ICS 35.240
L 60

# 团 体 标 准

T/ISC 0049—2024

# 匿名订阅通信服务技术规范

Technical Specifications for Anonymous Subscription Communication Services

2024-6-12 发布 2024-7 -12 实施

中 国 互 联 网 协 会 发 布

# 目　录

# 前　言

本标准按照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》给出的规则起草。

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这些专利的责任。

本标准由中国互联网协会归口。

本标准主要起草单位：中国信息通信研究院、中互智安（北京）科技有限公司、泰尔卓信科技（北京）有限公司、中互数科（北京）科技有限公司、中移动信息技术有限公司、联通数字科技有限公司、联通在线信息科技有限公司、天翼数字生活科技有限公司、中国移动通信集团天津有限公司、中国移动通信集团广东有限公司、中国移动通信集团湖南有限公司、中国移动通信集团江苏有限公司、中国电信股份有限公司上海分公司、中国联合网络通信有限公司无锡市分公司、新华网、人民网、北京火山引擎科技有限公司。

本标准主要起草人：王景尧、吴荻、范杰、郄世杰、田丰、秦丽芳、吴宝学、王娅琼、潘登，彭赫，马慕荻、梁斌、程福兴、牟建华、黄文建、任伟权，冯敏，刘炜、邢玉成，田雷，张杰、余刚、周二武、刘俊孜、张敦、吴刚、金韡、路成杰、陈建兵、童天、王美华、陈妙、冯维、胡增光、许朝夕、严忱、葛振斌、乔伟、孙华超、盛琨、林扬。

# 引　言

近年来，用户个人信息泄露事件频频发生，用户受到垃圾短信、骚扰电话带来的巨大困扰，也使得一些不法分子利用其开展诈骗等违法犯罪活动，给消费者带来无可挽回的损失。随着相关法律的颁布和实施，个人用户对于信息质量和信息安全的要求正在不断提高。同时，企业业务开展及用户经营过程中，普遍存在获客成本高，新客转化难，存客唤活难的问题。想要解决这些问题，除了考验产品业务设计及用户运营策略外，有效的用户触达渠道也是关键。目前，短信或电话仍然是对企业来说较为高效的用户触达方式，但近年来手机号码泄露事件频频发生，越来越多的用户注重隐私保护，使得企业通过电话或短信触达用户的效率逐步降低。企业生产经营及用户个人信息保护的矛盾日益凸显。

本规范旨在破解上述矛盾，提出并规范基于用户授权的匿名订阅通信服务技术规范。包括体系架构、功能要求、技术要求以及安全要求。规范国内电信运营商、公信第三方机构、服务应用方企业等主体遵循标准要求开发统一的技术架构及业务平台，方便技术开发者及相关应用接入、减小维护成本。

# 匿名订阅通信服务技术规范

## 1 范围

本标准规定了基于用户授权的匿名订阅通信服务技术规范，包括体系架构、功能要求、性能要求以及安全要求。

本标准适用于指导基于用户授权的匿名通信服务场景下，相关的电信运营商、公信第三方机构、应用方企业等，对匿名订阅通信服务技术平的设计、研发、合作及应用。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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／Z 28828-2012 信息安全技术 公共及商用服务信息系统个人信息保护指南》

《GB／T 35273-2020 信息安全技术 个人信息安全规范》

《GB／T 41479-2022 信息安全技术 网络数据处理安全要求》

《YD /T 3747-2020 区块链技术架构安全要求》等

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1 短信息服务（Short Message Service, SMS）

是指利用电信网向移动电话、固定电话等通信终端用户，提供有限长度的文字、数据、声音、图像等信息的电信业务。。

### 3.2 语音呼叫服务（Voice Call Service，VCS）

指利用电信网向向移动电话、固定电话等通信终端用户,提供的端到端的双向话音，以及以语音方式开展的国内呼叫中心、国内多方通信服务等电信业务。

### 3.3 匿名订阅通信服务（Anonymous Subscription Communication Services，ASCS）

指在相关业务环节单独提示并取得用户授权订阅确认的前提条件下，应用企业发起服务并得到公信第三方机构及电信运营商的授权验证后，向用户发起的通信服务，通信服务一般包含短信息服务及语音呼叫服务。

### 3.4 订阅授权（Subscription Authorization，SA）

指用户对相关消息触达服务发起的主动授权行为。

### 3.5 匿名标识（Anonymous Identifier，AID）

指针对匿名订阅通信服务场景下，针对用户生成的可变更的用户识别编码，该标识同用户授权绑定，机构间隔离，且具有有效期管理机制。通过该标识结合其他信息仅可在电信运营商内部转换关联出用户手机号，在其他参与方，仅基于该标识无法还原追踪出用户手机号。

### 3.6 授权存证（Authorization Evidence，AE）

指将用户对企业的授权数据存入到区块链中，形成可监管、可追溯、防篡改的存证数据的行为。

### 3.7 通信存证(Communication Evidence，CE)

指将企业对用户的通信触达记录数据存入到区块链中，形成可监管、可追溯、防篡改的存证数据的行为。

## 4 匿名订阅通信服务体系架构

匿名订阅通信服务体系架构如下：

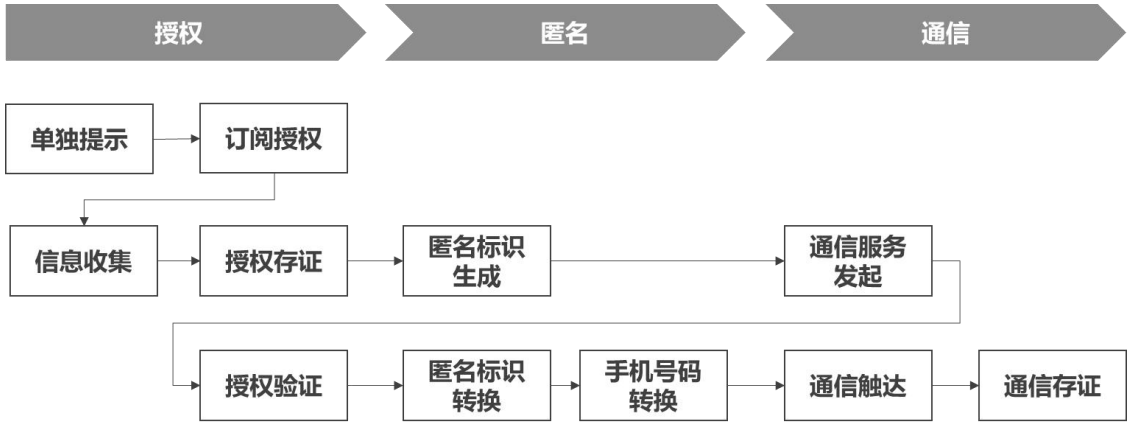


图1 匿名订阅通信服务体系架构图

匿名订阅通信服务体系总体架构包含授权、匿名、通信三个过程，其中：
授权过程包含单独提示、订阅授权、信息收集、授权存证、授权验证等相关功能环节；
匿名过程包含匿名标识生成、匿名标识转换、手机号码转换等相关功能环节；

通信过程包含通信服务发起、通信触达、通信存证等相关功能环节。

## 5 匿名订阅通信服务生态架构

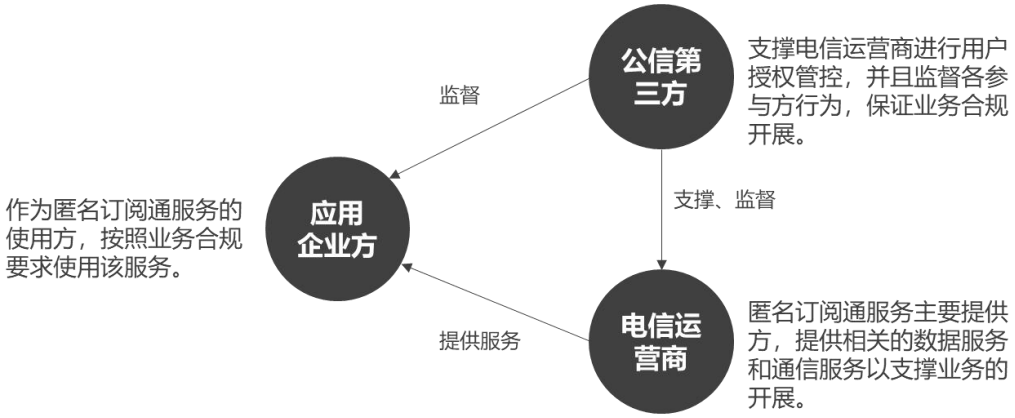


图2 匿名订阅通信服务生态架构

**应用企业方**：作为匿名订阅通信服务的使用方，需要按照业务合规要求面向个人用户进行服务单独提示并且提供订阅授权功能，在用户主动订阅授权的情况下，收集用户信息并使用匿名订阅通信相关服务。需依据业务的开展要求需设置应用企业方准入条件，并执行相关准入审批流程，此处不做详细约束，以实际业务开展情况为准。

**公信第三方**：作为匿名订阅通信业务的公信第三方，负责用户授权存证平台的构建及运营，并且基于该平台负责用户授权存证管理及围绕用户授权进行的用户匿名标识生成、失效及验证，以支撑电信运营商进行用户授权管控，并且监督各参与方行为，保证业务合规开展。

**电信运营商**：作为匿名订阅通服务主要提供方，在授权核验通过的前提下，提供相关的号码转化服务和通信服务（一般包含短信息服务及语音呼叫服务）等以支撑业务的开展。

## 6 匿名订阅通信服务各方平台功能要求

### 6.1 匿名订阅通信服务业务使用方平台功能要求

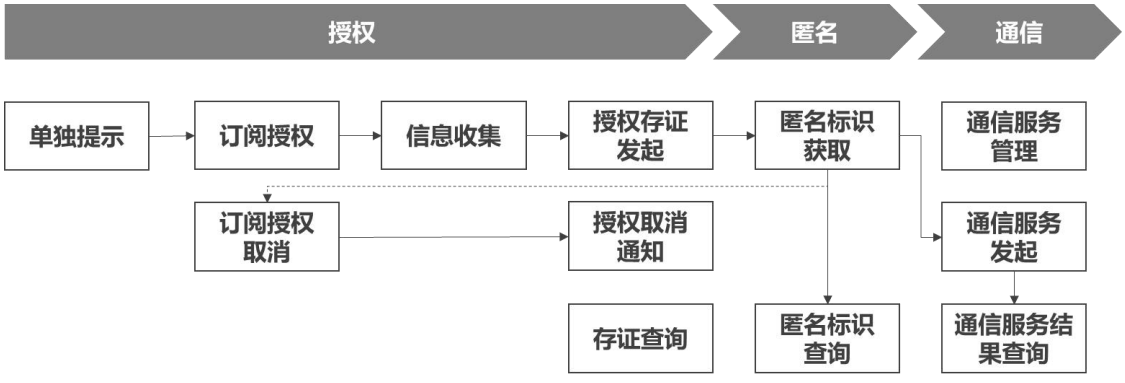


图3 匿名订阅通信服务-业务使用方体系架构图

#### 6.1.1 授权

##### 6.1.1.1 单独提示

在单独提示环节，应用企业应提供针对匿名订阅通信服务功能的单独提示授权页面。在页面中需包含如下关键节点：

- 匿名订阅通信服务授权确认功能，用户应有权选择是否同意其个人信息被收集和使用，以及在何种程度上使用；
- 匿名订阅通信服务授权协议简化版，并在简化版中明确服务运营主体、服务提供主体、服务内容及授权服务期限，同时附上服务授权协议完整版（或有）及涉及的个人信息保护政策相关条款链接，支持相关落地页面跳转。其中，授权服务期限建议可供用户自行选择。另外，个人信息保护政策中需列明涉及采集共享的信息项。
- 匿名订阅通信服务业务要点提示，需包括：
  - 明确告知用户应用企业无法获取用户手机号，仅能获取匿名标识，该标识仅在授权其内有效。
  - 告知用户订阅授权该服务后，应用企业将在什么时间段、以何种频率、通过什么号码向用户发送短信或者拨打电话。
  - 告知用户如何进行订阅授权的取消或者撤销，例如提供授权取消的网址、App内操作路径、有效的人工服务联系方式等。

##### 6.1.1.2 订阅授权

匿名订阅通信服务业务使用方平台中应包含明确的用户订阅授权确认行为，可在单独提示页面中设置相关按钮或通过其他方式。

平台需采用必要的技术手段确保用户订阅授权行为的真实性，并支持协助公信第三方及电信运营商确认用户订阅授权的真实性和有效性。

##### 6.1.1.3 信息收集

匿名订阅通信服务涉及用户信息的收集、存储及传输工作，应用企业应在用户授权范围内收集的用户信息，仅收集实现服务目的所必需的最少量个人信息，涉及的用户信息主要为用户设备标识或虚拟标识，包括：IMEI、IMSI、OAID、IDFA、卓信ID、通过电信运营商网关信令能力识别用户生成的用户标识等其中的一种或多种。

匿名订阅通信服务所涉及的信息收集、存储及传输工作，应采用对应的加密措施，采用的密码技术应遵循国家密码管理部门与行业主管部门要求，优先使用国家推荐密码算法，如SM2、SM3、SM4等。

##### 6.1.1.4 授权存证发起

匿名订阅通信服务业务使用方平台应包含授权存证发起功能，应用企业获得用户针对匿名订阅通信服务的相关授权后，应将用户授权协议信息提取并采用对应加密措施加密，连同加密后的用户设备标识或虚拟标识传输至公信第三方进行授权存证并生成同用户授权绑定的用户匿名标识。

##### 6.1.1.5 订阅授权取消

匿名订阅通信服务业务使用方平台应包含订阅授权取消功能，应用企业应向用户提供取消或者撤回匿名订阅通信服务订阅授权的功能，同时应在用户授权页面告知用户如何进行订阅授权取消或撤回，例如提供授权取消操作的网址、App内操作路径、有效的人工服务联系方式等。

#### 6.1.1.6 授权取消通知

匿名订阅通信服务业务使用方平台应包含授权取消通知功能，用户通过应用企业提供的方式进行匿名订阅通信服务授权取消后，应用企业应立即通知公信第三方，公信第三方更新用户授权存证状态为失效，并将绑定的用户匿名标识置为失效状态，匿名标识失效后，企业不可使用该匿名标识进行用户通信触达。

#### 6.1.1.7 存证查询

匿名订阅通信服务业务使用方平台应包含存证查询功能，应用企业可通过用户匿名标识查询用户授权存证及授权存证项下通信存证信息。

### 6.1.2 匿名

#### 6.1.2.1 匿名标识获取

匿名订阅通信服务业务使用方平台应包匿名标识获取功能，应用企业完成授权存证后，从公信第三方获取同用户授权绑定的用户匿名标识。

用户匿名标识具有有效期管理机制，有效期即为用户授权有效期，匿名标识到期自动失效，也支持用户主动取消授权失效。企业无法使用失效的用户匿名标识对用户进行通信触达。

#### 6.1.2.2 匿名标识查询

匿名订阅通信服务业务使用方平台应包匿名标识查询功能，应用企业可通过用户匿名标识从公信第三方查询当前用户匿名标识的状态信息，方便应用企业内部对用户匿名标识进行生命周期的管理。

### 6.1.3 通信

#### 6.1.3.1 通信服务管理

匿名订阅通信服务业务使用方平台应包含短信息服务管理和语音呼叫服务管理相关功能：

- 短信息服务管理应包括短信通道及端口管理、短信签名及模板管理、黑白名单管理、敏感词管理等。
- 语音呼叫服务管理应包括码号及线路管理、黑白名单管理、呼叫频率和地区管理、呼入和呼出管理、语音并发管理等。

#### 6.1.3.2 通信服务发起

匿名订阅通信服务业务使用方平台应该包含短信息服务任务创建和语音呼叫服务发起两种功能：

- 短信息服务支持短信息发送任务的创建，任务应支持立时发送和定时发送两种模式，创建任务时需提供用户匿名标识及短信内容等信息。如果短信接收用户回复短信时，应用企业应看到用户匿名标识而非真实的用户手机号。
- 语音呼叫服务支持语音呼叫服务的发起，服务发起时需提供被叫用户的用户匿名标识。如果被叫用户回拨时，应用企业应看到用户匿名标识而非真实的用户手机号。

#### 6.1.3.3 通信服务结果查询

匿名订阅通信服务业务使用方平台应包含通信服务结果查询功能，应用企业可查询通信服务结果状态：

- 短信息服务支持查询短信息发送任务状态、任务详情、话单等信息。
- 语音呼叫服务支持查询语音呼叫接通状态、通话时长、任务详情、话单等信息。

通信服务结果中应保证应用企业只能看到用户匿名标识，不返回显示任何用户手机号信息。

#### 6.1.3.4 其他

匿名订阅通信服务业务使用方平台还应包含必要的平台用户及权限管理、企业账户余额管理、报表管理等功能，支撑应用企业的业务运营与管控。

## 6.2 匿名订阅通信服务公信第三方平台功能要求

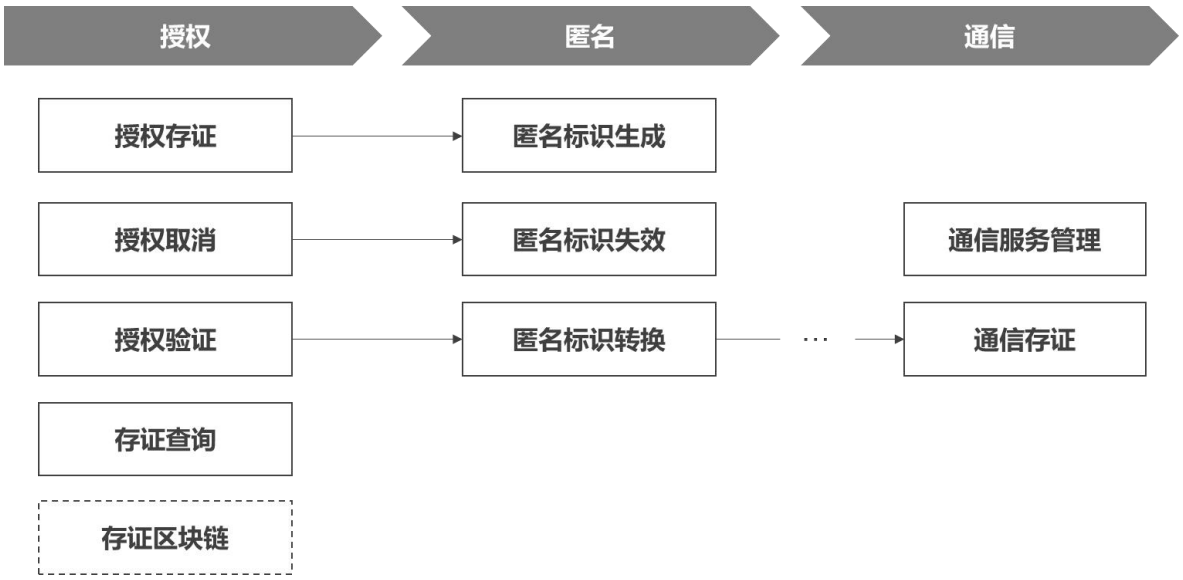


图4 匿名订阅通信服务-公信第三方体系架构图

### 6.2.1 授权

#### 6.2.1.1 授权存证

匿名订阅通信服务公信第三方平台应包含授权存证功能，应用企业获得用户针对匿名订阅通信服务的相关授权后，将用户授权协议信息提取并采用对应加密措施加密，连同加密后的用户设备标识或虚拟标识传输至公信第三方，公信第三方应验证用户授权信息的真实性和有效性后，将用户授权信息存入到存证区块链中，形成可监管、可追溯、防篡改的用户授权存证数据，方便后续相关参与方查询、验证等。

#### 6.2.1.2 授权取消

匿名订阅通信服务公信第三方平台应包含授权取消功能，用户通过应用企业提供的方式进行匿名订阅通信服务授权取消后，应用企业应及时通知公信第三方。公信第三方收到应用企业的通知后，应更新用户相关授权存证状态为失效，并将绑定的用户匿名标识置为失效状态。匿名标识失效后，企业不可使用该匿名标识进行用户通信触达。

#### 6.2.1.3 授权验证

匿名订阅通信服务公信第三方平台应包含授权验证功能，应用企业发起通信服务时提供用户匿名标识及相关通信内容等信息，公信第三方收到服务请求后，应验证应用企业提供的用户匿名标识的真实性以及其对应的用户授权的有效性，只有真实存在且授权有效的用户匿名标识，才能进行对应用户的通信触达。

#### 6.2.1.4 存证查询

匿名订阅通信服务公信第三方平台应包含存证查询功能，支持公信第三方可以通过用户匿名标识或手机号查询该用户在被投诉企业下的授权存证和通信存证信息，辅助进行业务监督和审查。

同时，也能支持在发生用户投诉时，相关监管部门可以通过用户匿名标识或手机号查询该用户在被投诉企业下的授权存证和通信存证信息，辅助进行用户投诉的审查及处理。

#### 6.2.1.5 存证区块链

匿名订阅通信服务公信第三方平台需存储并管理匿名订阅通信业务下的用户授权及通信信息，该平台底层可使用区块链技术，匿名订阅通信业务下的各参与方，包括电信运营商、业务适用方企业、监管部门等可作为区块链的节点接入，支持各方在区块链上查询、追溯相关用户授权存证及通信存证信息。

存证管理平台使用的底层技术需保证自主可控性，建议采用国产化组件或平台搭建。

### 6.2.2 匿名

#### 6.2.2.1 匿名标识生成

匿名订阅通信服务公信第三方平台应包含匿名标识生成功能，公信第三方收到应用企业提供的具有真实性保证的用户相关授权信息并完成授权存证后，应生成对应用户的用户匿名标识，并将用户匿名标识同用户授权存证关联绑定，记录用户匿名标识同连同加密后的用户设备标识或虚拟标识（例如：加加密后的IMEI、加密后的IMSI、加密后的OAID、加密后的IDFA、卓信ID、通过电信运营商网关信令能力识别用户生成的用户标识）的关联关系，然后将用户匿名标识返回给应用企业。

用户匿名标识的生成应满足以下条件：

a） 标识匿名：

1） 用户匿名标识不可逆，用户匿名标识的生成过程必须是单向的，即从用户信息到匿名标识的转换不可逆转。

2） 匿名表示生成过程中使用的相关密码算法和技术应符合国家主管部门以及相关国家标准/行业标准的要求。优先使用国家推荐密码算法，如 SM2、SM3、SM4 等，以确保匿名标识的生成过程安全可控。

3） 用户匿名标识能够抗密码分析，除生成标识的实施主体（即公信第三方）之外，其它任何机构主体无法识别和复原识别至特定信息主体。

4） 生成匿名标识如涉及使用秘钥，所使用的密钥应通过安全的密钥管理系统进行管理，包括密钥的生成、分发、存储、更新和销毁。

b） 有效期管控：

用户匿名标识具有有效期管理机制，不能为永久有效，有效期即为用户授权有效期，匿名标识到期自动失效，也支持用户主动取消授权失效。企业无法使用失效的用户匿名标识对用户进行通信触达。

c） 机构隔离：

1） 用户匿名标识在公信第三方域内具有唯一性。

2） 同一信息主体在各个应用企业方的“用户匿名标识”各不相同。

d） 有据可查：

1） 用户匿名标识生成的过程有据可查，以便于溯源。

#### 6.2.2.2 匿名标识失效

匿名订阅通信服务公信第三方平台应包含匿名标识有效状态管理功能，公信第三方应定时检查用户匿名标识对应的用户授权的有效性状态，并更新匿名标识的状态，以下关键节点必须将用户匿名标识置为失效：

- 用户匿名标识对应的用户授权被用户取消。
- 用户匿名标识对应的用户授权有效期到期。

#### 6.2.2.3 匿名标识转换

匿名订阅通信服务公信第三方平台应包含匿名标识转换功能，应用企业发起通信服务，公信第三方对应用企业提供的用户匿名标识验证通过后，公信第三方应基于应用企业提供的用户匿名标识转换为加密后的用户设备标识或虚拟标识（例如：加加密后的IMEI、加密后的IMSI、加密后的OAID、加密后的IDFA、卓信ID、通过电信运营商网关信令能力识别用户生成的用户标识），并将该标识提供给对应的电信运营商转化出用户手机号并进行通信触达。

### 6.2.3 通信

#### 6.2.3.1 通信服务管理

匿名订阅通信服务公信第三方平台应包含短信息服务和语音呼叫服务相关业务审批、监控、记录查询及报表统计等功能，例如短信息服务管理应包括短信签名及短信模板的审批及管理功能。

#### 6.2.3.2 通信存证

匿名订阅通信服务公信第三方平台应包含通信存证功能，应用方企业发起的匿名订阅通信服务在电信运营商方成功执行后，公信第三方应将针对该匿名标识用户的通信记录提取采用对应加密措施加密，然后存入到存证区块链中，形成可监管、可追溯、防篡改的用户通信存证数据，方便后续相关参与方查询、验证等。

### 6.2.4 其他

匿名订阅通信服务公信第三方平台还应包含必要的客户管理、用户权限管理等功能，支撑公信第三方对匿名订阅通信服务的业务监督、运营与管控。

## 6.3 匿名订阅通信服务电信运营商平台功能要求

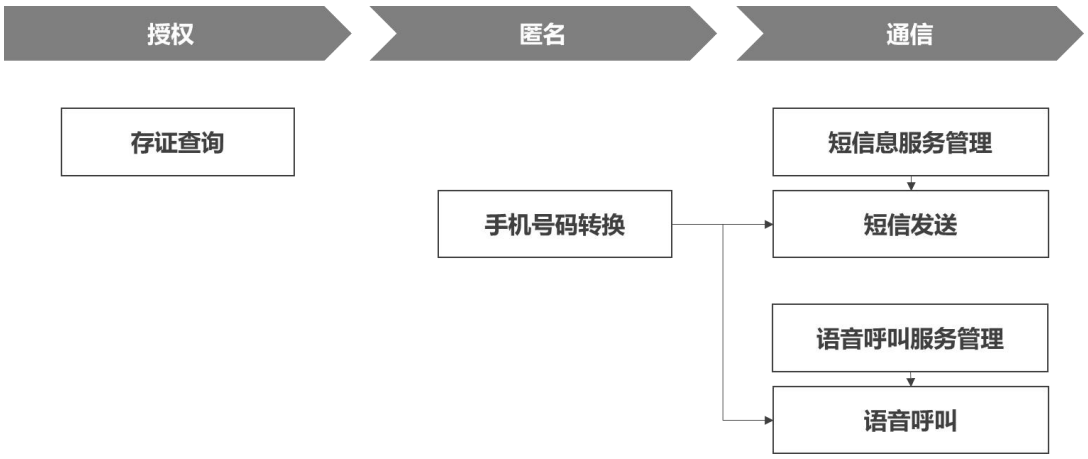


图5　匿名订阅通信服务-电信运营商体系架构图

### 6.3.1　授权

#### 6.3.1.1　存证查询

匿名订阅通信服务电信运营商平台应包含存证查询功能，电信运营商可通过用户手机号或匿名标识等查询用户授权存证及授权存证下的通信存证信息。电信运营商只能查询其自有用户的存证信息。

### 6.3.2　匿名

#### 6.3.2.1　手机号码转换

匿名订阅通信服务电信运营商平台应包含手机号码转换功能，应用企业发起通信服务并且公信第三方完成服务对应的授权验证及匿名标识转换后，电信运营商应基于加密后的用户设备标识或虚拟标识（例如：IMEI、IMSI、OAID、IDFA、卓信ID、通过电信运营商网关信令能力识别用户生成的用户标识等）转换出指定历史日期下对应的用户手机号码。

电信运营商转换出的用户手机号码，无需向外传输给供给公信第三方或应用企业方，仅在电信运营商域内传输供后续通信服务使用，以完成通信触达任务。

### 6.3.3　通信

#### 6.3.3.1　短信息服务管理

匿名订阅通信服务电信运营商平台应包含短信息服务相关管理功能，应包括短信通道及端口管理、短信签名及模板管理、黑白名单管理、敏感词管理、话单管理等。

#### 6.3.3.2　短信发送

匿名订阅通信服务电信运营商平台应包含短信发送相关功能，应支持通过用户手机号实时或者定时进行短信发送，获取并返回发送结果。

短信发送结果返回给公信第三方时应以加密后的用户设备标识或虚拟标识为ID返回，不以手机号返回，公信第三方基于加密后的用户设备标识或虚拟标识转化为用户匿名标识作为ID返回给应用企业。

如果短信接收用户回复短信时，应用企业应看到用户匿名标识而非真实的用户手机号，电信运营商可看到用户手机号信息。

#### 6.3.3.3　语音呼叫服务管理

匿名订阅通信服务电信运营商平台应包含语音呼叫服务相关管理功能，应包括码号及线路管理、黑白名单管理、呼叫频率和地区管理、呼入和呼出管理、语音并发管理、话单管理等。

#### 6.3.3.4 语音呼叫

匿名订阅通信服务电信运营商平台应包含语音呼叫功能，应支持通过手机号对用户进行语音呼叫，记录并返接通状态及通话时长等结果信息。

语音通话结果给公信第三方时以加密后的用户设备标识或虚拟标识为ID返回，不以手机号返回，公信第三方基于加密后的用户设备标识或虚拟标识转化为用户匿名标识作为ID返回给应用企业。

如果被叫用户回拨时，应用企业应看到用户匿名标识而非真实的用户手机号,电信运营商可看到用户手机号信息。

### 6.3.4 其他

匿名订阅通信服务电信运营商平台还应包含必要的客户管理、代理商管理、经销商管理等多角色机构管理功能，并且提供相关账户管理、计费管理、账单管理、报表管理及用户权限管理等功能，支撑电信运营商的匿名订阅通信业务的运营与管控。

## 7 匿名订阅通信服务各方平台非功能要求

### 7.1 可用性要求

匿名订阅通信服务各方平台应按照最大容量的80%或标准压力（系统的预期日常压力）情况下运行，能够稳定运行 7 * 24小时，并且系统的各项资源指标没有泄漏或异常。

### 7.2 可扩展性要求

匿名订阅通信服务各方平台应支持通过增加关键通信线路、关键网络设备和关键计算设备的硬件来提高系统的可扩展性。

### 7.3 可靠性要求

匿名订阅通信服务各方平台应提供通信线路、关键网络设备和关键计算设备的硬件冗余部署来保证系统的可靠性；还应提供数据的备份和恢复机制或通过数据多副本存储来提高系统的可靠性。

### 7.4 易用性要求

匿名订阅通信服务各方平台的表现和表述应贴近用户所在的环境和专业领域。对不同组成部分之间的设计目标、元素外观、交互行为模式应保持一致。针对容易引起错误发生的情况，应在用户完成提交之前系统能自行进行检查，并让用户确认。

### 7.5 可观测性要求

匿名订阅通信服务各方平台应记录详细的系统运行日志，在业务的关键点应记录业务日志、同时针对关键数据的变更也应有日志。日志的内容应包含：时间、日志级别、文件、行号、说明信息。

### 7.6 审计日志要求

匿名订阅通信服务各方平台应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。审计记录应包括事件的日期、用户、事件类型、事件是否成功及其它与审计相关的信息;应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。灾难恢复和裸机恢复、备份负载与应用程序分离、源端重复数据消重、备份数据压缩存储、异地备份。

## 8 匿名订阅通信服务各方平台安全要求

### 8.1 认证与用户管理要求

匿名订阅通信服务各方平台应在认证与用户管理方面的要求如下：

1) 系统应对登录的用户进行身份的标识和鉴别，身份标识应具有唯一性。身份鉴别机制应包含密码策略，要求密码具备一定的复杂度，并定期更换。推荐采用多因素认证机制，结合密码学方法，如数字证书、生物识别技术等，增强身份验证的安全性。
2) 系统应提供统一认证中心和用户管理中心，同时也系统应具备与企业现有的统一认证中心和用户管理中心集成的能力，以支持企业的现有安全架构。
3) 根据用户岗位职责，实施基于角色的访问控制(RBAC)，确保用户只能访问其角色对应的资源。实现管理用户的权限分离，确保关键操作需要多个角色或用户的共同授权。

### 8.2 数据存储安全要求

匿名订阅通信服务各方平台应对数据存储活动采取安全措施，包括：

4) 存储重要数据和个人信息等敏感网络数据，应采用加密、安全存储、访问控制、安全审计等安全措施;
5) 存储重要数据和信息时，不应超过与重要数据和个人信息主体约定的存储期限或个人信息主体授权同意有效期。
6) 实施基于角色的访问控制，确保用户仅能访问其角色所需的最小数据集。使用访问控制列表(ACLs)来精细管理用户和应用程序对数据的访问权限。
7) 定期对重要数据进行备份，并将备份数据存储在安全的离线位置，并制定数据恢复计划，以应对数据丢失或损坏的情况。

### 8.3 通信安全要求

匿名订阅通信服务各方平台应对数据传输活动和通信采取安全措施，包括：

8) 在数据传输过程中，使用国家认可的加密协议，例如TLS 1.2或更高版本，以确保数据传输的安全性和隐私性。
9) 采用HMAC（哈希消息认证码）或数字签名等完整性校验机制，确保数据在传输过程中未被非法篡改。
10) 在通信节点建立连接之前，实施双向身份认证机制，验证通信双方的身份，以防止身份伪造和中间人攻击。
11) 应采用密码技术对通信数据进行保密性和完整性保护，采用的密码技术应遵循国家密码管理部门与行业主管部门要求，优先使用国家推荐的安全加密算法，如SM2、SM3、SM4等。

### 8.4 系统安全要求

匿名订阅通信服务各方平台在系统安全方面的要求如下：

1) 运用防病毒软件、入侵检测系统(IDS)、防火墙等技术手段，保障执行环境的系统安全。
2) 实施白名单控制策略，仅允许已知安全的应用和服务运行。采用隐藏或掩码技术，防止侧信道攻击，如通过加密措施保护敏感信息。实施严格的访问控制策略，减少系统和网络服务的暴露面。
3) 部署流量监控系统，实时监控进出网络的流量，及时发现异常。
4) 配置DDoS流量清洗中心，对流量进行清洗，防止恶意流量进入核心网络。采用分布式防御体系，提高整体网络的抗DDoS攻击能力。
5) 实施多因素认证机制，如结合密码、生物识别、智能卡等，增强身份验证的安全性。细化访问控制策略，实施最小权限原则，确保用户只能访问其授权的资源。
6) 建立全面的安全审计系统，记录关键操作和安全事件，包括用户行为、配置变更、异常登录尝试等。实施有效的日志管理策略，确保日志的完整性、可追溯性，并定期进行日志审计。

## 8.5 区块链技术安全要求

在匿名订阅通信服务中，区块链技术用于确保用户授权和通信记录的不可篡改性和透明性，针对区块链技术在数据保护、网络通信安全、共识机制安全等方面的安全要求，应符合 YD/T 3747-2020《区块链技术架构安全要求》中的相关要求。