但不限于，由于系统维护而暂停某一单项服务；变更、终止提供某一单项服务等。                                                    |
|                                                |                                                            | <b>（发）充值汇款等涉及金融交易功能的短信通知：</b> 应用上购买服务，进行金融交易、银行汇款等服务时，应用基于业务进行短信发送                                                               |

7 技术要求

7.1 APP 申请短信权限

APP 申请系统短信权限应满足如下要求：

- a) APP（包括嵌入的 SDK）申请所需权限应在声明文件（如 AndroidManifest.xml）中严格按照格式规范逐个声明，代码示例见附录 A；
- b) APP 应在需要使用短信的功能页面启动运行时动态申请权限，不应提前申请，以提高用户对权限申请必要性的理解；
- c) APP 申请权限时应同步告知权限申请目的，目的应明确且易于理解，不包含广告及任何欺诈、诱骗、误导用户授权的描述；
- d) 如 APP 仅需使用权限组中部分权限，不应在权限声明文件中声明同一权限组其他权限，例如当 APP 仅需使用读短信权限时，不应在 AndroidManifest.xml 中声明发送权限；
- e) 如用户拒绝或撤回授予某服务类型非必要系统权限，APP 不应强制退出或关闭，且不影响与此权限无关的业务功能使用；
- f) APP 不得采用默认、捆绑或使用其他手段变相欺骗、误导、强迫用户授予权限；
- g) 如用户明确拒绝 APP 业务功能所需权限，APP 不应频繁申请权限干扰用户正常使用，除非由用户主动触发功能，且没有该权限参与此业务功能无法实现。

## 7.2 APP 使用短信权限

APP 使用短信权限应满足如下要求。

- a) APP 在使用短信权限前，应检查自身是否已获得权限。短信权限检查及处理相关代码示例参见附录 A。
- b) APP 被授予权限后应遵循最小必要原则合理使用权限，不应超频次、超范围、超精度收集短信信息。
- c) 若 APP 功能发生变化而不再需要使用短信权限时，应及时停止权限申请和使用。对于更新之后的 APP 应重新评估权限申请使用的必要性。

## 8 评估要求

APP 申请使用相册访问权限的评估要求如下。

- a) 应根据第 6 章典型场景判定是否允许 APP 申请权限访问短信。若 APP 功能场景未被表 1、表 2 涵盖，则应根据最小必要原则进行评估。对于不满足原则的 APP，应采用技术手段限制其申请或使用短信访问权限。
- b) 移动应用分发平台应通过 APP 的功能描述、截图/视频演示、触发路径描述等辅助材料判断 APP 申请使用短信访问权限的必要性。



附 录 A  
(资料性)  
短信权限检查与申请代码示例

以申请发送短信为例，其余权限替换相应权限名称即可。

```
private static final int REQUEST_SEND_SMS = 1;
private void checkAndRequestPermission() {
    if (ContextCompat.checkSelfPermission(this, Manifest.permission.SEND_SMS)
        != PackageManager.PERMISSION_GRANTED) {
        // 权限未获得
        if (ActivityCompat.shouldShowRequestPermissionRationale(this,
Manifest.permission.SEND_SMS)) {
            // 向用户解释为什么需要该权限
        } else {
            // 直接申请权限
            ActivityCompat.requestPermissions(this,
                new String[] {Manifest.permission.SEND_SMS},
                REQUEST_SEND_SMS);
        }
    } else {
        // 已获得权限
    }
}
// 权限申请结果处理
@Override
public void onRequestPermissionsResult(int requestCode, @NonNull String[] permissions,
                                       @NonNull int[] grantResults) {
    super.onRequestPermissionsResult(requestCode, permissions, grantResults);
    if (requestCode == REQUEST_SEND_SMS) {
        if (grantResults.length > 0
            && grantResults[0] == PackageManager.PERMISSION_GRANTED) {
            // 权限申请成功
        } else {
            // 权限申请失败
        }
    }
}
```

电信终端产业协会团体标准

移动互联网应用程序（APP）最小必要申请使用权限要求  
第7部分：短信

T/TAF 353.7—2026

\*

版权所有 侵权必究

电信终端产业协会发布

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](http://www.taf.org.cn)