

团体标准

T/CCSA 553—2024

T/CAAAD 006—2024

互联网广告 投放监测及验证要求

Internet advertising - Measurement and verification requirements

2024 - 07 - 03 发布

2024 - 10 - 01 实施

中国广告协会

中国通信标准化协会

发布

目次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 广告监测 3

5.1 概述 3

5.2 桌面端广告监测 3

5.3 移动端广告监测 5

5.4 OTT 终端广告监测 7

5.5 广告监测系统性能要求 8

5.6 个人信息保护 8

5.7 用户地理位置监测要求 9

5.8 监测质量指标 9

6 广告监测指标项及其计算要求 9

6.1 曝光数 9

6.2 独立访问者数 9

6.3 点击数 9

6.4 独立点击者数 9

7 广告验证 9

7.1 广告验证概述 10

7.2 广告无效流量验证 10

7.3 广告可见性验证 12

7.4 广告品牌安全验证 13

8 广告归因 14

8.1 广告归因概述 14

8.2 广告归因机制 14

8.3 渠道归因 15

8.4 归因模型 15

8.5 数据回调 16

8.6 广告归因无效流量验证 16

附录 A（规范性） 互联网广告监测代码接口 17

A.1 参数定义 17

附录 B（规范性） SDK 监测与验证 21

B.1 设计目的、适用范围与局限 21

B.2 SDK 工作环境和关联系统模块描述 21

B.3 数据通信流程 21

B.4 广告监测及验证 SDK 配置文件 22

B.5 广告监测及验证 SDK 初始化与安全校验 22

附录 C（规范性） 回调事件 24

 C.1 回调事件规范化的必要性 24

 C.2 回调事件模板 24

参考文献 26

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。

本文件由中国广告协会和中国通信标准化协会共同提出并分别归口。

本文件起草单位：上海亦拓广告有限公司、中国信息通信研究院、秒针信息技术有限公司、上海腾徽软件科技有限公司、央视市场研究股份有限公司、北京国双科技有限公司、北京腾云天下科技有限公司、北京热云科技有限公司、中国广告协会、宝洁中国、北京京东世纪贸易有限公司、尼洱市场研究(上海)有限公司、北京巨量引擎网络技术有限公司。

本文件主要起草人：丁新勇、杨正军、朱岩、刘力泉、范秋华、汪烁雷、宋菲菲、李济景、李志强、刘柏良、刘骏、黄腾、马良骏、张国华、霍焰、杨阳、张家绮、陈婉莹、王北云、王泳帅、赫阳、王其武、张贝贝。

引 言

随着互联网的快速发展，互联网广告已经成为重要的广告投放方式和渠道。为了规范、促进互联网广告市场的健康发展，国家先后对《广告法》进行了修订，并制定了《互联网广告管理办法》。为了充分释放互联网广告的市场效能，促进互联网广告的产业化发展，使互联网广告在规范、有序的市场环境中得以快速发展，在国家主管职能部门的指导下，由行业协会组织行业品牌企业、主导媒体和互联网广告公司等，对互联网广告术语、定义、分类、缩略语提出了规范使用要求；对接口技术和投放执行过程、数据采集方法、用户数据隐私和测量要求进行了统一。

本文件旨在统一规范的互联网广告条件下：明确互联网广告监测和验证及归因等概念的维度；保证互联网广告行业运作模式的规范性和可复制性；保证互联网广告监测、验证和归因的统一性。

互联网广告 投放监测及验证要求

1 范围

本文件规定了广告监测、广告监测指标项及其计算要求，广告可见性、无效流量、品牌安全等在广告验证过程中应遵循的规范，定义了广告归因的机制及其规范。

本文件适用于各类桌面端、移动端和OTT终端上的广告监测及验证。

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 35273-2020 信息安全技术 个人信息安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

用户 user

使用互联网服务的人。

3.2

广告主 advertiser

为推销商品、提供服务或推广概念而发布广告信息的市场主体。

3.3

媒体 media

发布、展示广告的载体。

3.4

OTT终端 over the top terminal

OTT终端是以公共互联网为传输介质，以绑定了特定编号的具备网络接入功能的电视为输出终端，并由经国家广电行政部门批准的集成播控平台，向全国范围内的用户提供视频点播为主的内容服务及其他相关增值业务服务且具有能够提供应用程序开发接口的开放操作系统，并能够安装和运行应用程序的电视、盒子终端及游戏主机等。

3.5

广告网络 ad network

连接媒体和广告主的平台，将广告主的广告内容在媒体的广告位上予以呈现，实现流量资源和广告需求的对接。

3.6

需求方平台 demand side platform

帮助广告主执行广告投放策略的平台，可以设定投放金额、单价、数量、物料等执行策略。

3.7

供给方平台 supply side platform

帮助媒体进行广告资源销售的平台，记录了媒体销售的广告位、物料尺寸、售卖金额、库存等信息。

3.8

广告交易平台 ad exchange

联系广告主和媒体，或者需求方平台和供给方平台，组织竞价、撮合交易的市场平台。

3.9

广告投放 ad serving

是一种利用广告代码将广告投放到媒体上的技术或服务。

3.10

广告服务器 ad server

完成广告投放的服务器，可以是媒体自己的服务器，也可以是第三方的服务器，如广告网络、广告交易平台、需求方平台、供给方平台。

3.11

广告曝光 ad impression

根据用户的请求，广告平台向媒体发送广告素材，在媒体上开始渲染并进行一定时间的展示。

3.12

广告点击 ad click

用户与广告的有效交互行为（点击、摇晃、划动等），该行为促成广告页面的打开。

3.13

广告监测 ad measurement

对广告投放的过程及效果进行监控及测量，并对投放数据进行综合分析。

3.14

监测平台 measurement platform

采集广告曝光、广告点击等各种数据，并实现监测、验证、归因等一个或多个功能的平台。

3.15

302 重定向 302 redirect

302重定向是HTTP状态码中的302代码，通过此代码，浏览器将从一个URL临时跳转到另一个URL。

3.16

广告标识符 advertising identifier

应用于互联网广告业务的非永久性标识符，能够标记、识别互联网广告服务对象，如IDFA、OAID等。

3.17

一般无效流量 general invalid traffic

通过使用名单或者其他标准化参数、定义及预设规则可检出的无效流量。一般无效流量可通过列表和预设参数特征进行识别。

3.18

复杂无效流量 sophisticated invalid traffic

通过高级分析，多方合作、配合，乃至人工介入等方法以及广告投放活动以外更大范围的数据信号进行分析和辨识的无效流量。复杂无效流量无法直接通过特征数据列表识别，需要依靠多维度的高级分析进行识别。

3.19

广告归因 ad attribution

是用于确定促成转化的点击和展示的过程。

3.20

归因模型 attribution model

是指一条或一组规则，用于确定如何将销售/转化功劳分配给转化路径中的各个接触点。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

APP：应用（Application）

CAID：移动互联网广告标识符（CAA Advertising ID）

C2S：客户端到服务器（Client to Server）

CookieID: Cookie标识符 (Cookie ID)
DUID: 设备唯一标识符 (Device Unique Identifier)
GIVT: 一般无效流量 (General Invalid Traffic)
HTML: 超文本标记语言 (Hypertext Markup Language)
HTTP: 超文本传输协议 (Hyper Text Transfer Protocol)
IAB: 互动广告局 (Interactive Advertising Bureau)
IDFA: iOS广告标识符 (Identifier For Advertising)
IP: 互联网通信协议 (Internet Protocol)
IPv4: 互联网通信协议第四版 (Internet Protocol Version 4)
IPv6: 互联网通信协议第六版 (Internet Protocol Version 6)
JS: 一种脚本语言 (JavaScript)
MAC: 媒体存取控制位址 (Media Access Control Address)
MRAID: 移动富媒体广告接口定义 (Mobile Rich Media Ad Interface Definitions)
MRC: 媒体评级委员会 (Media Rating Council)
OAID: 匿名设备标识符 (Open Anonymous ID)
OS: 操作系统 (Operating System)
SDK: 软件开发工具包 (Software Development Kit)
SIVT: 复杂无效流量 (Sophisticated Invalid Traffic)
S2S: 服务器到服务器 (Server to Server)
TS: 时间戳 (Timestamp)
UA: 用户代理 (User Agent)
URL: 统一资源定位符 (Uniform Resource Locator)
VPAID: 视频播放器广告接口定义 (Video Player Ad Interface Definition)
XML: 可扩展标记语言 (Extensible Markup Language)

5 广告监测

5.1 概述

互联网广告的监测主要集中在三种技术环境下：桌面端、移动端和OTT终端。在不同的环境下，由于广告运行环境及技术机制的不同，广告的监测机制存在差异。

对于监测数据传输，主要存在C2S和S2S两种模式。C2S是由监测平台通过在媒体端部署的监测代码实时获得用户端触发的广告行为数据，而S2S是由媒体端将实时获取的用户触发的广告行为数据通过监测代码接口上报到媒体服务器，媒体服务器将采集到的数据实时或者批量上报到监测平台。宜采用C2S的模式，也可采用S2S的模式。两种监测模式采集的数据均应来自于用户端。实施S2S传输模式的媒体方与监测方宜定期测试数据传输质量的稳定及有效性。

5.2 桌面端广告监测

5.2.1 概述

桌面端的互联网广告展示在浏览器或客户端页面的广告模块上，各广告平台渠道将实时获取的广告行为数据通过监测代码接口上报到监测平台，监测平台负责对采集到的数据进行清洗、分析、挖掘处理，生成监测结果。

桌面端浏览器广告监测主要使用API和嵌入JavaScript两种方式实现数据上报，两种方式实现的功能一致，区别在于调用方式不同。桌面端客户端通常使用API的方式进行数据上报。

常见的桌面端广告监测流程如图1所示，图中主要模块职能描述：

- API：实现对监测代码接口上报数据的采集；
- JavaScript：实现对监测代码接口上报数据的功能进行封装的脚本语言；
- 监测平台：接收各个渠道上报的广告行为数据，并对数据进行清洗，分析和挖掘，生成测量结果；

- d) 监测代码接口：完成浏览器或客户端与监测平台之间的通信，包括各类监测的原始数据的上报。具体监测代码接口详见附录 A。

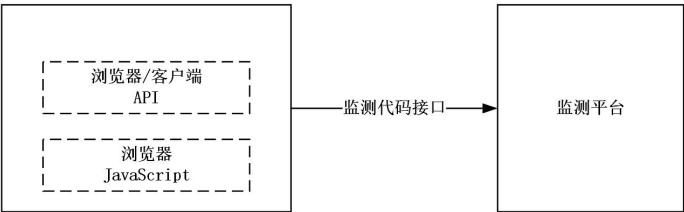


图 1 桌面端广告监测机制

5.2.2 监测流程

5.2.2.1 概述

广告行为经历三个阶段：曝光→点击→进入着陆页面。广告监测主要监控广告曝光和点击两个阶段。

5.2.2.2 广告曝光行为监测

桌面端的浏览器或客户端在需要展示广告时，即时地从广告平台加载广告，在广告素材开始渲染时，浏览器或客户端将曝光行为数据上报给监测平台。监测流程如图2所示。

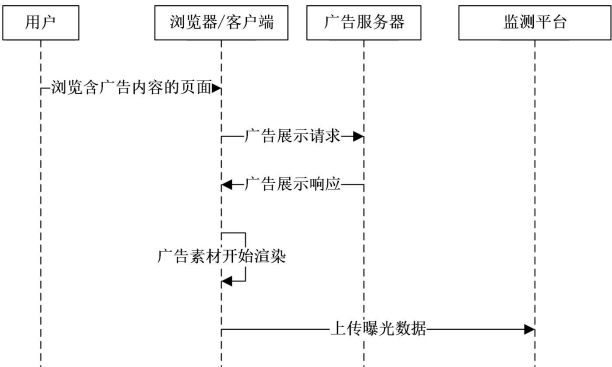


图 2 桌面端广告曝光监测流程

流程说明：

- a) 用户通过浏览器或客户端浏览广告；
- b) 浏览器或客户端实时向广告服务器请求广告创意；
- c) 广告服务器响应并返回广告创意及监测平台提供的监测代码；
- d) 广告创意开始渲染时，浏览器或客户端通过监测代码接口，将曝光数据提交到监测平台。数据格式参考附录 A。加载监测代码不应影响 Web 页面、广告的显示及排版造成可见的影响。

5.2.2.3 广告点击行为监测

5.2.2.3.1 同步模式

用户点击广告，浏览器或客户端接收到用户点击事件并处理，同时将点击行为数据上报给广告服务器，然后依次重定向到监测平台及目标站点。监测流程如图3所示。

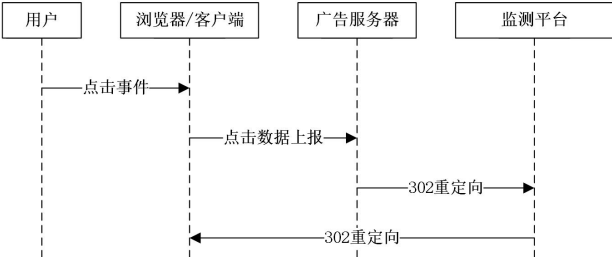


图3 桌面端广告同步模式的点击行为监测流程

流程说明：

- 用户点击广告；
- 浏览器或客户端处理点击事件，并将点击行为数据上报给广告服务器；
- 广告服务器 302 重定向且将广告点击行为数据上报给监测平台；
- 监测平台收集和处理上报的数据，详见附录 A；
- 监测平台计数完成后进行 302 重定向到目标站点。

5.2.2.3.2 异步模式

客户端广告点击行为监测也可采用异步模式。即用户点击广告，客户端触发点击后续动作的同时，将广告行为数据异步上报给监测平台。监测流程如图4所示。

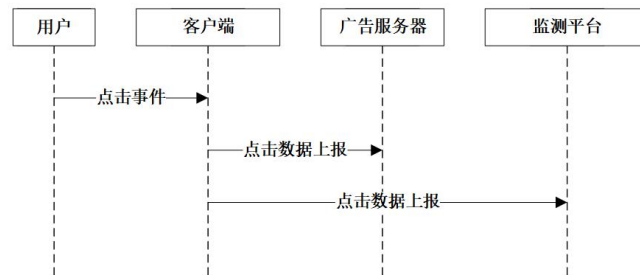


图4 桌面端广告异步模式的点击行为监测流程

流程说明：

- 用户点击广告；
- 客户端处理点击事件，并将点击行为数据上报给广告服务器；
- 客户端通过异步方式将点击数据上报到监测平台，数据格式详见附录 A。

5.3 移动端广告监测

5.3.1 概述

移动端广告监测按照广告运行环境的不同，可分为移动网站广告监测和移动客户端广告监测。其中，移动网站广告监测机制与桌面端广告的监测机制一致，参照本文件5.2执行。

对于移动客户端的广告监测，APP将实时获取的广告行为数据通过监测代码接口上报到监测平台，监测平台负责对采集到的数据进行清洗、分析、挖掘处理，生成监测结果。

常见的移动客户端监测流程如图5所示，图中主要模块职能描述：

- API：实现对监测代码接口上报数据的采集；
- 监测 SDK：实现对监测代码接口上报数据的功能进行封装的模块。在附录 B 中对其功能和实现进行了描述；
- 监测平台：接收各个渠道上报的广告行为数据，并对数据进行清洗，分析和挖掘，生成测量结果；
- 监测代码接口：完成 APP 与监测平台之间的通信，包括各类监测的原始数据的上报。具体监测代码接口详见附录 A。

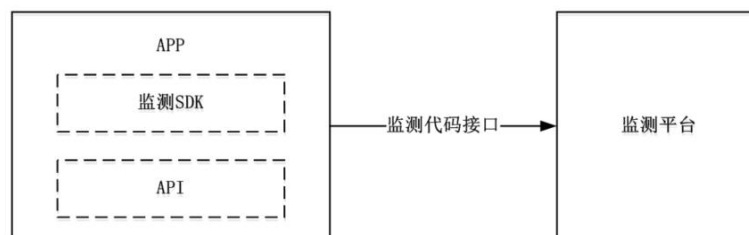


图 5 移动客户端广告监测机制描述

5.3.2 监测流程

5.3.2.1 概述

监测平台主要进行广告监测，APP将采集到的广告行为数据通过监测代码接口上报到监测平台，监测平台负责对汇总的广告行为数据进行清洗、分析、挖掘处理。

广告行为经历三个阶段：曝光 -> 点击 -> 进入着陆页面。广告监测主要针对广告曝光和广告点击行为进行监测。

5.3.2.2 广告曝光监测

APP在需要展示广告时，从广告服务器来加载广告，广告素材开始渲染时，APP将曝光数据上传给监测平台。

监测流程如图6所示。

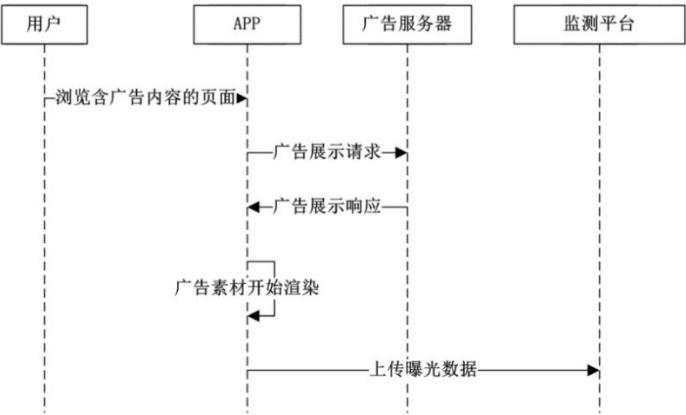


图 6 移动客户端广告曝光监测流程

流程说明：

- a) 用户浏览 APP 中包含广告内容的页面；
- b) APP 向广告服务器请求广告；
- c) 广告服务器给 APP 返回广告创意及监测平台提供的监测代码；
- d) 广告创意开始渲染时，APP 通过监测代码接口，将曝光数据提交到监测平台。数据格式详见附录 A。

5.3.2.3 广告点击行为监测

5.3.2.3.1 同步模式

用户点击广告，客户端接收到用户点击事件并处理，同时将点击行为数据上报给广告服务器，然后依次重定向到第三方监测平台及目标站点。监测流程如图7所示。

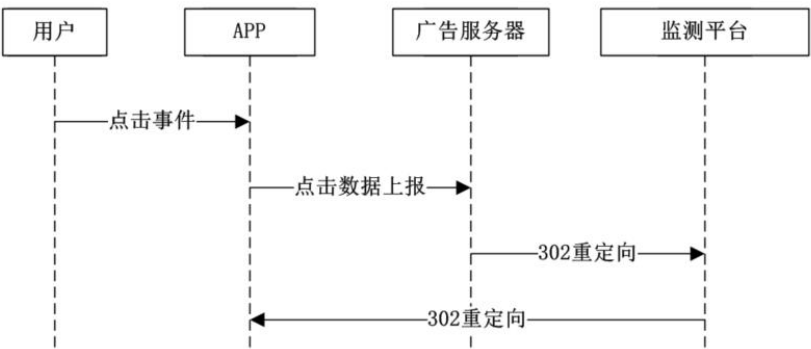


图7 移动客户端广告同步模式的点击行为监测流程

流程说明：

- 用户点击广告；
- 客户端处理点击事件，并将点击行为数据上报给广告服务器；
- 广告服务器 302 重定向到监测平台；
- 监测平台收集和处理上报的数据，详见附录 A；
- 监测平台计数完成后进行 302 重定向到目标站点。

5.3.2.3.2 异步模式

用户点击广告，APP接收到用户点击事件之后，在处理点击事件，发送点击数据给广告服务器的同时，将点击数据异步上传给第三方监测平台。

监测流程图8所示。

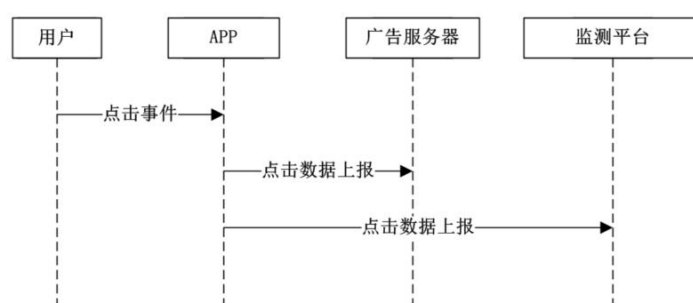


图8 移动客户端广告点击监测流程

流程说明：

- 用户点击广告；
- APP 处理点击事件，并将点击数据上报给广告服务器；
- APP 通过异步方式将点击数据上报到监测平台。数据格式详见附录 A。

5.4 OTT 终端广告监测

5.4.1 概述

OTT终端广告监测是通过统一的监测组件，实时记录OTT操作系统及应用内广告的呈现和交互等事件，再将事件数据发送到监测平台，监测平台对数据进行处理和分析，生成监测结果。

与移动客户端的广告监测类似，由监测SDK或API实时获取广告行为数据，通过监测代码接口上报到监测平台，监测平台负责对收集汇总的数据进行清洗、分析、挖掘处理，生成监测报告。

监测机制如图9所示。



图9 OTT 终端广告监测机制

其中各模块及功能包括：

- API：实现对监测代码接口上报数据的采集；
- 监测 SDK：封装有各种监测参数的获取方法，统一的监测提交的方法，相关细节部分见附录 B；
- 监测代码接口：实现 OTT 操作系统及应用与监测平台之间的通信，包括各类监测的原始数据的上报；
- 监测平台：接收各个渠道上报的广告行为数据，并对数据进行清洗，分析和挖掘，生成监测结果。

5.4.2 监测流程

监测平台主要进行广告监测，通过监测SDK或API采集OTT终端广告行为数据，再通过监测代码接口上报到监测平台，监测平台负责对收集汇总的广告行为数据进行清洗、分析、挖掘处理。

OTT终端广告行为一般有三个阶段：曝光，交互，跳转响应。OTT终端广告监测主要针对广告曝光进行监测。

OTT操作系统及应用在需要展示广告时，从广告服务器来加载广告，在广告素材开始渲染时，系统及应用将曝光数据上传给监测平台。

监测流程如图10所示。

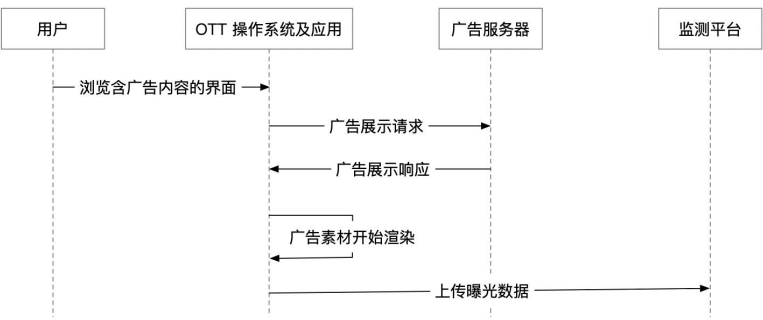


图 10 OTT 终端广告监测流程

流程说明：

- a) 用户通过 OTT 操作系统及应用浏览广告；
- b) OTT 操作系统及应用实时向广告服务器请求广告创意；
- c) 广告服务器响应并返回广告创意及监测平台提供的监测代码；
- d) 广告创意素材开始渲染时，OTT 操作系统及应用通过监测代码接口，将曝光数据提交到监测平台。数据格式参见附录 A。

5.5 广告监测系统性能要求

5.5.1 可用性

可用性要求包括：

- a) 保障线上 99.99%的可用性；
- b) 对数据有灾备和恢复方案，避免数据丢失。

5.5.2 扩展性

扩展性要求包括：

- a) 采用服务器集群方式部署监测服务器，根据流量和业务需要，灵活增减配置；
- b) 弹性带宽配置方案，确保不发生网络堵塞。

5.5.3 安全性

安全性要求包括：

- a) 保证服务器所在 IDC 机房或云机房的严格运维，确保控制网络的安全性，避免控制内网直接暴露于外网；
- b) 未经允许，机房服务提供商不得对服务器进行任何操作。包括：私自登陆服务器，开、关机等；
- c) 对服务器具有 100%的控制权；
- d) 保证机房硬件和网络的严格运维，保证硬件设备和网络正常运行，并 7×24 小时响应服务器发生的硬件或网络故障；
- e) 机房服务提供商需保证不对监测接入的域名进行过滤，保证服务器正常使用。

5.6 个人信息保护

监测平台应符合GB/T 35273个人信息处理要求。

5.7 用户地理位置监测要求

媒体方和广告监测平台应使用行业统一的IP地址信息库进行用户定向和验证。对于IP地理位置不能明确界定到城市级的广告流量（包括但不限于4G、5G移动互联网广告流量、卫星上网等广告流量），媒体、监测平台可采用综合判断广告受众常住地归属城市的逻辑来界定广告流量的城市归属。

5.8 监测质量指标

以下监测指标宜控制在误差5%之内：

——曝光数；

——点击数；

——独立访问者数。

有定向要求（如地域、人群等）的广告，广告主宜和媒体协商约定具体误差。

6 广告监测指标项及其计算要求

6.1 曝光数

每次广告曝光，当广告创意开始渲染时，由用户端向监测平台发起1次HTTP请求，并携带广告活动、广告位、用户唯一标识等信息。监测平台为收到的每次请求记录1条曝光日志。统计曝光日志的总数作为广告曝光量。HTTP请求可通过（但不限于）HTML中的、<IFRAME>、<SCRIPT>标签触发，根据实际需求，监测平台可返回（但不限于）1x1图片、HTML、JavaScript、302跳转等。监测平台应通过设置HTTP头等技术方式最大程度减少缓存对曝光数监测的影响。

6.2 独立访问者数

曝光日志中广告标识符去重后的数量应作为独立访问者数量。

基于浏览器网页环境的广告监测，包括桌面端网页和移动端网页，宜为每个新访问者分配一个广告标识符，并使用CookieID存储此标识。

基于客户端环境的广告监测，包括移动客户端、OTT终端，宜使用广告标识符作为用户唯一标识。当数据统计存在多种广告标识符时，宜根据广告标识符的有效性和可用性来综合决定采用何种用户唯一标识。

基于客户端环境广告监测的广告标识符优先级顺序为：

a) 移动客户端宜采用的优先顺序：OAID、IDFA、CAID、IP+UA；

b) OTT终端宜采用的优先顺序：OAID、MAC、IP+UA。

注：桌面客户端由于没有统一可使用的广告标识符，不做用户唯一标识选择的规定。

以下特殊情况中，对应的广告标识符不宜用于用户唯一标识：

a) 某种广告标识符因操作系统不支持而获取到程序报错、空字符串、null等特殊计算机字符取值，此种广告标识符不宜用于用户唯一标识。媒体与监测平台均应对此类广告标识符进行识别。向监测平台传输的数据宜保持对应广告标识符的宏参不替换。

b) 因用户主动选择不授权追踪而导致广告标识符被重置为缺省值，此种广告标识符不宜用于用户唯一标识。向监测平台传输的数据宜为获取到的实际值，客观反应授权行为和意愿。

6.3 点击数

每次广告点击，由访问者端向监测服务器发起1次HTTP请求。监测服务器应为收到的每一次请求记录1条点击日志。统计点击日志的总数作为点击量。

6.4 独立点击者数

统计访问者产生的点击日志中，通过广告标识符去重后得到的数量去重逻辑参照本文件6.2执行。

7 广告验证

7.1 广告验证概述

广告验证用于检查广告是否在正确且安全的设备、页面和位置中展示，以及是否被真实用户看到。广告验证包括广告无效流量验证、广告可见性验证、品牌安全验证。

7.2 广告无效流量验证

7.2.1 无效流量验证概述

无效流量是不符合某些质量或完整性标准的媒体流量或行为（与广告和其内容相关的度量指标包括受众和曝光；衍生度量指标包括点击、互动和效果等），或者不应被包括在合理计数中的流量。

无效流量验证由监测平台在广告投放环境中部署验证代码或验证SDK，对广告的真实有效性进行验证。

7.2.2 无效流量验证技术规范

监测平台应通过获取广告投放环境的数据来判断广告流量是否符合无效流量验证标准，并通过报告展示界面提供广告无效流量统计结果。

无效流量验证技术应用在桌面端、移动端和OTT终端。对于桌面端，媒体方应提供验证代码的运行环境，包括如JS、VAST、VPAID等；对于移动端和OTT终端，媒体方宜接受验证代码或验证SDK或其他等效的验证方式来提供广告验证所需获取的广告状态信息。

监测平台收集和处理上报的数据，详见附录A。验证SDK功能和实现原理，详见附录B。

7.2.3 无效流量特征

无效流量划分为“一般无效流量”和“复杂无效流量”两大类，两者具有不同的流量特征。

7.2.3.1 一般无效流量特征

一般无效流量可包含但不限于以下一种或多种特征类型：

- 来自数据中心的且不具备明确真实用户特征的流量（即来自服务器的流量而非真实用户的电脑、手机等设备的流量）；
- 来自已知的高危设备或者作弊来源IP的流量（基于数据过滤列表）；
- 来自已声明的机器人或爬虫的流量（基于数据过滤列表）；
- 用户代理信息（UA）为空及其它形式的未知浏览器带来的流量；
- 基于广告活动出现明显异常高速的用户活动、连续或重复请求、严重超出用户正常合理频次的流量；
- 采用预加载或预渲染技术并且广告创意没有被真实用户看到的流量；
- 来自已知的高危或者作弊来源APP、网站的流量（基于数据过滤列表）；
- 基本信息缺失或不一致或矛盾的流量（基本信息包含事件类型、广告活动ID、时间戳、IP地址、HTTP请求方式、设备类型）；
- 设备因硬件配件缺失而不具备渲染广告素材的能力（用户主动禁止图像展现除外），以及使用0x0或1x1等几乎不可见广告位渲染广告素材的情况而产生的流量。

7.2.3.2 复杂无效流量特征

复杂无效流量可包含但不限于以下一种或多种特征类型：

- 来自未声明的、高度模拟真人访客的机器人和爬虫流量；
- 来自广告插件和恶意软件通过欺骗行为（包括广告注入和未经授权的覆盖）产生的流量；
- 来自非专用的设备（如受计算机病毒感染被劫持的设备）自动浏览产生的流量；
- 来自专用设备（如自动化系统或工具、设备仿真器、群控设备等设备）产生的流量；
- 来自被劫持的广告代码产生的流量；
- 通过隐藏/堆叠/覆盖或其它方式导致用户没有机会看到正常广告内容的流量；
- 通过广告域名嵌套以及APPID伪造而恶意制造的流量；
- 以金钱补偿为动机的操纵测量数据行为（广告主策划或授权的营销活动除外）；

- i) 故意插入、删除、重复使用或错误匹配用户 cookieID 信息或广告标识符来伪造用户特征的流量；
- j) 操纵或伪造曝光、点击、可见度、转化、来源网址、用户同意、归因、用户人群属性、用户位置数据（主要针对有位置定向需求的广告活动）、Server Side Ad Insertion (SSAI) 等信息试图欺骗监测平台的流量；
- k) 作弊代理或无效代理流量（即通过中间代理设备实现的无效流量，包括通过代理设备操纵流量计数、创建或传输非人类流量或无法通过协议验证的流量）；
- l) 通过强制打开新浏览器窗口、强制打开标签页、强制安装移动应用程序（移动重定向）、强制点击行为、诱骗用户点击或意外点击、点击劫持（UI redress attack）和劫持测量事件所产生的流量；
- m) 故意通过盗版内容所制造的数量较大的流量。

7.2.4 一般无效流量数据列表

一般无效流量判定所依据的数据列表，由行业协会指导相关企业进行协作制作，用于增强一般无效流量的判定。简称“GIVT判定数据列表”（GIVT LIST）。

“GIVT判定数据列表”（GIVT LIST）的制作原则应遵循行业共识和实践研究，数据列表的制作宜采用开源区块链技术（或类似技术）实现数据列表制作过程开放、高效，数据结果透明、可溯源。

GIVT的判定数据列表应保持与行业需求同步，包括但不限于以下四类：

- a) 行业企业通过协作共识确认的无效流量来源 IP 地址列表（GIVT-IP 地址）；
- b) 行业企业通过协作共识确认的无效流量来源设备识别特征列表（GIVT-广告标识符）；
- c) 行业企业通过协作共识确认的无效流量来源用户代理信息特征列表（GIVT-UA 特征）；
- d) 行业企业通过协作共识确认的无效流量来源 APP、网站特征列表（GIVT-域名包名）。

GIVT判定过程中，应避免将如下已知情况所产生的流量直接判定为GIVT。这些流量形态符合一般无效流量特征的定义，但有较大可能为客观技术或机制导致的流量形态异常（即流量可能是由真人产生），简称“非透明流量判定数据列表”。包括但不限于：

- a) 行业企业通过协作研究共同确认的移动装置系统默认识别特征列表（通常由用户刷机修改操作系统、关闭广告追踪等行为而产生）；
- b) 行业企业通过协作研究共同确认的软件程序语言特殊字符移动装置识别特征列表；
- c) 行业企业通过协作共识确认的山寨设备（未获入网许可而生产的）移动装置、和使用大规模重复硬件标识符的 OTT 终端等硬件的识别特征列表；
- d) 来自媒体方实名声明为归属为其自身系统使用的 IP 地址（并使用此类 IP 作为代理触发外部广告监测系统）。

监测平台不应将命中如上“非透明流量判定数据列表”的流量判定为GIVT，宜将此类广告曝光或点击数量进行统计，并在报告中单独呈现。流量的用户唯一标识符选择机理与6.2中描述的唯一标识符选择机理相同。

对于国外一般无效流量的判定，宜使用有公信力的等效列表以增强一般无效流量的判定能力。

7.2.5 无效流量数据报告

监测平台提供的无效流量数据报告应满足如下要求：

- a) 应从媒体、广告位、设备类型等主要细分维度区分流量总数、GIVT 数、SIVT 数；
- b) SIVT 报告最长滞后延迟不应超过 14 天；
- c) 已被检出为无效流量的曝光不能计入可见曝光。可见曝光测量机构应当在判断广告曝光是否属于可见曝光的基础上增加对其是否属于无效流量的判别，并在报告中将不可见曝光类别下的无效流量单独汇报呈现。

7.2.6 程序化前置过滤

在技术环境许可的投放方式如在程序化广告投放中，宜在广告投放前基于无效流量数据预判数据结果进行流量筛选，基于无效流量预判数据放弃竞价或进行实时广告阻挡控制，即当广告无效流量概率较高或明确认定为无效流量时基于广告采购供需双方的合约做出放弃、退还、跳过、替换等广告投放控制。

7.2.7 第三方合规审计要求

提供无效流量验证服务的监测平台宜接受第三方审计。审计范围应包括但不限于计数方法和过程处理、控制、系统安全等环节。

7.2.7.1 无效流量认证要求

提供无效流量验证服务的监测平台宜接受第三方审计。审计范围应包括但不限于计数方法和过程处理、控制、系统安全等环节。

监测平台申请无效流量认证，应提供以下文档和说明：

- a) 关于保证数据完整性的说明；
- b) 关于检测一般无效流量的方法说明；
- c) 关于检测复杂无效流量的方法说明（如果提交了此审计项）；
- d) 无效流量相关的内部政策和流程（例如根据无效流量情况改进检测方法的数据分析情况和记录）；
- e) 业务合作伙伴检查的政策流程；
- f) 审计公司要求的为了理解系统、制度和流程的其他文件。

7.2.7.2 业务合作伙伴检查要求

业务合作伙伴指和监测平台有合作关系的机构。对业务合作伙伴的检查应满足如下规定和流程要求：

- a) 业务合作伙伴是否合法（例如是否有国家机关颁发的相关证件，是否有固定地址和电话联系人等，是否有相关行业机构认证等）；
- b) 业务合作伙伴是否有不良行为记录（例如被行业黑名单记录）；
- c) 业务合作伙伴的产品是否有无效流量相关的功能；
- d) 业务合作伙伴是否出于逃避无效流量检测的目的来寻求合作；
- e) 对于业务合作伙伴，应了解其相关业务流程，以及其取得的相关第三方审计认证（如果有）；对于影响无效流量检测过程的合作伙伴需要提供独立的审计认证，证明这些业务合作伙伴符合本部分；如果本部分对业务合作伙伴不适用，需保留对应的记录用于今后检查和审计。

7.3 广告可见性验证

7.3.1 可见曝光概述

数字广告在满足以下条件时可被定义为可见曝光：广告创意出现在聚焦的浏览器页面的可见空间上（移动端为终端可见空间上），并且满足设定的曝光条件。可见曝光表明广告是“有机会被看到”的。

7.3.2 计数要求

7.3.2.1 一般要求

广告可见曝光的计数，应在曝光监测的基础上，遵循如下要求：

- a) 客户端计数；
- b) 过滤无效流量。

监测平台宜在报告广告活动可见性的情况时附加说明不可见广告曝光的具体属性以及致使其不可见的原因。

7.3.2.2 展示广告可见曝光要求

像素阈值要求：广告中大于或等于50%的广告像素面积位于聚焦的浏览器页面的可见空间上（移动端为终端可见空间上），时间阈值要求：广告呈现后，满足像素呈现的时间要大于或等于连续1秒。

其他要求：

- a) 强交互可见曝光：如果能够确定用户与广告之间产生了比观看广告更强的互动，那么即使广告不符合上述像素和时间条件，也可视为发生了可见（即强用户交互可直接定义可见广告曝光）。监测平台需要披露强交互可见曝光的具体定义，并在报告中体现强交互可见曝光数；

- b) 对于没有达成可见曝光时长阈值要求的曝光，除了直接报告为不可见曝光外，也可提供其各时间分段的曝光次数报告，用来细化评估广告的价值。可将广告从未满足过面积阈值的曝光数，满足面积阈值的连续时长大于0秒、且小于等于0.5秒的曝光数，以及满足面积阈值的连续时长大于0.5秒、且小于等于1秒的曝光数分别报告。这三种数据分别称为“绝对不可见曝光”、“0~0.5秒曝光”及“0.5~1秒曝光”。

在信息流等广告格式中，也可报告次秒级曝光：即当广告被渲染后，像素的50%以上被连续观看了0.5s~1s。次秒级曝光不属于可见曝光。该指标只适用于信息流展示广告，不适用于信息流视频广告。

7.3.2.3 视频广告可见曝光要求

像素阈值要求：广告中大于或等于50%的广告像素面积位于聚焦的浏览器页面的可见空间上（移动端为终端可见空间上），时间阈值要求：广告呈现后，满足像素阈值的同时视频需要连续播放2秒，所需时间不一定是视频广告的前2秒；任何无重复内容的连续2秒广告播放都是合规的。

其他要求：

- a) 如果能够确定用户与广告之间产生了比观看广告更强的互动，那么即使广告不符合上述像素和时间条件，也可视为发生了可见曝光（即强用户交互可直接定义可见广告曝光）。监测平台需要披露强交互可见曝光的具体定义，并在报告中体现强交互可见曝光数；
- b) 对于没有达成可见曝光时长阈值要求的曝光，除了直接报告为不可见曝光外，也可以提供其各时间分段的曝光次数报告，用来细化评估广告的价值。对于视频类广告，可将广告从未满足过面积阈值的曝光数，满足面积阈值的连续时长大于0秒、且小于等于1秒的曝光数，以及满足面积阈值的连续时长大于1秒、且小于等于2秒的曝光数分别报告。这三种数据分别称为“绝对不可见曝光”、“0~1秒曝光”及“1~2秒曝光”；
- c) 对于展示广告内嵌有视频广告的特殊情况，宜以展示广告的可见性标准对整个广告进行验证。如果验证可见性的对象是视频播放器，而不是整个广告，宜将该测量方法在报告中说明。

7.3.3 广告可见性验证指南

7.3.3.1 技术机制

广告可见性验证是通过验证代码或SDK，从浏览器/客户端中获取各种参数来判断当前广告创意是否满足可见性标准，最终通过用户界面提供广告可见性统计结果。

7.3.3.2 最低验证频率

应按照以下的验证测量时间间隔执行：在验证展示类广告时，最低100毫秒一次；验证视频广告时，最低每200毫秒一次。需要至少连续10次相同的测量结果才能判定可见曝光。监测平台可不保存这些区间测量结果。

7.3.3.3 投放控制

可在投放前基于历史经验值对结果做流量筛选，在广告投放中基于可见率结果做实时广告阻挡控制（即广告可见性几率高时做投放，判断广告可见性低甚至始终不可见时基于供需双方的合约做放弃、退还、跳过、替换等广告投放控制）。

7.3.4 可见曝光验证技术规范

可见曝光的验证主要集中在三种技术环境下：桌面端、移动端和OTT终端。在不同的环境下，由于广告运行环境及技术机制的不同，广告的验证机制存在差异。

对于桌面端，根据广告类型的不同，媒体方应提供广告验证运行环境，包括如JS、VAST、VPAID等；对于移动端和OTT终端，媒体方应提供广告验证运行环境，包括如广告验证代码、MRAID、广告验证SDK等。

7.4 广告品牌安全验证

7.4.1 品牌安全概述

品牌安全验证是通过技术和其他手段验证数字广告是否出现在对广告主品牌有损害的内容旁。对品牌安全的验证既可在投放中实时进行，也可在后置测量过程中执行。

7.4.2 广告环境验证

监测平台应提供技术手段，通过在广告展示的页面上搜集特定的参数，来评估广告展示的环境。对广告展示环境的验证基于需要规避的上下文内容类型来进行，如下是潜在需要规避的内容类型：

- a) 成人内容；
- b) 协助非法活动；
- c) 有争议的主题（即违反现有的社会规范，如神秘，禁忌，反常的生活方式等）；
- d) 侵犯版权；
- e) 药物/酒精/管制药品；
- f) 极端的图像/明显暴力内容；
- g) 诱导对测量进行操纵；
- h) 仇恨/亵渎；
- i) 骚扰/间谍软件/恶意软件/盗版软件；
- j) 政治/宗教；
- k) 未经认证的由用户生成的内容；
- l) 在广告主媒介计划以外的媒体点位。

监测平台应遵循潜在规避类别并清楚地向广告主披露设定参数细节。

注：监测平台可在维护潜在规避类别的过程中做更详细的子类区分，以进一步细化和区分所提供的服务。

7.4.3 执行规范

对广告品牌安全的验证可采用如下方法来执行：

- a) 在广告展示页执行能够可见页面内容的监测方法；
- b) 爬虫方法。爬虫产生的流量必须能与人类产生的广告流量中区分出来，避免影响测量数据；
- c) 抽样执行验证方法。使用上述两种方式进行验证时，均可采用抽样方法进行品牌安全验证，但是抽样的方法及范围、计算方法必须完整披露给媒体及广告主；
- d) 人工检查，可作为技术验证手段的后续步骤进行，为验证结果提供判断依据。

7.4.3.1 广告投放控制

如广告主有明确的广告计划（如规定投放在采购的网站列表或视频网站内的广告），则媒介计划外的广告投放是不满足品牌安全要求的。移动端广告投放时应有机制返回APP包名以确认投放地点。如应用APP属于不满足品牌安全的分类，应阻止广告投放至该APP。

媒体可使用iFrame来投放，但宜依据最小化原则使用跨域iFrame。

8 广告归因

8.1 广告归因概述

广告归因是用于追溯促成目标转化效果的指定广告触点行为的过程。媒体在其广告位中为用户展示相应广告，用户产生广告触点行为（以广告浏览或点击为例）并在目标推广的APP或落地页中产生转化行为时，监测平台将接收这些数据，并通过相应的归因模型进行广告效果渠道归因，最终将归因后的转化数据回调至为用户分发广告的相应广告服务器中，完成整个归因过程。

8.2 广告归因机制

进行广告归因宜遵循图11所述机制。

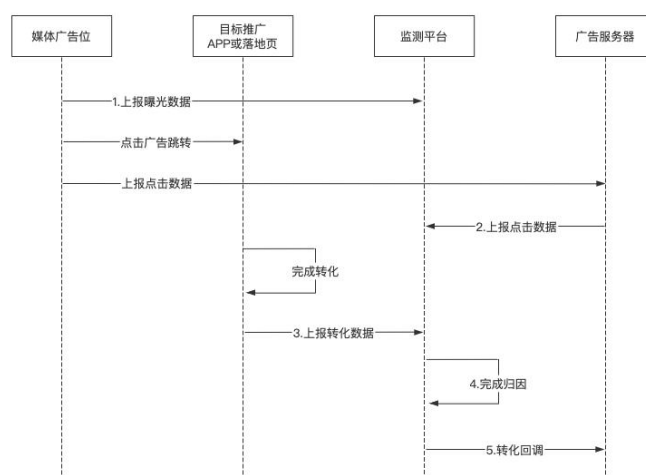


图 11 广告归因机制

流程说明：

- 1) 用户浏览广告后，由客户端向监测服务器上报告告曝光数据；
- 2) 用户点击广告后，在用户跳转至目标推广 APP 下载地址或落地页的同时，由客户端先向广告服务器上报告告点击数据，再由广告服务器向监测服务器上报告告点击数据；
- 3) 用户完成转化事件后，将通过事先在广告主 APP 内植入的监测 SDK 或落地页内嵌入的监测 JS 向监测平台上报告告用户转化数据；
- 4) 监测平台在接收到转化数据后，进行渠道归因；
- 5) 监测平台完成归因后，将通过广告服务器接口回调转化数据用作渠道广告效果优化算法，回调事件参考 8.5 所述数据回调。

8.3 渠道归因

广告投放后通常会产生一些广告主所期望的转化行为（如APP下载激活，点击广告跳转落地页等），为了实现对不同渠道之间的转化效果的评估，一般会基于可测量的方法论将其转化行为的贡献归因到不同的渠道上，主要的方法论有两类，分别适用于不同的场景：

- a) 广告标识符归因：广告行为（曝光、点击）与转化行为（激活、浏览、其他转化）的数据中至少存在一个相同的、具备唯一性的广告标识符时，可通过该标识符来确认其广告行为和转化行为的关联性；
- b) 渠道标识归因：该方法是通过为不同渠道生成不同的标识，通过判断转化时是否带着可识别的渠道标识，从而认为该用户一定时间范围内的贡献属于该渠道标识对应的渠道，常见的场景：
 - 1) 点击广告跳转到落地页：在落地页 URL 或小程序链接的参数部分拼接渠道标识；
 - 2) 在应用市场下载 APP：应用安装包投放到应用市场前，在应用安装包中预埋渠道标识。

8.4 归因模型

归因模型是指用于分析广告活动对业绩影响的一种方法。它是通过将业绩归因于不同的渠道、广告、营销活动 etc 来确定每个因素对业绩的贡献度。在数字营销中，归因模型被广泛用于评估不同渠道或广告的效果，以便优化广告投放或调整营销策略。常见的归因模型一般包括：末次归因、首次归因、线性归因、时间衰减归因、位置归因、模型算法归因以及其它归因。常见的归因周期一般默认为30天，最长一般不超过90天。

- a) 末次归因：将转化事件的功劳 100%归于用户在转化之前的归因周期内采取的最后一次行动；
- b) 首次归因：将转化事件的功劳 100%归于用户在转化之前的归因周期内采取的第一次行动；
- c) 线性归因：将转化事件的功劳平均分配给用户在转化之前的归因周期内采取的每一次行动；
- d) 时间衰减归因：将转化事件的功劳按照时间衰减的权重分配给用户在转化之前的归因周期内采取的每一次行动。越接近转化时间点的触达，比更早时间点的触达有更多的价值；

- e) 位置归因：将转化事件的功劳分配给用户在转化之前的归因周期内采取的每一次行动。其中第一次和最后一次行动得到最多的权重，其余的权重平均分配给两次触达之间的行动。通常第一次和最后一次行动分配 40%权重，其余的行动平均分配剩余的 20%权重；
- f) 模型算法归因：依据用户在转化之前的归因周期内采取的每一次行动的数据表现，利用算法将转化功劳归因于各个行动；
- g) 其它归因：因媒体平台的环境、广告主需求差异，可以根据实际需要制定不同的归因模型。

需要注意的是，使用任何一种归因模型评估广告效果时，评估者应告知广告主其所应用的归因模型的计算方式或计算原理，并且避免将不同归因模型的结果进行横向对比，以帮助广告主得到广告的效果反馈。

8.5 数据回调

8.5.1 回调的定义

将广告投放事件数据反馈给渠道方，使渠道得到投放效果反馈，从而实现优化，提高转化率。广告投放事件数据包括但不限于激活、注册、登录等后链路事件。

具体的常用回调事件请参见附录C。

8.5.2 回调的方式

- a) call_back 动态地址回调：回调参数中包含 call_back 回调地址参数，广告服务器可用此参数将数据回调地址动态传输过来；
- b) 固定地址回调：媒体提供固定的数据接收方地址用于回调。

8.6 广告归因无效流量验证

8.6.1 验证概述

广告归因无效流量验证指在数字广告环境中对广告归因的真实有效性进行的验证。

8.6.2 广告归因无效流量特征

广告归因无效流量特征，按照广告归因流程可分为以下三类：广告数据无效流量特征、归因匹配数据无效流量特征、转化行为数据无效流量特征。

广告数据无效流量特征：

- a) 来自不具备明确真实用户特征的流量；
- b) 基本信息缺失或不一致的流量（基本信息至少应包含事件类型、广告系列 ID、时间戳、IP 地址、请求方式、完整用户代理信息）；
- c) 基于广告活动用户行为出现的明显异常的高速、连续或重复请求、严重超出用户正常合理频次的流量，或缺少有效流量的关键数据信息；
- d) 用户代理信息为空或非浏览器用户代理头及其它形式的未知浏览器带来的流量；
- e) 归因匹配数据无效流量特征：广告数据与转化行为数据基础信息不一致的流量；
- f) 转化行为数据无效流量特征：
 - 基本信息缺失或不一致的流量（基本信息至少应包含事件类型、广告系列ID、时间戳、IP 地址、请求方式、完整用户代理信息）；
 - 基于转化事件用户行为出现的明显异常的高速、连续或重复请求、严重超出用户正常合理频次的流量，或缺少有效流量的关键数据信息。

附 录 A
(规范性)
互联网广告监测代码接口

A.1 参数定义

表 A.1 监测系统需要采集的参数定义

参数	用途描述	格式和示例	是否必填	参数可使用的终端类型	获取方法
OS	用户终端的操作系统类型	0 - Android 1 - iOS 2 - WP 3 - Others 4 - Harmony 5 - aliyunOS	是	移动端、OTT 终端	SDK/API
MAC	OTT 终端的 eth0 接口的 MAC 地址（大写去除冒号分隔符），md5 加密	去除分隔符“:”，（保持大写）取 md5 摘要	否	OTT 终端	SDK/API
MAC1	OTT 终端的 eth0 接口的 MAC 地址（大写且保留冒号分隔符），md5 加密	保留分隔符“:”，（保持大写）取 md5 摘要	否	OTT 终端	SDK/API
MAC2	OTT 终端的有线 MAC 地址	保持大写，去除分隔符“:”，取 md5 摘要	否	OTT 终端	SDK/API
MAC3	OTT 终端的无线 MAC 地址	保持大写，去除分隔符“:”，取 md5 摘要	否	OTT 终端	SDK/API
MAC4	OTT 终端的蓝牙 MAC 地址	保持大写，去除分隔符“:”，取 md5 摘要	否	OTT 终端	SDK/API
IDFA	iOS IDFA 适用于 iOS6 及以上	保留原始值	否	移动端、OTT 终端	SDK/API
IDFA1	iOS IDFA 适用于 iOS6 及以上	保持大写，取 md5 摘要	否	移动端、OTT 终端	SDK/API
CAID	用户终端的 CAID	版本号以及具体的 CAID 值以 json 格式传输，应包括当前最新版本号和上一版本号的 CAID 值。示例： [{ "caid": "bed47550547dc8d51c98b668eb690140", "version": "20220501" }, { "caid": "cb187c190ba19b7863c803cb27ab2523", "version": "20210501" }] 传输前进行	否	移动端、OTT 终端	SDK/API

		url_encode			
CAID_MD5	用户终端的 CAID, 适用于 iOS 系统	CAID 原值保持小写取 md5 摘要后, 版本号以及具体的 CAID 摘要值以 json 格式传输, 应包括当前最新版本号和上一版本号的 CAID 值。示例: [{ "caid_md5": "27dc3f5a7c02e8cba6e699c3ee07b295", "version": "20220501" }, { "caid_md5": "34ae823c759e5c0480867247c77462bb", "version": "20210501" }] 传输前进行 url_encode	否	移动端、OTT 终端	SDK/API
DUID	Windows Phone 用户终端的 DUID, md5 加密	取 md5 摘要	否	移动端	SDK/API
OAID	用户终端的 OAID, 适用于 Android 系统	保留原始值	否	移动端、OTT 终端	SDK/API
OAID1	用户终端的 OAID, 适用于 Android 系统	OAID 原值取 md5 摘要	否	移动端、OTT 终端	SDK/API
IP	媒体投放系统获取的用户终端的公网 IP 地址, 用于比对智能路由 IP 差异	IPv4 或 IPv6	是	桌面端、移动端、OTT 终端	服务端通过 IP 协议获取/API
UA	数据上报用户终端设备的 User Agent	字符串, 需 URLEncode, 如 Mozilla%2F5.0(Linux%3BAndroid4.0.4%3BG T-I9220%20Build%2FIMM76D)	否	桌面端、移动端、OTT 终端	请求头
TS	客户端触发监测的时间, 用于计算离线监测时间	UTC 时间戳, 自 1970 年起的毫秒数	是	桌面端、移动端、OTT 终端	SDK/API
EVNT	用于区分监测的事件, 如: 播放开始或者播放完成	英文数字下划线, 如 "Start"	否	桌面端、移动端、OTT 终端	输入
MUDS	用于媒体自定义信息, 如 IES-ID 或投放订单 ID	字符串, 需 URLEncode	否	桌面端、移动端、OTT 终端	输入
MUID	媒体分配的浏览者 Cookie ID 或 用户 ID	字符串, 需 URLEncode	否	桌面端、移动端、OTT 终端	输入

OSVS	用户终端的操作系统版本	字符串，需 URLEncode	否	桌面端、移动端、OTT 终端	SDK
TERM	用户终端的机型	字符串，需 URLEncode	否	移动端、OTT 终端	SDK
WIFI	客户端触发监测时是否使用 wifi	0=2/3G mode 1=wifi mode	否	移动端、OTT 终端	SDK
SCWH	用户终端的屏幕分辨率	宽 x 高，用字母 x 分割	否	移动端、OTT 终端	SDK
ADWH	素材实际播放时的尺寸（考虑素材的缩放）	宽 x 高，用字母 x 分割	否	移动端、OTT 终端	SDK
AKEY	媒体 APP Key	字符串，需 URLEncode	是	移动端、OTT 终端	SDK
ANAME	媒体 APP Name	字符串，需 URLEncode	否	移动端、OTT 终端	SDK/API
SDKVS	SDK 版本	字符串，需 URLEncode	是	移动端、OTT 终端	SDK
SIGN	签名串	字符串，需 URLEncode	否	移动端、OTT 终端	SDK
ImpressionType	在曝光监测中，标志是否满足广告开始渲染（BtR）的要求	0=不满足 1=满足	否	桌面端、移动端、OTT 终端	SDK
ImpressionID	每次曝光时生成的唯一 ID，用以关联用户在同一次会话中的曝光、可见/不可见曝光、点击事件	字符串，需 URLEncode	是	移动端、OTT 终端	SDK
isRoot	标志设备是否 ROOT/越狱	0-否， 1-是， 2-未知	否	移动端	SDK
isSimulator	标志设备是否是模拟器	0-否， 1-是， 2-未知	否	移动端	SDK
isHook	设备是否被 hook，	0-否， 1-是， 2-未知	否	移动端	SDK
isADB	是否处于，仅用于 Android 设备	0-否， 1-是， 2-未知	否	移动端	SDK

下表A. 2中是可见曝光相关参数，在这个表中，“是否必填”是针对进行可见性测量的前提而言的；对于未进行可见性测量的情况下，不受到下表约束。可见曝光参数可应用于桌面端、移动端、OTT终端。

表 A. 2 可见性验证需要采集的参数定义

参数	用途描述	格式和示例	是否必填	获取方法
AdviewabilityResult	标识广告的可见性	0 - 可见监测中发出的普通曝光 1-可见曝光 4-不可见曝光 2-监测中出现不可测量报告	是	SDK
AdviewabilityRecord	可见监测的时间片数据是否上报，在监测代码中预先配置本参数的值为 1，SDK 将会把时间片数据（AdviewabilityEvents）上报	仅能等于 1	否	预先配置
AdviewabilityEvents	可见性监测中采集的时间片信息	以 json 数组的方式将时间片信息拼接起来，并做 URLEncode 如：%5b%7b1%3a15619562768	否	SDK

		26%2c2%3a1080x715%2c3%3a0x1313%2c4%3a1%2c5%3a1%2c6%3a0%2c7%3a1080x715%2c8%3a1%7d%2c+%7b1%3a1561956277535%2c2%3a1080x715%2c3%3a0x-265%2c4%3a1%2c5%3a1%2c6%3a0.68%2c7%3a1080x230%2c8%3a1%7d		
AdviewabilityConfigArea	表示可见曝光面积阈值。如果在监测代码中预先配置，也可以用于指导 SDK 以相应的可见面积阈值进行可见性测量	一般取值 50，表示以 50%作为可见面积阈值	是	预先配置或 SDK
AdviewabilityConfigThreshold	表示可见曝光时长阈值。如果在监测代码中预先配置，也可以用于指导 SDK 以相应的可见时长阈值进行可见性测量	一般取值 1 或 2，表示以 1s 或 2s 作为 Display 广告和 Video 广告的可见时长阈值	是	预先配置或 SDK
AdviewabilityVideoDuration	视频广告素材的总播放时长	整型，例如：15，表示视频广告总时长是 15 秒	否	预先配置
AdviewabilityVideoProgress	标识视频广告播放的进度	共 4 种取值：25、50、75、100，分别表示视频播放进度达到了 25%、50%、75%、100%	否	SDK
AdviewabilityVideoProgressPoint	要监测的进度点。在监测代码上预先配置，用于指导 SDK 进行特定进度点的监测	取值为 4 个标识位，分别表示 25%、50%、75%、100%的进度是否上报 例如取值 0101，表示对 50%和 100%的播放进度进行上报	否	预先配置
AdviewabilityVideoPlayType	视频广告素材是否自动播放	0-未知， 1-自动播放， 2-手动播放	否	SDK
AdviewabilityStrongInteract	强用户交互标识位，仅出现在可见曝光上报中	取值为 1，表示这是通过广告点击行为判断出来的可见曝光，而非面积及时长阈值	否	SDK

注1：监测平台对于参数的命名不强制和上述定义完全一致，但是含义及用途必须完全符合上述定义。

注2：统一动态参数的宏定义格式为参数名全大写，前后加双下划线“__”。表中参数统一后的部分宏定义如下：
__OS__、__MAC__、__MAC1__、__MAC2__、__MAC3__、__MAC4__、__IDFA__、__IDFA1__、__DUID__、__OAID__、
__OAID1__、__CAID__、__CAID_MD5__、__IP__、__UA__、__TS__。

注3：注3：非必选的媒体输入参数，输入空值表示该值缺省。

注4：注4：对同一设备的参数采集频率，应采取最小频次、不能多次持续采集的原则。

注5：注5：SDK获取的可禁用的参数，可以通过修改配置文件实现禁用。

附录 B (规范性) SDK 监测与验证

B.1 设计目的、适用范围与局限

本附录列出的技术方案适用于移动客户端广告监测，方案定义了一种通用可配置的、供移动APP与广告监测平台完成数据通信的SDK（下文中统称为“广告监测及验证SDK”）。本方案不适用于其它媒体形式或其他监测方式。

广告监测及验证SDK，通过结构化的灵活配置项，兼顾APP媒体和移动APP广告平台在接入多家监测平台、版本更新铺量等现实情况，有效的控制APP程序包的文件尺寸、避免监测接入带来的版本升级困扰。

B.2 SDK 工作环境和关联系统模块描述

B.2.1 媒体广告投放系统

即媒体部署的用于广告管理、决策和投放的服务器，应存储有以下三种文档和信息：

- 监测参数配置文档，XML 格式文档，用于定义各监测平台的参数配置规则，内容包括：
 - 已接入的监测平台及其参数配置；
 - 可监测的事件。
- 广告素材，用于投放的广告主的创意，如 GIF、视频前贴片等文件；
- 监测代码，由监测平台提供，一般包括曝光监测和点击监测两段 HTTP URL。

B.2.2 媒体APP

除了正常的APP内容和场景外，还包含以下模块：

- 广告监测及验证 SDK，封装有各种监测参数的获取方法；封装有解析监测参数 XML 配置文档的方法；定义了通用的监测提交的方法；
- SDK 中包含不开源的签名加密包，按监测或验证公司需要对监测 URL 进行签名，提供反作弊功能，签名包中不含有任何网络操作，只对监测 URL 签名；
- 投放管理(模块)，媒体 APP 内用于呈现广告素材的模块，并在特定事件或交互时触发 SDK 内相应的监测提交方法。

媒体APP运行被用户运行时，会加载并初始化SDK。

B.2.3 监测和验证系统

监测平台部署的服务器，用于记录数据并向广告主提供统计报告。

B.3 数据通信流程

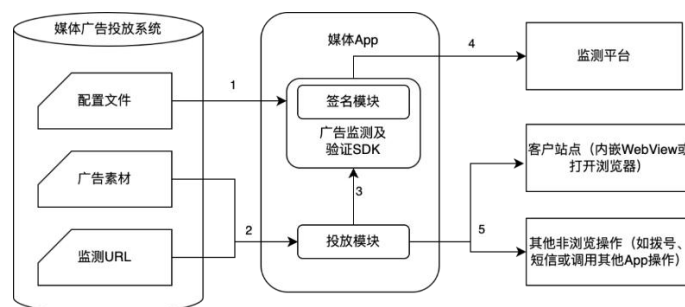


图 B.1 广告监测及验证 SDK 架构设计

- 1) SDK 远程加载存放于媒体广告投放系统的监测参数 XML 配置文档，并解析保存相应配置规则；

- 2) 媒体 APP 内的投放管理模块从投放系统加载广告素材及其监测代码;
- 3) 媒体 APP 内的投放管理模块调用广告监测及验证 SDK 的“提交监测”方法,并传递监测代码,如有需要还可以传递特定的监测事件、媒体自定义信息(如投放订单 ID,投放系统获取的用户 IP、媒体自定义的用户 ID);
- 4) 广告监测及验证 SDK,根据投放管理模块传递的参数,按照监测参数配置文档,在提供的监测代码后拼接 SDK 获取的参数,向监测平台服务器提交监测请求;
广告监测及验证 SDK 中的签名模块可以对监测代码进行签名校验。广告监测及验证 SDK 生成签名校验串并拼接在监测代码后,发送到监测平台,监测平台在服务器端反解签名串进行校验,避免发送数据被篡改;
- 5) 媒体 APP 内的投放管理模块响应用户的交互操作,内嵌浏览器组件或打开浏览器跳转到广告主站点或执行拨号、短信、打开其他 APP 等操作。用户的跳转或交互操作将与其监测提交异步执行;
- 6) 如果用户处于断网状态,广告监测及验证 SDK 将暂时无法提交的监测请求存放到待发送队列。广告监测及验证 SDK 会定时检查用户网络连接情况,在重新联网时,将一并发送存储于待发送队列的监测请求。

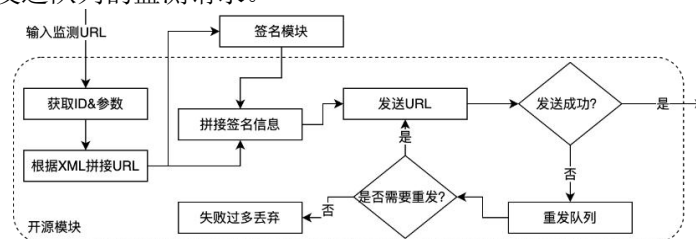


图 B.2 监测或验证请求的签名、发送和错误重发

B.4 广告监测及验证 SDK 配置文件

B.4.1 配置文件更新频率

SDK 优先使用本地的配置文件,同时会定期下载远程的配置文件覆盖本地的配置,并支持 WIFI 环境和 3/4G 网络环境下不同的更新策略。

B.5 广告监测及验证 SDK 初始化与安全校验

B.5.1 初始化配置更新策略

具体要求如下:

- a) 更新时段: SDK 初始化阶段;
- b) 检测当前用户使用网络方式如果是 wifi 网络,检测当前系统时间与上次更新时间间隔超过 1 天,则更新配置文件;
- c) 检测当前用户使用网络方式如果是 3G/4G 网络,检测当前系统时间与上次更新时间超过 3 天,则更新配置文件;
- d) 更新后的配置文件存储到本地缓存中。

B.5.2 广告监测及验证 SDK 安全校验相关

具体要求如下:

- a) iOS 编译、解包、校验:
 - 1) 签名模块编译为静态连接库.a 文件;
 - 2) 该链接库和开源部分的代码一起再次由各家独立编译为 ipa,嵌入 APP 中(经过静态链接库的整合后,发布为 ipa 文件时,SDK 开源部分和签名模块.a 库,会产生特征性的二进制代码段);
 - 3) 校验方法:解压 APP 发行包后,抽检 SDK、签名模块 .a 资源文件对应的的二进制代码段。
- b) 安卓编译、解包、校验:
 - 1) 签名模块采用 C 语言 NDK 方式独立编码为 .so 资源文件;

- 2) 编译方法：开源代码部分各媒体单独编译，并嵌入签名模块 .so 资源文件后，发布 APP；
- 3) 校验方法：解压 APP 的发行包 apk 文件，检查签名模块 .so 资源文件的 MD5 校验串。

附录 C

(规范性)

回调事件

C.1 回调事件规范化的必要性

在数据回传中，由于不同类型应用有着不同的事件类型，同时也为了渠道对接的规范化，在这里举出八类回调事件模板。

C.2 回调事件模板

C.2.1 通用事件

- a) 注册：注册成功；
- b) 受邀注册：受邀注册成功的事件；
- c) 登录：登录成功；
- d) 唤醒：利用 Deeplink 成功调起/唤醒应用；
- e) 收藏：收藏成功，例如：收藏书单、收藏商品、收藏攻略等；
- f) 分享：分享成功，例如：分享行程、分享商品、分享应用；
- g) 添加支付信息：添加支付信息成功，例如：完成绑定微信支付、成功添加银行卡等；
- h) 签到打卡：签到打卡成功，例如：学习签到、景点打卡等；
- i) 搜索：搜索的事件，例如：搜索航班、搜索书单、搜索商品等。

C.2.2 电商零售专属事件

- a) 预订：预订成功的事件，例如：预订商品；
- b) 联系：联系的事件，例如：联系店家、联系客服；
- c) 查看商品：查阅商品详情的行为事件；
- d) 查看购物车：查看购物车的行为事件；
- e) 添加购物车：添加商品到购物车的行为事件；
- f) 订单：下订单的事件；
- g) 支付订单：订单中支付成功的订单事件；
- h) 退单：退单成功事件，例如订单退货、退款、退订等；
- i) 完成试用体验：完成试用体验的事件。

C.2.3 游戏娱乐专属事件

- a) 付费：付费成功事件，例如：游戏充值；
- b) 创建角色：创建角色成功的事件；
- c) 完成新手教程：完成新手教程的事件；
- d) 通过关卡：通过关卡的事件；
- e) 解锁成就：解锁成就的事件。

C.2.4 金融借贷专属事件

- a) 预约：预约成功的事件数，例如：预约理财、预约定期等；
- b) 联系：联系的事件数，例如：联系平台、联系资方等；
- c) 浏览详情：浏览详情的行为事件，例如：浏览借贷详情页等；
- d) 授信：授信成功的事件；
- e) 交易：交易成功的事件，例如：定期、借贷、理财等；
- f) 退单：退单成功事件；
- g) 完成试用体验：完成试用体验的事件，例如：完成理财体验金等。

C.2.5 旅游出行专属事件

- a) 预订：预订成功的事件，例如：预订酒店、预订航班等；
- b) 联系：联系的事件，例如：联系领队、联系导游等；
- c) 浏览详情：浏览详情的行为事件；
- d) 付费：付费成功事件；
- e) 退单：退单成功事件；
- f) 完成试用体验：完成试用体验的事件。

C.2.6 在线教育专属事件

- a) 预约：预约成功的事件，例如：预约课程、预约教师等；
- b) 联系：联系的事件，例如：联系助教、联系班主任等；
- c) 课程学习：课程学习的行为事件；
- d) 付费：付费成功事件，例如：充值学习点券；
- e) 退单：订单退货/退款/退订成功的事件；
- f) 完成课程试听：完成课程试听的事件；
- g) 解锁成就：解锁成就的事件。

C.2.7 小说阅读专属事件

- a) 文章阅读：文章阅读的行为事件；
- b) 付费：付费成功事件，例如：购买电子书、充值阅读点券等；
- c) 完成免费阅读：完成免费阅读的事件。

C.2.8 其他行业专属事件

- a) 浏览详情：浏览详情的行为事件；
- b) 付费：付费成功事件；
- c) 完成试用体验：完成试用体验的事件。

参 考 文 献

[1] IAB, MMA, MRC Mobile Application Advertising Measurement Guidelines, Version 3.0, MMTF Final Version 1.1 - October 2017: begin to render, Enhancing Mobile Application Impression Tracking Accuracy

[2] IAB Anti-Fraud Principles and Proposed Taxonomy - September 2014: Anti-Fraud Principles

[3] MRC MRC Mobile Viewable Ad Impression Measurement Guidelines, Final Version - June 28, 2016: Requirements for Mobile Viewable Display Advertising Impressions, Requirements for Mobile Viewable Video Advertising Impressions

[4] MRC Invalid Traffic Detection and Filtration Standards Addendum - June 2020 - Update (Final): Categories of IVT and Associated General Requirements
