

ICS 33.050

CCS M 30

团体标准

T/TAF 252—2024

基于手机号码的移动应用认证技术要求

Technical requirements for mobile application authentication based on
cell phone number

2024-11-01 发布

2024-11-01 实施

电信终端产业协会 发布

目 次

前言	II
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 技术架构	2
6 业务流程	2
7 功能要求	3
7.1 应用 APP 客户端功能	3
7.2 应用 APP 服务功能	4
7.3 应用接入系统功能	4
7.4 号码认证系统功能	4
8 性能要求	5
8.1 应用 APP 客户端性能	5
8.2 应用接入系统性能	5
8.3 号码认证系统性能	5

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提出并归口。

本文件起草单位：联通在线信息科技有限公司、中国联合网络通信集团有限公司、中国信息通信研究院、国民认证科技（重庆）有限公司、郑州信大捷安信息技术股份有限公司、北京一砂信息技术有限公司。

本文件主要起草人：梁斌、张宏星、程福兴、袁琦、王九九、杨亮、张林、徐慧姣、王昱龙、穆向宇、曹德光、俞永贵、高军、刘献伦、李俊、刘萧萧、闫彦、张楚、路如毅。



基于手机号码的移动应用认证技术要求

1 范围

本文件规定了基于手机号码的移动应用认证技术要求，包括技术架构、业务流程、功能要求和性能要求。

本文件适用于运营商、互联网服务提供商，为基于手机号码的移动应用身份认证技术设计、开发和运营提供技术依据。

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。

GB/T 25069—2022 信息安全技术 术语
YD/T 3039—2023 移动应用软件安全技术要求
T/TAF 057—2020 移动智能终端应用软件SDK安全

3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

软件开发工具包 software development kit (SDK)

一组软件开发工具组成的可安装包，通常具有编译器、调试器、软件框架和接口实现等来方便应用程序编写的工具集合，又称软件开发包。

3.2

置换码 access code

一组具有时效性的随机数编码，用于获取真实手机号码，具有唯一性，且使用一次后立即失效。

4 缩略语

下列缩略语适用于本文件。

SDK: 软件开发工具包 (Software Development Kit)

APP: 手机应用软件 (Mobile Application)

UE: 用户设备 (User Equipment)

5 技术架构

基于手机号码的移动应用认证技术架构由UE侧、应用服务端侧和运营商侧组成，如图1所示，包括应用APP客户端（SDK）、应用APP服务端、应用接入系统、号码认证系统，具体如下：

- a) 应用 APP 客户端（SDK）：应用 APP 客户端位于 UE 侧，在内部集成 SDK 组件（由运营商提供），负责发起手机号码移动应用认证请求，应用 APP 客户端与应用 APP 服务端共同实现基于手机号码的移动应用认证登录；
- b) 应用 APP 服务端：应用 APP 服务端位于应用服务端侧，和 APP 客户端共同实现基于手机号码的移动应用认证登录，与应用 APP 客户端、应用接入系统进行交互，负责传送置换码和手机号码；
- c) 应用接入系统：应用接入系统位于运营商侧，应用接入系统负责转发应用接入鉴权请求，向号码认证系统获取认证凭据，提供应用鉴权和号码认证系统服务地址，并转发置换码和手机号码片段；
- d) 号码认证系统：号码认证系统位于运营商侧，负责生成认证凭据和置换码，通过置换码置换手机号码。

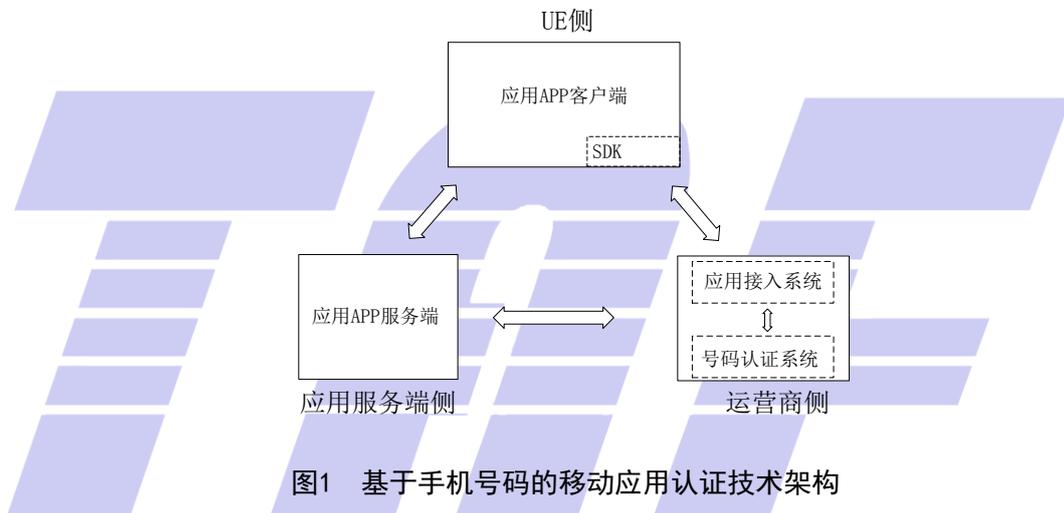


图1 基于手机号码的移动应用认证技术架构

6 业务流程

基于手机号码的移动应用认证业务流程如图2所示，具体如下：

- a) 用户点击并启动应用 APP 客户端，应用 APP 客户端调用 SDK；
- b) SDK 向应用接入系统发起预取手机号码的请求消息；
- c) 应用接入系统向 SDK 返回携带号码认证系统服务地址的响应消息；
- d) SDK 根据号码认证系统服务地址发起访问号码认证系统请求消息；
- e) 号码认证系统向 SDK 返回携带认证凭据的响应消息；
- f) SDK 向应用接入系统发送携带认证凭据的认证请求消息；
- g) 应用接入系统转发携带认证凭据的认证请求消息；
- h) 号码认证系统向应用接入系统返回包含置换码和手机号码片段的响应消息；
- i) 应用接入系统向 SDK 转发包含置换码和手机号码片段的响应消息；
- j) SDK 启动请求授权，应用 APP 客户端显示授权登录页面，向用户展示手机号码片段；
- k) 用户点击确认登录后，应用 APP 客户端向 SDK 发送确认登录消息；
- l) SDK 向应用 APP 客户端传递置换码；

- m) 应用 APP 客户端向应用 APP 服务端传递置换码；
- n) 应用 APP 服务端使用置换码和身份验证参数，向应用接入系统发起置换真实手机号码的请求消息；
- o) 应用接入系统向号码认证系统转发置换真实手机号码的请求消息；
- p) 号码认证系统向应用接入系统返回携带真实手机号码的响应消息；
- q) 应用接入系统向应用 APP 服务端转发携带真实手机号码的响应消息；
- r) 应用 APP 服务端接收携带真实手机号码的响应消息，使用真实手机号码进行授权登录，向应用 APP 客户端返回授权登录结果；
- s) 应用 APP 客户端页面显示用户通过真实手机号码登录成功。

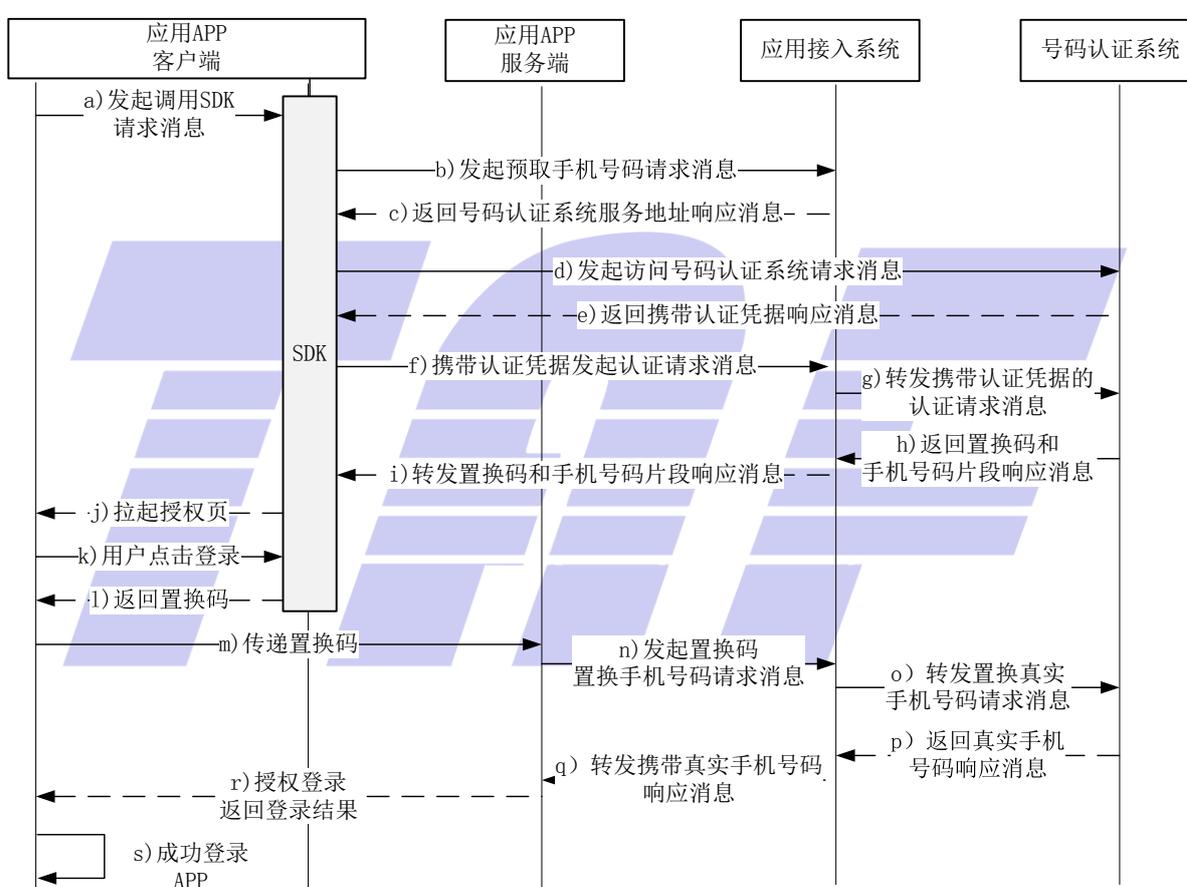


图2 基于手机号码的移动应用认证业务流程

7 功能要求

7.1 应用 APP 客户端功能

应用APP客户端通过集成SDK的方式，实现手机号码认证服务，应满足以下功能要求：

- a) 在发起号码认证前，应用 APP 客户端应初始化 SDK 的执行环境；
- b) 在发起号码认证服务时，应用 APP 客户端应调用 SDK 获取置换码和手机号码片段；
- c) 在预取手机号码时，应用 APP 客户端应调用 SDK 传递安全加密参数；

- d) 在应用 APP 客户端和服务端之间传输安全参数时,应用 APP 客户端应采用机密性和完整性保护机制;
- e) 在接收 SDK 启动请求授权后,应用 APP 客户端应在授权登录页面显示用户手机号码片段;
- f) 应用 APP 客户端安全要求应符合 YD/T 3039—2023。
- g) SDK 应支持初始化和设置安全加密参数;
- h) SDK 应获取应用包的唯一标识名;
- i) 在 SDK 发起预取手机号码请求前,SDK 应获取系统网络访问能力,包括:1) 获取联网状态,以区分用户设备是移动网络或 Wi-Fi;2) 查询终端 IP 地址;3) 同时开启 Wi-Fi、蜂窝网时,可将网络接入切换为蜂窝网;
- j) 在预取手机号码过程中,SDK 应支持采用基于密码技术的机密性和完整性保护向应用接入系统传输安全参数;
- k) SDK 应支持接收认证凭据,支持接收并缓存置换码和手机号码片段;
- l) 用户授权后,SDK 应向应用 APP 客户端传递置换码和手机号码片段;
- m) SDK 安全要求应符合 T/TAF 057—2020。

7.2 应用 APP 服务功能

基于手机号码的移动应用认证的应用 APP 服务端,应满足以下功能要求:

- a) 用户在应用 APP 客户端确认登录后,应用 APP 服务端应向应用接入系统传递置换码;
- b) 在用置换码置换手机号码时,应用 APP 服务端应支持获取真实手机号码;
- c) 在应用 APP 服务端和应用接入系统之间传输安全参数时,应用 APP 服务端应采用机密性和完整性保护机制。

7.3 应用接入系统功能

基于手机号码的移动应用认证的应用接入系统,应满足以下功能要求:

- a) 在预取手机号码请求过程中,应用接入系统可提供号码认证系统服务地址;
- b) 在预取手机号码请求过程中,应用接入系统应对 SDK 请求的安全参数进行验证;
- c) 在预取手机号码请求过程中,应用接入系统对 SDK 请求的安全参数验证通过后,可向号码认证系统转发认证凭据;
- d) 在预取手机号码请求过程中,应用接入系统校验 SDK 请求错误时,可向 SDK 返回异常错误码及必要的提示信息;
- e) 在置换码置换手机号码阶段,应用接入系统可向号码认证系统请求真实手机号码,并将收到的置换码和手机号码片段进行转发;
- f) 应用接入系统应支持账号及权限管理,支持新增系统管理账号,并设置管理账号的基本信息和操作权限;支持删除系统管理账号及相关信息;支持修改系统管理账号的基本信息及操作权限;
- g) 应用接入系统可支持日志管理,对所做的各种操作的日志记录、日志删除、日志查询及日志统计管理;
- h) 应用接入系统可支持业务管理,统计业务运营中的数据信息,并提供统计信息的详细列表等。

7.4 号码认证系统功能

基于手机号码的移动应用认证的号码认证系统,应满足以下功能要求:

- a) 号码认证系统可支持应用接入申请与管理;
- b) 号码认证系统应支持生成和缓存唯一认证凭据,支持一次一码,即认证凭据使用一次后立即失效;

- c) 号码认证系统应支持实时预取手机号码片段功能，根据认证凭据获取；
- d) 号码认证系统应支持生成替换码，根据蜂窝网 IP 地址和请求信息绑定替换码；
- e) 号码认证系统应支持唯一替换码过时不可用，具备时效性；
- f) 号码认证系统应支持替换码实时查询手机号码功能；
- g) 号码认证系统应支持对移动应用认证业务信息实施访问控制，仅允许运营商管理员访问，管理员可以查询和统计应用接入信息和应用认证服务信息，应用认证服务信息包括：认证时间、认证应用、认证结果等；
- h) 号码认证系统应支持黑白名单管理，能够基于服务地址配置应用的黑白名单功能，只有属于白名单范围内的应用才可以访问号码认证平台；
- i) 号码认证系统应支持日志管理，对所做的各种操作的日志记录、日志删除、日志查询及日志统计管理；
- j) 号码认证系统应支持对系统运行状况通过自动检测、告警、监控等方式实现实时观测；
- k) 号码认证系统应具有安全防御能力，防止非法入侵。

8 性能要求

8.1 应用 APP 客户端性能

应用 APP 客户端进行基于手机号码的移动应用认证登录时间应不大于 10 秒。

8.2 应用接入系统性能

基于手机号码的移动应用认证的应用接入系统，应满足以下性能要求：

- a) 应用接入系统从接收到请求消息，到返回响应消息的时间间隔平均不超过 2 秒，最大不能超过 10 秒；
- b) 应用接入系统每秒钟应能够处理不少于 10000 个并发的用户请求。

8.3 号码认证系统性能

基于手机号码的移动应用认证的号码认证系统，应满足以下性能要求：

- a) 号码认证系统从接收到请求消息，到返回响应消息的时间间隔平均不超过 2 秒，最大不能超过 10 秒；
- b) 号码认证系统每秒钟应能够处理不少于 10000 个并发的用户请求。

电信终端产业协会团体标准
基于手机号码的移动应用认证技术要求

T/TAF 252—2024

*

版权所有 侵权必究

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