ICS 33.030
CCS M21

团　体　标　准

T/TAF 321—2026

公众无线局域网接入服务 APP 业务框架安全与个人信息保护要求

Security business framework and personal information protection requirements for public WLAN access service mobile application software

2026-01-06 发布　　2026-01-06 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：中国信息通信研究院、南京尚网网络科技有限公司、北京快手科技有限公司、南德认证检测（中国）有限公司深圳分公司。

本文件主要起草人：方斌、陈鑫爱、张作裕、王淞鹤、荣蓉蓉、王渊明、武林娜、王艳红、李可心、杜云、落红卫、周世乐。

公众无线局域网接入服务 APP 业务框架安全与个人信息保护要求

1 范围

本文件规定了公众无线局域网接入服务 APP 安全业务框架，明确了其技术要求与管理要求。

本文件适用于规范基于自身路由器等硬件设备提供公众无线局域网接入服务 APP 在设计、研发、运营时的安全实践与个人信息保护行为，同时为应用分发平台审核、主管监管部门、第三方评估机构等组织提供参考依据。

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。

YD/T 4184 移动互联网应用程序（APP）用户权益保护测评规范

YD/T 6221 移动应用软件个人信息保护要求和评估方法

T/TAF 148 电信和互联网个人信息保护保障能力评估规范

T/TAF 209 移动互联网应用程序（APP）合规开发管理测评规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

个人信息 personal information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

[来源：《中华人民共和国个人信息保护法》第四条]

3.2

匿名化 anonymization

个人信息经过处理无法识别特定自然人且不能复原的过程。

[来源：《中华人民共和国个人信息保护法》]

3.3

用户 user

使用产品或服务的个人信息主体。

[来源：GB/T 25069-2022，3.733，有修改]

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 application software）
BSSID：基础服务标识符（basic service set identifier）
TLS：传输层安全协议（transport layer security）
SSID：服务集标识符（service set identifier）

5 安全业务框架

公众无线局域网接入服务APP是指向用户提供公共场所无线局域网基于位置信息发现无线局域网、连接、认证、管理及相关服务的移动互联网应用程序。无线局域网运营者是指公众无线局域网接入服务APP的开发、运营及维护的责任主体，包括机场、车站、商场、酒店等提供公众无线局域网接入服务的实体机构。公众无线局域网接入服务的业务框架图如图1所示。

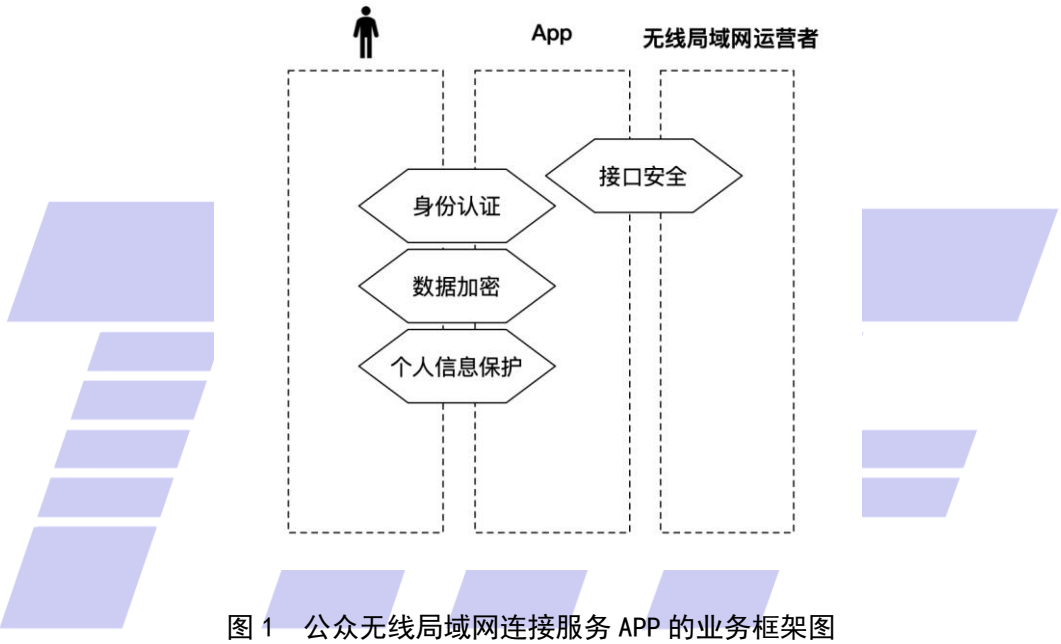

图 1 公众无线局域网连接服务 APP 的业务框架图

用户打开提供公众无线局域网服务的APP，通过定位信息获取当前位置信息的无线局域网，使用6.1.1的认证方式之一连接无线局域网；连接过程中需要使用的认证信息如手机号、生物特征、网络身份等认证信息需要无线局域网运营者依据第六章和第七章要求进行保护。

6 技术要求

6.1 身份认证

6.1.1 认证策略

APP应制定安全的认证策略，可采取以下至少一种的认证方式：

a) 手机号结合短信验证码的认证方式；
b) 基于用户已持有的、经过实名验证的第三方账户（如运营商、互联网平台）进行授权认证的方式；
c) 基于国家网络身份认证的认证方式。

6.1.2 认证服务器安全防护

认证服务器应满足以下安全防护要求：

a) 应部署在隔离的网络区域，并通过防火墙、访问控制列表（ACL）等技术手段实施严格的网络访问控制策略，仅开放必要的服务端口给指定的源地址；
b) 应建立漏洞管理机制，定期进行安全漏洞扫描与修补，并及时更新系统及组件补丁；
c) 应对管理后台的登录访问实施双因素认证，并对所有认证尝试进行日志审计和监控。

6.2 数据加密

6.2.1 数据传输加密

APP应对认证凭据、用户标识、WiFi密码等敏感数据的传输进行加密，并满足如下要求：

a) 所有通信通道（包括用户设备与接入点之间、APP 与业务服务器及认证服务器之间）均应使用 TLS 1.2 及以上版本的安全协议进行加密，宜优先采用 TLS 1.3；
b) 对于极高敏感度的数据，宜在应用层进行端到端的二次加密。

6.2.2 数据存储加密

APP应对敏感数据的存储进行加密，并满足如下要求：

a) 存储在终端设备本地的敏感数据应使用密钥管理设施支持的强加密算法进行保护，例如 SM4 或 AES-256 算法；
b) 存储在服务端的敏感个人信息（如认证凭证、个人身份信息）应进行加密存储，并实施严格的密钥生命周期管理。

6.3 接口安全

APP在调用终端操作系统接口实现公众无线局域网连接服务时，应满足以下要求：

a) 应调用终端操作系统官方开放文档中定义的安全接口（Android 系统接口参见附录 A，鸿蒙系统接口参见附录 B）实现连接服务；
b) 不应利用系统漏洞调用终端操作系统未开放的接口；
c) 接口调用应遵循权限最小化原则，仅限于实现当前连接服务功能的必要场景；
d) 应对接口调用传入的参数进行严格校验，防止参数篡改等攻击，并对调用频率进行限制，防止滥用。

6.4 个人信息保护

APP的个人信息处理活动除应满足YD/T 6221-2024第5章至第10章、YD/T 4184-2023第5章至第14章的要求外，还应满足如下要求。

a) 使用连接服务时，应遵循最小必要原则向用户申请权限。
   1） 位置权限。申请获取位置信息权限时，应清晰告知用户其目的是用于发现周边的可用 WiFi 热点。原则上，在满足热点发现功能的前提下，宜优先选择精度较低的位置服务模式。
   2） 其他权限。除位置权限外，如无充分必要的业务功能依据，不应申请与核心功能无关的权限（如通讯录、短信、传感器等权限）。确需申请传感器等权限用于增强定位等辅助功能时，必须向用户进行清晰说明并获得单独同意，且应提供不授权仍能使用核心功能的选项。
b) 使用连接服务时，应遵循最小必要原则收集个人信息。
   1） 用户数据，模糊地理位置（如基于网络定位获取的街区级位置）、设备标识符（如经过匿名化处理的 OAID）。如无特殊必要且未获用户明确单独同意，不应收集用户的精准实时

经纬度坐标。收集用于热点定位辅助的传感器数据时，应在端侧进行匿名化处理，确保数据无法回溯至特定个人。

2） 网络数据，周边 WiFi 热点的 SSID、BSSID。

c） 收集的个人信息应在其使用目的达成后的合理时间内及时删除或进行匿名化处理。

7 管理要求

7.1 访问控制与审计

访问控制与审计应满足T/TAF 148 6.2.2要求。

7.2 组织架构

组织架构应在满足T/TAF 148 6.2.5要求的基础上，明确用户服务和权益保护的牵头管理部门和负责人。

7.3 机制制度

机制制度应在满足T/TAF 148 6.2.6基础上，满足如下要求：

a） 应建立全生命周期个人信息保护机制；

b） 应健全考核问责制度；

c） 应参照 T/TAF 209 制订合规开发管理规范，覆盖需求、设计、开发、测试、发布全生命周期的合规开发流程，将个人信息保护要求融入其中；

d） 应制定测试管理规范：

1） 明确测试计划和测试流程，确保测试覆盖所有用户权益保护相关的典型场景和操作流程；

2） 按照测试计划和流程执行，详细记录测试的日期、时间、参与人员、测试用例、发现的问题、测试结果等测试过程日志，并形成测试报告；

3） 定期审查和更新测试流程，确保测试的有效性和时效性。

e） 应制定运行监测规范，实时监测产品或服务在运行时是否存在恶意程序、安全漏洞、个人信息泄露、用户投诉等情况，并建立预警和处置流程；

f） 应制定更新管理规范：

1） 明确 APP 产品的更新原则、策略、流程和回滚机制等内容；

2） 所有更新包在上线前必须通过安全与合规测试；

3） 当更新涉及重大功能变更或隐私政策调整时，应以显著方式提前告知用户变更内容和影响，并重新获取用户同意。

7.4 人员管理与考核

人员管理与考核应满足T/TAF 148 6.2.7要求。

7.5 第三方管理

第三方管理应满足T/TAF 148 6.2.8要求。

7.6 影响评估

影响评估应满足T/TAF 148 6.2.9要求。

7.7 安全审计

安全审计应满足T/TAF 148 6.2.10要求。

7.8 保护技术

保护技术应满足T/TAF 148 6.2.11要求。

7.9 事件应急处置

事件应急处置应满足T/TAF 148 6.2.12要求。

附 录 A
（资料性）
Android 系统接口

提供公众无线局域网连接服务的APP在Android系统进行连接服务时调用的接口见表A.1。

表A.1 Android系统接口

接口名称	API
API 类名	android.net.wifi.WifiManager
	android.net.wifi.WifiConfiguration
	android.net.wifi.WifiManager$ActionListener
连接 WiFi	WifiManager.connect(int networkId, ActionListener listener)
	WifiManager.connect(WifiConfiguration config, ActionListener listener)
	WifiManager.reconnect()
	WifiManager.addNetwork(WifiConfiguration config)
	WifiManager.enableNetwork(int netId, boolean attemptConnect)
	WifiManager.updateNetwork(WifiConfiguration config)
断开 WiFi	WifiManager.disconnect()
	WifiManager.disable(int netId, ActionListener listener)
	WifiManager.disableNetwork(int netId)
删除 WiFi	WifiManager.removeNetwork(int netId)
	WifiManager.forget(int netId, ActionListener listener)
注：以上接口选自 Android 8.0 及以上版本，请参考 Android 系统版本为 15.0 及以上的主流版本调用接口，	

附　录　B
（资料性）
鸿蒙系统接口

提供公众无线局域网服务的APP在鸿蒙系统进行连接服务时调用的接口见表B.1。

表B.1　鸿蒙系统接口

接口名称	API
添加候选网络配置	wifiManager.addCandidateConfig
使用该接口连接候选网络	wifiManager.connectToCandidateConfig
注：以上接口选自鸿蒙 5.0及以上版本，如行业系统版本有更新，以最新接口为准。	

参 考 文 献

[1] 《中华人民共和国个人信息保护法》，2021 年 8 月 20 日

电信终端产业协会团体标准

公众无线局域网接入服务 APP 业务框架安全与个人信息保护要求

T/TAF 321—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
电子版下载网址：www.taf.org.cn