ICS 33.030
CCS M21

# 团　体　标　准

T/TAF 326—2026

# 端云联动的移动互联网业务风险防控框架

Cloud and terminals coupling framework for mobile internet business risk control

2026-02-09 发布　　2026-02-09 实施

电信终端产业协会　发布

# 版权声明



邮箱：tafrb@taf.org.cn

电话：010-82052809

# 目　　次

# 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。

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：OPPO广东移动通信有限公司、中国信息通信研究院、蚂蚁科技集团股份有限公司、维沃移动通信有限公司、小米通讯技术有限公司、华为技术有限公司、荣耀终端股份有限公司、北京快手科技有限公司、北京三星通信技术研究有限公司。

本文件主要起草人：付艳艳、徐腾、王艳红、陈鑫爱、杜云、李京典、李可心、李腾、曾德康、林冠辰、徐曼、衣强、赵晓娜、胡建园、颜秉武、王彬、罗元海。

# 端云联动的移动互联网业务风险防控框架

## 1 范围

本文件提供了端云联动的移动互联网业务风险防控建议，给出了与端云联动架构、基础模块和安全功能等相关的信息。

本文件适用于指导智能终端侧和云侧联合进行业务风险防控的场景，也适用于指导不同参与者间进行风险防控合作。

## 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。

GB/T 35273 信息安全技术 个人信息安全规范

T/TAF 078.10 APP用户权益保护测评规范 第10部分：自启动和关联启动行为

T/TAF 110—2022 智能终端侧业务风险防控安全指南

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**业务安全风险 business security risk**

业务正常逻辑面临的被滥用或篡改的威胁，导致业务目的与业务结果产生的不确定性，包含但不限于金融欺诈、账户盗刷、内容违规等。

[来源：YD/T 3796—2020]

3.2

**业务风险防控 business risk control**

为控制业务安全风险，识别和判定安全风险、做出风控决策和进行决策响应的过程。

## 4 缩略语

下列缩略语适用于本文件。

APP：应用程序（application）

## 5 移动互联网业务风险防控场景概述

移动互联网业务风险防控场景包括防控营销活动作弊、信贷欺诈、钓鱼网站、虚假流量、垃圾内容等。通过风险防控工作，可以有效帮助业务防范业务安全风险和减少损失。按照移动互联网业务流程，

在其风控活动中有众多风险信息输入，包括业务 APP 内部用户异常活动、外部系统及 APP 风险状况等，如用户异常登录、APP 高危漏洞或 APP 签名异常等。

在长期持续的业务风险防控过程中，可根据多维业务风控体系指标、丰富的业务风险防控策略、高效的风险防控引擎更加灵活快速地进行风险防控和策略优化部署等。

在业务风险防控过程中，如涉及到用户个人信息处理过程，应满足GB/T 35273的要求。风险防控的任何参与方均需采用相应的技术和管理手段以确保业务、数据、用户个人信息和权益等多方面安全，不应以风险防控为理由超范围获取用户数据，或通过不正当手段获取其他参与方数据，或干扰、妨碍其他参与方产品、服务的正常运行。

## 6 移动互联网业务风险防控通用需求

由于移动互联网业务的特殊性，其部分业务流程依靠移动智能终端支持，部分业务流程由业务服务提供者自行提供。因此在业务开展过程中，单独依赖移动智能终端或业务服务提供者进行风险防控，存在着数据缺失、风险画像不全等缺陷，使得单方的风险防控机制难以有效遏制业务风险。

为有效结合移动智能终端提供者、业务服务提供方、以及其他可能的安全风险防控支持方的能力，当前移动互联网业务联动的风险防控通用需求主要包括以下方面：

a） 黑名单类信息合作，如高度可疑或涉案账号、设备、应用信息等，可通过云侧能力或平台共建等方式实现；

b） 风控特征类信息合作，如账号、设备以外的其他风控关键特征等，可通过云侧、终端侧算法合作等方式实现；

c） 风控算法合作，如多方间通过联邦学习、多方安全计算等算法进行风控模型离线训练、风控实时决策等。

## 7 端云联动的移动互联网业务风险防控架构

### 7.1 概述

如图1所示，端云联动的移动互联网业务风险防控架构包括终端侧和云侧两部分。本文件将涉及到跨终端侧和云侧的数据流动的联合防控称为联动，将仅基于终端侧数据或仅基于云侧数据的联合防控称为协同。例如，APP终端侧风控模块与APP云侧风控模块的联合防控属于联动，APP终端侧风控模块与操作系统终端侧风控模块的联合防控属于协同。联动防控中可有一个或多个不同主体参与方，协同防控中至少有两个不同主体参与方。

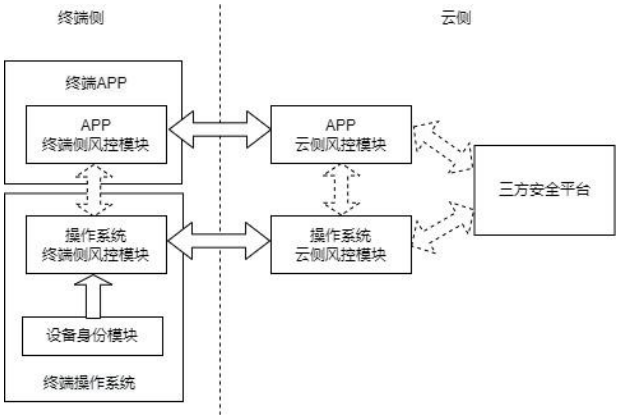


图1 端云联动的移动互联网业务风险防控架构

其中，终端侧风控模块可包括操作系统终端侧风控模块、APP终端侧风控模块和设备身份模块。操作系统终端侧风控模块和APP终端侧风控模块可在终端侧进行协同，获取终端侧风险信息并在终端内进行部分处理，联动云侧风控模块进行风控决策支持、响应。云侧风控模块可包括操作系统云侧风控模块、APP云侧风控模块、三方安全平台，各方可在云侧进行协同，从云侧对业务风险进行监测，结合三方安全平台的威胁情报输入快速响应，联动终端侧风控模块进行风控决策，更新风控配置、模型等。终端侧风控模块和云侧风控模块联动和协同开展风控的目的在于提高本地处理、响应效率，减少非必要的跨端数据传输等处理，并利用终端侧和云侧各自优势充分发挥数据价值。

### 7.2 移动互联网业务风险防控参与方

移动互联网业务风险防控的参与方包括：智能终端提供者、业务应用服务提供者、三方安全服务提供者。

智能终端提供者关注终端整体安全环境，支持正常APP安全运行。

业务应用服务提供者关注业务安全和用户保护，对恶意用户或黑灰产侵害业务活动的行为进行打击，保护业务安全和正常用户合法权益。

三方安全服务提供者关注安全服务、安全能力的质量和性能等，对一个或多个来源的业务安全威胁信息进行整合、分析、响应、处置，对外提供业务风险防控服务、产品等。

智能终端上的设备身份模块、操作系统终端侧风控模块由智能终端提供者单独提供，云侧的三方安全平台由三方安全服务提供者单独提供。终端APP内的APP终端侧风控模块、云侧的APP云侧风控模块由业务应用服务提供者单独提供。

如有两方或多方合作参与防控，各参与方需通过合同等形式共同确定应满足的安全要求，以及各方应分别承担的责任和义务。风险防控合作需要建立在各方自愿、平等参与的基础上，充分尊重各方的合作意愿以及确定的合作范围。

## 8 基础模块和功能

### 8.1 设备身份模块

#### 8.1.1 模块风控功能

设备身份模块主要负责收集设备指纹相关特征信息，以SDK或系统服务API等形式对终端侧风控模块提供服务。通过终端侧风控模块的联动，设备身份模块也可以向云侧系统提供相关信息。

设备指纹相关特征信息包括非可唯一识别设备的信息，如：

a） 系统版本；

b） 手机型号。

设备指纹相关特征信息还可包括描述设备、系统状态的相关信息，如：

a） 系统是否被root；

b） 系统中是否安装作弊工具；

c） 是否模拟器环境；

d） 是否系统调试状态。

#### 8.1.2 模块安全防护

设备指纹相关特征信息宜在终端安全环境中使用，或宜通过设备指纹ID等形式标识风控设备，以保护数据安全。

如通过可信执行环境等终端安全环境保护设备指纹信息，则宜满足T/TAF 110—2022中考虑的因素。

如通过设备指纹ID的形式标识风控设备，则宜满足以下要求：

a） 仅通过设备指纹ID无法获得设备具体特征；

b） 宜采用密码技术等保护生成设备指纹ID所需相关特征信息的机密性、完整性和可用性；

c） 宜在风控各参与方间统一设备指纹ID生成算法，避免ID无法匹配问题。

## 8.2 终端侧风控模块

### 8.2.1 模块风控功能

终端侧风控模块主要负责在终端侧进行风险检测、风险判定及联动云侧风控决策、依据风控决策结果进行风险拦截和提示等，其功能和工作流程如下：

a） 终端侧风险检测：

1） APP终端侧风控模块对自身内部业务活动进行监控和检测，发现其中的异常，以作为后续进行业务风险判定的输入，监控对象包括注册、登录、点击、授权等用户操作，以及APP使用的数据库等业务辅助工具；

2） 操作系统终端侧风控模块对移动互联网业务上线后的安全环境进行监测，发现其中的异常，以作为进行业务风险判定的输入。如APP安装包是否包含病毒木马、是否存在违规使用权限等风险。

b） 业务风险判定及联动云侧风控决策：

1） APP终端侧风控模块将发现的APP业务风险信息传输到APP云侧风控模块，或进行本地风险判定并将风险判定结果传输到云侧；

2） 操作系统终端侧风控模块将发现的终端风险信息传输到操作系统云侧风控模块，或进行本地风险判定并将风险判定结果传输到云端；

3） APP终端侧风控模块获取来自APP云侧风控模块的决策；

4） 操作系统终端侧风控模块获取来自操作系统云侧风控模块的决策；

5） 协同场景中，操作系统终端侧风控模块可将该业务应用APP运行时的本地风险判定部分结果提供给APP终端侧风控模块，APP终端侧风控模块可将云侧风控决策部分结果提供给操作系统终端侧风控模块。

c） 终端侧风险拦截、提示：

1） 支付类应用宜具备可疑支付拦截、提示功能；

2） 内容类应用宜具备可疑链接提示功能。

### 8.2.2 模块安全防护

终端侧风控模块宜在终端安全环境中使用，或宜采用加密、认证等措施进行保护，以保障功能安全和自身安全。

终端侧风控模块如需双方或多方进行协同计算，需采用相应安全措施防止数据泄露，如安全多方计算等。

## 8.3 云侧风控模块

### 8.3.1 模块风控功能

云侧风控模块主要负责在云侧进行风控管理，联动终端侧风控模块进行风控决策和下发风控决策，其主要功能和工作流程如下：

a） 风控管理：

1） APP云侧风控模块、操作系统云侧风控模块、三方安全平台对自身的风控规则、风控决策进行单独管理和配置；
2） 协同场景中，APP云侧风控模块、操作系统云侧风控模块、三方安全平台协同训练风控模型，更新对应的自身风控决策。

b） 联动终端侧风控模块进行风控决策：
1） 与端侧风控模块交互，获得相关风控信息，如APP业务风险信息、终端侧风险判定结果等；
2） 基于已有风控信息和参数，利用风控决策生成风控决策；
3） 协同场景中，与三方安全平台交互，如输出可疑账号或设备、IP地址等信息和获得安全威胁信息等，与操作系统云侧风控模块、三方安全平台交互，进行风控决策。

c） 根据风控决策调用验证码等风险控制功能；

d） 联动终端侧风控模块，下发风控决策，由终端侧 APP、操作系统在各自职责范围内接收、处理决策。

#### 8.3.2 模块安全防护

云侧风控模块如需协同交互时，宜通过身份认证、加密传输等手段保护数据安全。

云侧风控模块如需双方或多方进行协同计算，需采用相应安全措施防止数据泄露，如安全多方计算等。

### 8.4 其他安全功能

#### 8.4.1 跨应用风险特征研判

基于终端侧和云侧风控模块联动，智能终端可以设备、账号为维度进行风控画像，支撑跨应用风险特征研判等风险防控活动。在充分告知用户获得同意、参与方签订相应数据合作协议或合同的基础上，智能终端或应用间也可相互协同，进一步识别风险特征。

风控画像宜定期更新。

#### 8.4.2 全链路风险管控

基于终端侧和云侧的风控模块联动建立安全环境，可覆盖移动互联网业务上线后的风险行为监测和安全管理。如通过病毒、恶意应用检测和应用运行时攻击系统、频繁自启动和关联启动等行为发现业务运行环境中存在的风险应用；通过终端侧风控模块和云侧风控模块联动分别对业务核心接口进行验证核验遏制黑灰产非法调用接口等；通过云侧风控模块对链路中发现的风险行为进行持续跟踪和决策，并持续升级优化风控模型；通过信息合作等方式将风控过程中发现的运行环境中存在的风险应用在各环节进行共享，并采取适当管理和技术保障措施，进一步降低移动互联网业务风险。

**注：**自启动和关联启动行为应符合T/TAF 078.10中的规定。

# 参 考 文 献

[1] YD/T 3796—2020 基于云计算的业务安全风险解决方案技术要求

[2] YD/T 4600—2023 面向互联网业务的大数据风险控制系统技术要求

[3] 工业和信息化部关于开展纵深推进APP侵害用户权益专项整治行动的通知(工信部信管函〔2020〕164号)

[4] 工业和信息化部关于进一步提升移动互联网应用服务能力的通知(工信部信管函〔2023〕26号)

# 电信终端产业协会团体标准

# 端云联动的移动互联网业务风险防控框架

T/TAF 326—2026

*



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