

团体标准

T/CAAAD 00X—2020

互联网广告投放监测及验证要求

(征求意见稿)

XXXX - XX - XX 发布

XXXX - XX - XX 实施

中国广告协会 发布

目 次

| | |
|-------------------------------------|----|
| 前言 | IV |
| 引言 | V |
| 1 范围 | 1 |
| 2 规范性引用文件 | 1 |
| 3 缩略语（术语和定义） | 1 |
| 4 广告监测 | 3 |
| 4.1 概述 | 3 |
| 4.2 桌面端广告监测 | 3 |
| 4.3 移动端广告监测 | 6 |
| 4.4 OTT 广告监测 | 8 |
| 4.5 广告监测系统性能要求 | 10 |
| 4.6 广告信息保存要求 | 10 |
| 4.7 数据安全与个人信息保护 | 10 |
| 4.8 用户地理位置监测要求 | 10 |
| 4.9 监测质量指标 | 10 |
| 5 广告监测指标项及其计算要求 | 10 |
| 5.1 广告曝光数 | 11 |
| 5.2 广告独立访问者数量 | 11 |
| 5.3 广告点击数 | 11 |
| 5.4 广告独立点击者数量 | 11 |
| 6 广告验证 | 11 |
| 6.1 广告验证概述 | 11 |
| 6.2 广告验证技术规范 | 12 |
| 6.3 广告无效流量验证 | 12 |
| 6.4 广告可见性验证 | 14 |
| 6.5 广告品牌安全验证 | 18 |
| 附 录 A（规范性附录） 互联网广告监测代码接口 | 20 |
| A.1 参数定义 | 20 |
| 附 录 B（规范性附录） SDK 监测与验证 | 26 |
| B.1 设计目的、适用范围与局限 | 26 |
| B.2 SDK 工作环境和关联系统模块描述 | 26 |
| B.3 数据通信流程 | 27 |
| B.4 广告监测及验证统一 SDK (UM SDK) 配置文件 | 28 |
| B.5 广告监测及验证统一 SDK (UM SDK) 初始化与安全校验 | 28 |
| 附 录 C（规范性附录） 无效流量监测字段 | 30 |

C.1 无效流量监测字段..... 30

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。

本标准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和验证的统一性。

互联网广告投放监测及验证要求

1 范围

GB/T XXXXX 的本部分规定了广告监测、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。

本部分适用于各类桌面端、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/TXXXXX.1—XXXX 互动广告 第1部分:术语概述。

3 缩略语（术语和定义）

下列缩略语适用于本文件。

- API: Application Programming Interface, 在数据合规的前提下, 通过技术对接数据提供方和接收方, 自动传输数据。
- APP: Application, 在本标准中特指移动设备里可独立运行的应用。
- DUID: Device Unique Identifier, Windows Phone 操作系统唯一设备身份识别码。
- GIVT: General Invalid Traffic, 一种无效流量的甄别标准, 行业通用的利用技术和数据手段, 对无效流量进行甄别的解决方案。
- HTML: Hypertext Markup Language, 一种用于创建网页的标准标记语言。
- HTTP: Hyper Text Transfer Protocol, 超文本传输协议, 互联网常用的数据传输协议。
- IAB: Interactive Advertising Bureau。
- OAID: Open Anonymous ID, 开放匿名广告标识符, 一种非永久性设备标识符, 使用 OAID 可在保护用户个人数据隐私安全的前提下, 向用户提供个性化广告。
- IDFA: Identifier For Advertising, 苹果广告标识码, Apple 公司为 IOS 移动设备提供的用户追踪用户的广告标识码。
- IFrame: iFrame 标签, 是浏览器上一种包含其他内容的框架, iFrame 元素会创建包含另外一个文档的内联框架（即行内框架）。
- IMEI: International Mobile Equipment Identity, 用于识别每一部独立的移动通信设备。
- JavaScript: 一种编程语言, 通过埋设在用户交互页面, 来触发和收集用户的使用行为数据。
- Cookie ID: 基于网页浏览器的受众识别码。

- MAC: 基于网卡的唯一码, 通过线下的智能探针和进行 APP SDK 监测的时候都可以获取。但 Apple 设备在 iOS 7 版本之后, 安卓在 2019 年 4 月公布 10.0 版本之后, 屏蔽了所有通过数字技术获取 Mac 的方法。
- MRAID: Mobile Rich Media Ad Interface Definitions, 移动富媒体广告接口定义。MRAID 通用接口协议使广告与移动应用之间产生了通讯的能力, 以执行如获取地理位置, 改变广告创意大小, 调用重力感应等交互功能。
- MRC: Media Rating Council, 媒体评级委员会。
- OS: Operating System, 操作系统。
- SDK: Software Development Kit, 软件开发工具包, 在 APP 开发时候的标准的模块化软件开发工具包, 在开发 APP 时只需植入标准 SDK 就能实现部分功能, 而不需要从零开始写源代码。
- SIVT: Sophisticated Invalid Traffic, 一种无效流量甄别标准, 针对通用的 GIVT 标准无法识别的高阶异常流量, 通过更实时, 更高阶的算法分析进行识别, 但需要产生客户的成本。
- TS: Timestamp, 时间戳。
- UA: User Agent, 用户代理, 一个特殊字符串头, 使得服务器能够识别客户使用的操作系统及版本、CPU 类型、浏览器及版本、浏览器渲染引擎、浏览器语言、浏览器插件等。
- VPAID: Video Player Ad Interface Definition, 视频播放器广告接口定义。VPAID 通用接口协议使广告与视频播放器之间产生了通讯的能力, 以执行如播放、回放、跳过等交互功能。
- XML: 可扩展标记语言, 用于标记电子文件使其具有结构性的标记语言, 可以用来标记数据、定义数据类型, 是一种允许用户对自己的标记语言进行定义的源语言。
- 广告点击: Advertisement 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。
- 广告投放: Ad Serving, 是一种利用广告代码将广告投放到网站上的技术或服务。
- 广告曝光: Advertisement Impression, 根据用户的请求, 广告平台向用户移动终端发送广告素材, 并在用户的移动终端上进行一定时间的展示。
- 异步上传: 本标准中特指点击行为数据上传方式, 即不通过第三方监测服务器跳转, 而直接将点击行为数据上报至监测平台。
- 监测数据: 上报至第三方监测公司后, 在第三方监测公司服务器生成的记录, 以及用于统计、分析所加工后的各项数据。
- 广告网络/广告联盟: Ad Network, 长尾流量的资源整合者, 当中小媒介无法直接和大型广告主对接, 或者大型媒体有尚未销售的广告流量时, 广告联盟作为中间商对这些流量进行收集后统一销售。
- 广告交易平台: Ad Exchange, 广告的竞价平台, 当消费者出现在某个媒体的时候, 多个广告主为在这个消费者页面展示广告进行竞价的地方, 对接买方的 DSP、TD, 对接卖方的 SSP 和 Ad Network。
- 需求方平台: DSP, 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。
- 供应方平台: SSP, Supply Side Platform, 媒体把广告资源进行销售的系统, 记录了媒体销售的广告位, 物料尺寸, 售卖金额, 库存等信息。

4 广告监测

4.1 概述

互联网广告监测主要集中在三种技术环境下——桌面端、移动端和OTT终端上。在不同的终端下，由于广告运行环境及技术机制的不同，广告监测机制存在差异。对于互联网广告，无论采用何种监测机制，都必须符合客户端到服务器(client to server)的大原则。

4.2 桌面端广告监测

4.2.1 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第三方监测平台，监测平台负责对采集到的数据进行清洗、分析、挖掘处理，生成测量结果，并将结果展示给广告监测平台的运营人员。

4.2.2 监测机制

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。

监测机制如图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。
- 第三方监测平台：接收各个渠道的广告监测代码接口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。

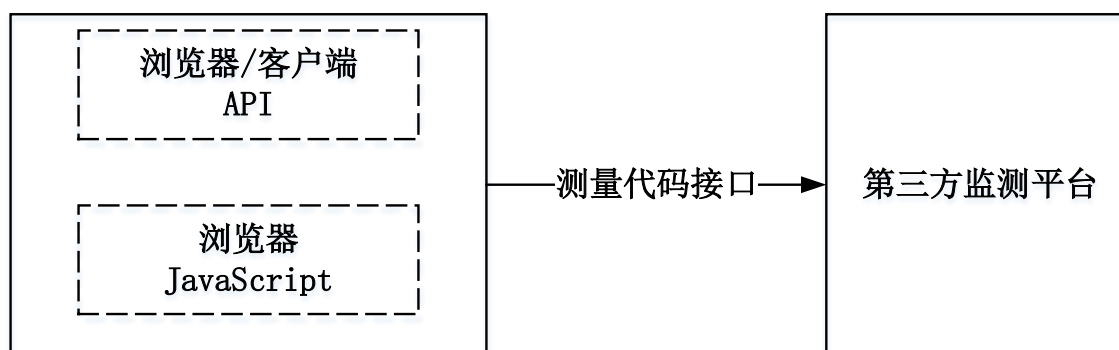


图1 桌面端广告监测机制

4.2.3 监测流程

4.2.3.1 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。

4.2.3.2 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：

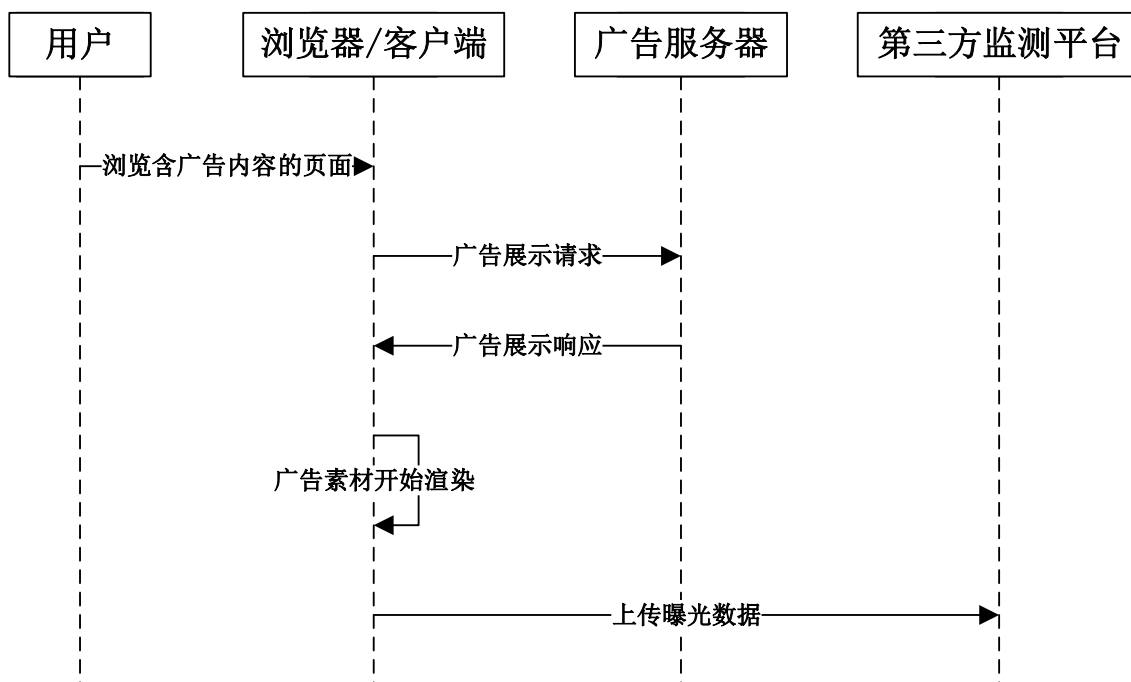


图2 桌面端广告曝光监测流程

流程说明：

- 用户通过浏览器或客户端浏览广告；
- 浏览器或客户端实时向广告服务器请求广告创意；
- 广告服务器响应并返回广告创意及第三方监测平台提供的监测代码；
- 广告创意开始渲染时，浏览器或客户端通过监测代码接口，将曝光数据提交到第三方监测平台，数据格式参考附录A。加载监测代码不应对Web页面、广告的进行及排版造成可见的影响。

对于广告网络中以应用程序接口方式接入的库存的广告曝光监测，一般需要媒体与广告网络间的广告投放程序接口支持该监测机制。即广告网络在通过程序接口返回广告给媒体时，将监测平台的曝光监测代码一并返回，随后媒体依上述流程说明完成广告展示及监测流程。广告网络的展示计费，亦应使用同样方式，多个曝光监测请求应同时并行发送。

4.2.3.3 广告点击行为监测

4.2.3.3.1 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第三方监测平台，监测平台计数完成后进行302重定向到目标站点。监测流程图3所示：

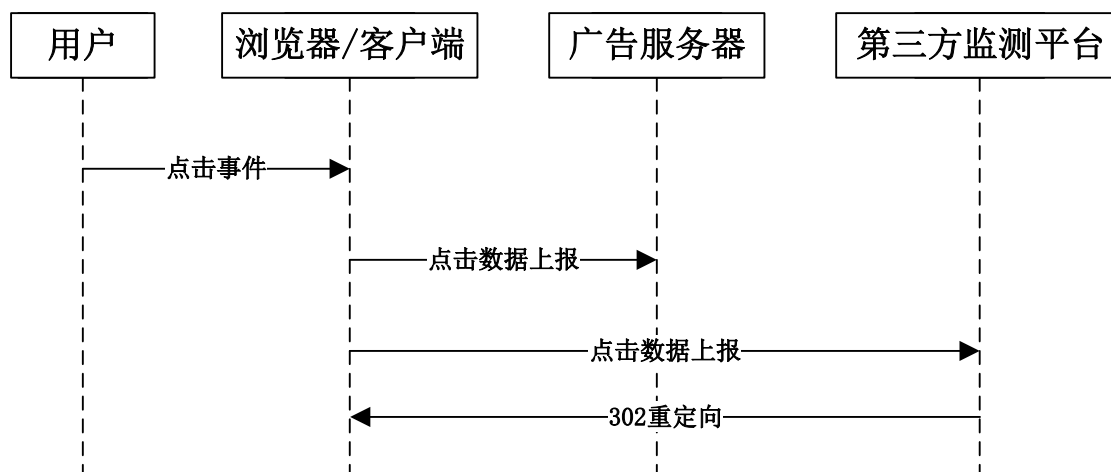


图3 桌面端广告同步模式的点击行为监测流程

流程说明：

- a) 用户点击广告；
- b) 浏览器或客户端处理点击事件；
- c) 浏览器或客户端将广告点击行为数据上报给第三方监测平台；
- d) 监测平台收集和处理好上报的数据，详见附录A；
- e) 监测平台计数完成后进行302重定向到目标站点。

上述方式同样适用于广告网络的广告点击监测。即广告网络将监测平台的广告点击监测代码作为点击链接返回，用户点击后先上报第三方监测平台计数，然后由监测平台将浏览器或客户端重定向到目标站点。广告网络的广告点击计费，亦应使用同样方式，多个点击监测串行执行，建议重定向的顺序从前到后依次为广告网络、监测平台、目标站点。

4.2.3.3.2 异步模式

广告点击行为监测也可采用异步模式。即用户点击广告，浏览器或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第三方监测平台。监测流程如图所示：

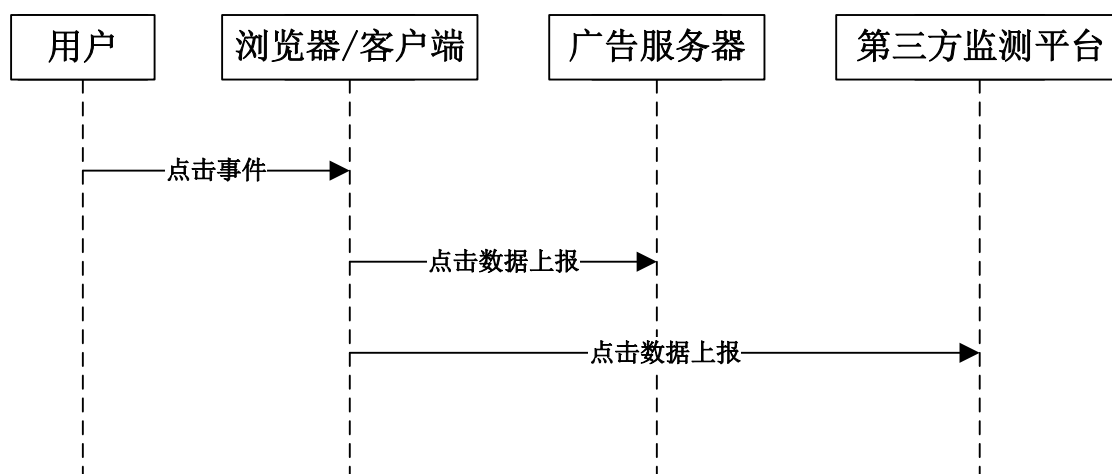


图4 桌面端广告异步模式的点击行为监测流程

流程说明：

- a) 用户点击广告。
- b) 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。
- c) 浏览器或客户端通过异步方式将点击数据上报到第三方监测平台，数据格式详见附录A。若点击动作会导致用户离开或关闭当前页面窗口，应采用延时、新窗口等方法确保浏览器有足够时间完成异步上报。

上述方式可同样适用于广告网络的广告点击监测，一般需要媒体与广告网络间的投放应用程序接口单独支持。广告网络的点击计费，亦可使用同样方式，多个点击监测并行上报。

4.3 移动端广告监测

4.3.1 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及移动客户端广告监测。其中移动网站广告监测机制和桌面端网站广告的监测机制基本一致，不再展开描述；下文将介绍移动客户端广告监测的机制及流程。

4.3.2 机制描述

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第三方监测平台，第三方监测平台负责对采集到的数据进行清洗、分析、挖掘处理，生成测量结果。

机制如图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，对于监测SDK一般推荐使用由中国广告协会（CAA）和中国无线营销联盟（MMA中国）共同发布的数字广告监测及验证统一SDK（即UM SDK）以保证一致性、透明性以及公平性。在附录B中对其功能和实现进行了描述。
- 第三方监测平台：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。

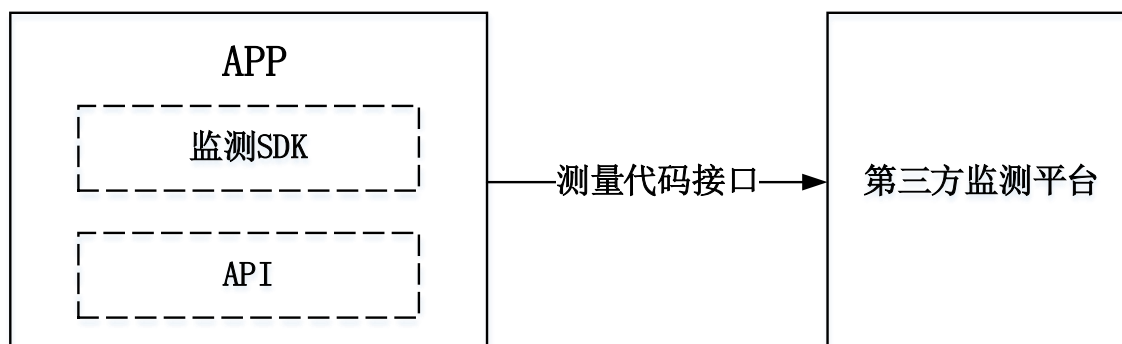


图5 移动客户端广告监测机制描述

4.3.3 监测流程

4.3.3.1 概述

第三方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广告监测平台，第三方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。

4.3.3.2 广告曝光监测

APP在需要展示广告时，从广告服务器(Ad Server)来加载广告，广告素材开始渲染时，APP将曝光数据上传给第三方监测平台。

监测流程如图6所示：

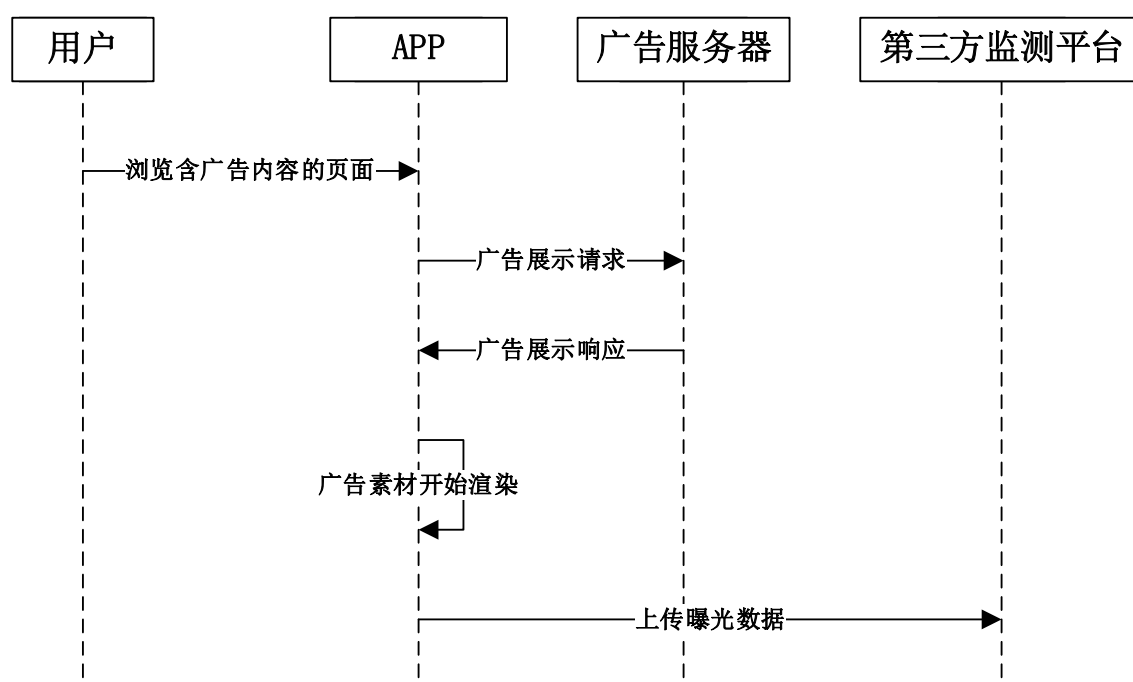


图6 移动客户端广告曝光监测流程

流程说明：

- 用户浏览APP中包含广告内容的页面。
- APP 向广告服务器请求广告。
- 广告服务器给 APP 返回广告创意及第三方监测平台提供的监测代码。
- 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。数据格式详见附件 A。

广告服务器，可以是媒体自己的Ad Server，也可以是第三方的Ad Server，如广告网络(Ad Network)、广告交易平台(Ad Exchange)、需求方平台(DSP)、供给方平台(SSP)。

4.3.3.3 广告点击行为监测

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7所示：

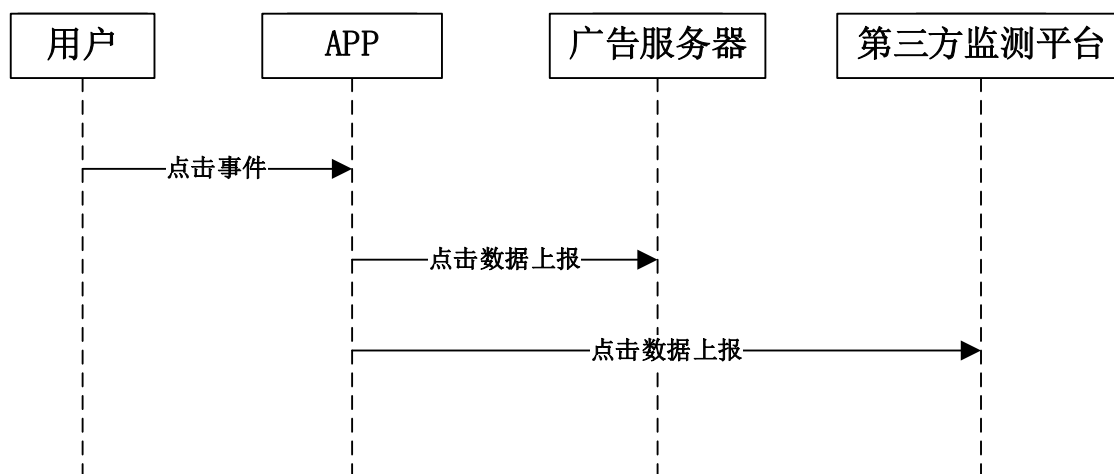


图7 移动客户端广告点击监测流程

流程说明：

- a) 用户点击广告。
- b) APP 处理点击事件，并将点击数据上报给广告服务器。
- c) APP 通过异步方式将点击数据上报到第三方监测平台，数据格式详见附录 A。

4.4 OTT 广告监测

4.4.1 概述

OTT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，再将数据发送到第三方监测平台，第三方监测平台对数据进行分析 and 处理，生成数据报告，下面更具体的说明OTT广告监测机制及流程。

4.4.2 机制描述

与移动客户端的广告监测类似，由监测SDK实时获取的广告行为数据，通过监测代码接口上报到第三方监测平台，第三方监测平台负责对收集汇总的数据进行清洗、分析、挖掘处理，生成监测结果。

监测机制如下图，其中各模块及功能包括：

- 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。
- 第三方监测平台：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。



图8 OTT 广告监测机制

4.4.3 监测流程

第三方监测平台主要进行广告监测，通过监测SDK将采集到的OTT广告行为数据通过监测代码接口上报到广告监测平台，第三方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。

广告行为一般有三个阶段：曝光，交互，跳转响应。广告监测主要针对广告曝光和交互行为进行监测。如下图，详细细节见附录B，过程主要包括：

- 1) OTT操作系统及应用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，一般包含曝光监测代码、点击监测代码。
- 2) OTT操作系统及应用内的投放管理模块调用监测SDK的“提交监测”方法（包括提交曝光监测、提交点击监测、提交事件或交互监测等），并传递监测代码，如有需要还可传递特定的监测事件、媒体自定义信息。
- 3) 监测SDK根据投放管理模块传递的参数，在提供的监测代码后拼接SDK额外获取的参数，向第三方监测系统提交监测请求。
- 4) OTT操作系统及应用内的投放管理模块响应用户的交互操作，跳转到广告落地界面，用户的跳转或交互操作与监测提交异步执行。

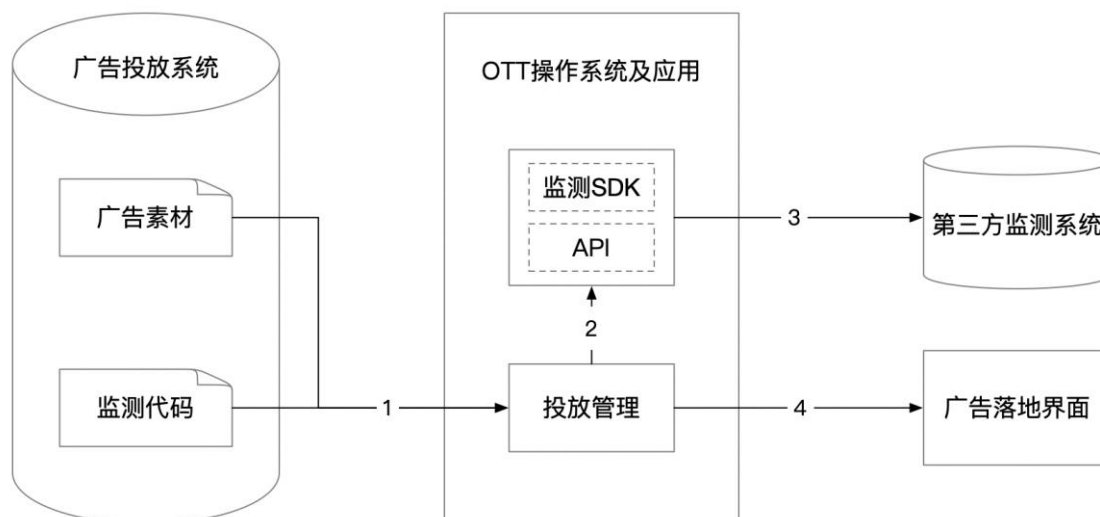


图9 OTT 广告监测流程

4.5 广告监测系统性能要求

广告监测系统性能要求见表1。

表1 监测系统的性能要求

| 项目 | 要求 |
|-----|---|
| 可用性 | 保障线上 99.99%的可用性 |
| | 对数据有灾备和恢复方案，避免数据丢失 |
| 扩展性 | 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 |
| | 弹性带宽配置方案，确保不发生网络堵塞 |
| 安全性 | 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 |
| | 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 |
| | 对服务器具有 100%的控制权 |
| | 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 h 响应服务器发生的硬件或网络故障 |
| | 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 |

4.6 广告信息保存要求

广告监测过程中采集的数据应以数据采集原始格式在媒体平台至少保存 2 年。向监测公司传输的数据应以数据传输原始格式在监测公司平台至少保存 2 年。

4.7 数据安全与个人信息保护

若媒体方提供的数据中包含个人信息，广告监测平台须按照国家法律、行政法规和国家标准的要求收集、使用、提供和保存个人信息。

4.8 用户地理位置监测要求

若广告营销活动有使用 IP 地址精准定向技术的要求，媒体方和广告监测平台须使用行业统一的 IP 地址信息库进行用户定向和验证。对于 IP 地址信息库一般推荐使用由中国广告协会（CAA）发布并定期更新的统一 IP 地址库，以保证一致性、透明性以及公平性。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、广告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。

4.9 监测质量指标

允许正常误差 5%，行业一般定义 5% 为显著性检验的水平，如果超出此范围需基于实证研究进行说明和行业确认：

- 曝光数
- 点击数
- 独立访问人数

5 广告监测指标项及其计算要求

5.1 广告曝光数

每次广告曝光，当广告创意开始渲染时（begin-to-render），由访问者端向监测服务器发起 1 次 HTTP 请求，并携带广告活动、广告位、用户唯一标识等信息。监测服务器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, 监测服务器可返回(但不限于) 1x1图片、HTML、JavaScript、302跳转等。监测服务器应通过设置HTTP头等技术方式最大程度减少缓存对曝光数监测的影响。

5.2 广告独立访问者数量

每个访问者应具有唯一标识; 统计访问者产生的曝光日志中, 用户唯一标识去重后的数量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PC网站和移动网站(移动网站说明可参考4.3), 为每个新访问者分配一个用户唯一标识, 并使用第三方Cookie存储此标识; 基于PC客户端或移动客户端环境的广告监测,

使用设备ID(ANDROID系统使用IMEI; IOS系统使用IDFA; 其他系统使用MAC)作为用户唯一标识, 若前述设备ID无法正常获取, 依据如下顺序优先级来确定用户唯一标识的最终识别方案:

ANDROID系统

- OAID
- MAC
- AAID
- IP+UserAgent: IP地址和用户代理标识的组合

iOS系统

- MAC
- IP+UserAgent: IP地址和用户代理标识的组合

其他操作系统

- IP+UserAgent: IP地址和用户代理标识的组合

5.3 广告点击数

每次广告点击, 由访问者端向监测服务器发起1次HTTP请求, 并携带广告活动、广告位、用户唯一标识等信息。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。

5.4 广告独立点击者数量

统计访问者产生的点击日志中, 通过用户唯一标识进行去重后得到的数量。计算要求需根据4.3中的点击日志进行唯一标识去重得出。用于去重的唯一标识符选择机理同5.2中描述的唯一标识符选择机理相同。

6 广告验证

6.1 广告验证概述

广告验证是一个验证广告营销活动是否按照由广告主或者代理机构签订的条款中的一个或多个条件要求(包括但不限于如无效流量验证、广告可见性验证、品牌安全验证等要求)执行的验证过程。广告验证服务商是完成验证项目的服务提供方。

6.2 广告验证技术规范

数字广告的验证主要集中在两种技术环境下——桌面或移动设备的网页端以及移动应用端(以下简称网页环境和应用APP内环境)。网页环境在桌面以及移动设备上的运行环境类似效果相仿, 且

在 HTML5 的大力推行下技术框架更趋于统一。而应用APP内环境由于移动操作系统的底层差异导致广告运行的技术环境不统一，因此在验证时需要广告供应方尽最大可能提前支持技术框架和协议。例如网页环境，根据广告类型的不同，媒体供应方需提供验证代码的运行环境；类似得，对应用APP内环境，媒体供应方需提供广告验证代码运行环境（如MRAID、广告验证 SDK等）。对于验证SDK一般推荐使用由中国广告协会（CAA）和中国无线营销联盟（MMA中国）共同发布的“数字广告监测及验证统一SDK”（下称UM SDK）以保证一致性、透明性以及公平性。

6.3 广告无效流量验证

6.3.1 无效流量验证的定义

无效流量验证指在数字广告环境中对广告的真实有效性进行的验证，验证技术通常依靠在网页环境中部署的验证代码，以及在应用APP内以及OTT环境内部署验证代码或验证SDK并与验证平台进行数据交互从而实现广告无效流量验证。

6.3.2 无效流量验证的技术机制

无效流量验证是通过验证代码，其形式包括网页验证代码，应用APP内以及OTT环境内的验证代码或UM SDK，与被验证广告创意素材同时投放到广告位后，验证代码从浏览器、应用APP内以及OTT环境内获取各种参数来判断当前广告曝光是否满足无效流量验证标准，最终通过报告展示界面提供广告无效流量统计结果。广告验证技术应用在网页环境、应用APP内和OTT环境内。对于网页环境，媒体方需提供验证代码的运行环境；对于应用APP内和OTT环境内，媒体方需接受验证代码或UM SDK来提供广告验证所需获取的广告状态信息。

6.3.3 无效流量的细分

无效流量划分为“一般无效流量”和“复杂无效流量”两大类。

6.3.3.1 一般无效流量

“一般无效流量”（General Invalid Traffic）以下简称GIVT。即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。GIVT之特点是可通过列表和预设参数特征进行识别。进行GIVT识别分析的参数范围详见附录D。

6.3.3.1.1 一般无效流量特征

- a) 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）。
- b) 来自高危设备或者作弊来源 IP 的流量。
- c) 来自声明的机器人或爬虫的流量。
- 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) 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。
- f) 媒体方发起的对广告主提供的点击链接和着陆页面的定期例行检测流量。
- g) 广告主或其代表与媒体方发起的、通过协商约定以测试为目的之流量。
- h) 预获取或浏览器预览且没有指定触发时间的流量。
- i) 已知的来自高危或者作弊来源 App、网站的流量。
- j) 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)。

6.3.3.1.2 一般无效流量判定数据列表

一般无效流量判定所依据的数据列表，由中国广告协会指导并委托中国无线营销联盟(MMA中国)，联合相关企业进行协作制做“GIVT判定数据列表”(GIVT LIST)，并定期发布更新，供各数字广告行业企业优先遵照使用。

“GIVT判定数据列表”(GIVT LIST)的制作原则应遵循行业共识，数据列表的制作应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-设备 ID)。
- 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6.3.3.1.1一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)。这些已知情况地定义和对应判定数据列表地生产，同样由中国广告协会指导并委托中国无线营销联盟(MMA中国)，联合相关企业进行协作制做的“非透明流量判定数据列表”(媒体方IP列表、设备缺省值等列表)，并定期发布更新，供各数字广告行业企业遵照使用。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)。

广告测量机构不应将用户唯一标识符命中如上“非透明流量判定数据列表”的流量判定为GIVT，而是应酌情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5.2中描述的唯一标识符选择机理相同。

随着数字广告行业技术的演进，这些数据列表的数据范围将随之更新扩充。参与协作制定数据列表的企业有对列表进行完善改进和建议的责任及权利。对于国内一般无效流量的判定，在优先使用由中国广告协会指导并委托中国无线营销联盟(MMA中国)，联合相关企业进行协作制做统一发布的GIVT LIST为判定基础的同时，可使用更多有公信力的等效列表以增强一般无效流量的判定能力。

6.3.3.2 复杂无效流量

“复杂无效流量”(Sophisticated Invalid Traffic)，以下简称为SIVT。包括了需要通过高级分析，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才可能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，需要多维度的高级分析进行识别。分析的范围包含但不限于以下一种或多种特征类型：

- a) 未声明的、高度模拟真人访客的机器人和爬虫流量。
- b) 广告插件、恶意软件产生的流量。
- c) 被劫持的设备以及群控设备产生的流量。
- d) 虚拟化设备中产生的流量。

- e) 被劫持的广告代码产生的流量。
- f) 通过作弊代理服务器产生的流量。
- g) 通过隐藏/堆叠/覆盖或其它方式导致用户无机会看到正常广告内容的流量。
- h) 通过在不同于主要广告域名的网页内蓄意嵌套并恶意制造流量。
- i) 以金钱补偿为动机的操纵测量数据行为。
- j) 伪造的可见性曝光判定属性参数的流量。
- k) 篡改或重复使用窃取获得的 cookie 信息或移动装置标识的流量。
- l) 操纵或伪造用户位置数据以及相关属性的流量。
- m) 无效代理流量（即来自中间代理设备的无效流量，包括通过代理设备操纵流量计数、创建/传输非人类流量或无法通过协议验证的流量）。

6.3.4 无效流量数据报告

- a) 确定为一般无效流量（GIVT）的广告曝光数量应从总投放曝光数中标记并在各主要细分维度予以数量上的排除，并与报告更新周期同步提供数据。
- b) 对于“复杂无效流量”（SIVT）的报告，出于鉴别的复杂性，需要至少在投放项目维度报告整体维度体现数据，适当的数据延迟和判定调整是允许的，但最长滞后延迟不能超过 14 天。测量机构根据收集到的数据，计算输出过滤前的流量总量。
- 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。
- d) 广告测量机构必须应用对“一般无效流量”（GIVT）的检测和过滤。测量机构需要输出一般无效流量过滤之前的流量总量，在后续对流量的统计分析中，一般无效流量应当被过滤。

6.3.5 程序化前置过滤

由于广告验证机构对广告中的无效流量在投放前已有大规模的分析，基于对广告主品牌资产的保护以及事前预防优先的原则，本标准建议广告投放前基于无效流量数据预判数据结果进行做流量筛选，在技术环境许可的投放方式中，例如在程序化广告投放中，基于无效流量预判数据进行做放弃竞价或实时广告阻挡控制，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。

6.3.6 第三方合规审计要求

无效流量验证测量机构应接受第三方审计。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。

6.3.6.1 无效流量验证测量机构申请无效流量认证，需要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。

6.3.6.2 业务合作伙伴检查应该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，需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）。
- f) 对于重要的业务合作伙伴（即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。

注：合作伙伴是指和无效流量验证测量机构有合作关系且在广告行业中充当一定角色的机构。

6.4 广告可见性验证

6.4.1 可见曝光的定义

数字广告在满足以下条件时可被定义为可见曝光：广告创意出现在浏览器的可见窗口页面的活跃标签上，并且满足设定的曝光条件（如像素露出面积的百分比和连续有效曝光的时长）。并非每次广告加载都会产生可见曝光，而只有可见曝光才被认为是“有机会被看到”的。以下是不同类型广告的可见曝光条件：

| | 展示类广告 | 视频类广告 |
|--------|--------|--------|
| 像素露出要求 | 50%像素 | 50%像素 |
| 露出时长要求 | 连续 1 秒 | 连续 2 秒 |

6.4.2 计数要求

6.4.2.1 前置要求

不满足某些广告投放的质量或完整条件，或不能合规的广告曝光而无法被计入曝光计数的被称为无效曝光。广告曝光可能被归入无效的多个原因之一是非人类流量（爬虫，机器人等），或是主观故意的流量欺诈。

通过恶意操纵合规的广告投放、测量，或者主观故意造假，由此产生的被虚增的曝光量被定义为虚假流量。所有虚假流量都是无效流量（但反之不成立），且已被定义为虚假流量的曝光绝不可能是可见曝光。一些可见曝光测量机构会应用更多的技术在判断广告可见性的基础上增加对其是否有作弊行为的判别，并在报告中将不可见曝光类别下的虚假流量单独体现出来。

6.4.2.2 一般要求

关于可见广告曝光的计数，应遵循广告衡量的基本要求：

- 客户端计数
- 过滤无效流量
- 缓存清除技术

注：缓存清除技术的目的是防止广告代码请求在浏览器中因为重复触发而由浏览器缓存代替网络请求导致代码没有触发而使曝光计数不准确

- 移动端广告渲染时开始计数曝光

6.4.2.3 展示广告可见曝光要求

除了上述要求，当展示类广告符合以下条件时，才会计入可见展示广告曝光数：

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，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一秒。

上述过程中，确定像素的要求和确定时间的要求，应当在测量广告的可见性时以先后顺序执行。换句话说，最少展示像素是否满足要求应该优先于测量持续时间是否满足要求；例如，只有当确定广告已经满足 50% 像素阈值要求时，时钟才会开始计时以确定第二个条件，即广告是否满足一个连续时间的要求。

其他注意事项：

1) 用户互动的注意事项：如果验证方能够确定用户与广告之间产生了更强互动，那么即使广告不符合上述像素和时间条件，该广告也可能被视为可见（即强用户交互可直接定义可见广告曝光）。然而，鼠标悬停通常不会被视为用户与广告的交互，通常它会被视为可见性的中间代理（注意：发起点播视频广告的点击，这个动作本身不会被视为满足可见标准的用户交互）。

满足“强用户交互”的条件与特定用户间交互应当对广告和其呈现环境和内容都恰到好处，并且这些交互应该在实践中证明了其能强有力的表示广告可见。每种类型的合格用户交互都应当由测量组织进行完整公开。此外，在提供报告时，强用户交互规则（此规则并非 50% 的像素阈值和一秒持续时间的规则）带来的可见度效果应当和可见曝光分开说明。

信息流的展示广告，如果广告不满足像素和观赏时长的要求，但是如果强用户交互存在，依然可以算作可见曝光。一个真实的广告点击就可算强用户交互从而算可见曝光。但是简单的对屏幕的上下滑动通常不被认为是强用户交互。在某些情况下，例如富媒体广告或者大尺寸或全屏广告的情况下用户进行了滑动可以代表强用户交互。

每一类符合要求的强用户交互定义都需要被测量机构披露。除此之外，由用户交互规则导致的可见曝光广告数量需要被单独报告。

2) 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，也可以辅助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。可以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”。

在信息流等类似广告格式中，由于展示广告内容以特别的方式呈现给用户，这种情况下可以在次秒级建立一个可见性的新标准，这个新的度量标准叫做次秒级曝光（Sub-Second Ad Impression）：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，因为时间过短不符合可见的要求。信息流广告观看时长虽然短但却依然可以起到广告宣传的作用，（例如有的带有品牌 LOGO 的广告可以被观众更快的识别）。所以可以单独对该类曝光进行报告，协助买方和卖方测算这类曝光的价值。该度量标准只适用于信息流展示广告，不适用于信息流视频广告。

6.4.2.4 视频广告可见曝光要求

如果满足以下时间条件，并在浏览器页面的可见空间中（移动端 InApp 为终端可见空间上），符合广告像素的 50% 的面积露出标准的视频广告可以被视为可见视频广告曝光：

可见视频时间要求：要满足可见视频广告效果的计数条件，该视频广告需要被连续播放 2 秒，并且广告要满足此前提及的可见度展示的像素要求（即展示类广告中要求的 50% 或以上像素露出）。这个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 秒广告都是合规的。

其他注意事项：

1) 在某些情况下, 和视频广告相关的强用户交互也可以被视为可见曝光的替代指标。与展示广告类似, 如果有强用户交互存在, 此时可以忽略像素和时长的要求, 将其视为可见曝光。满足“强用户交互”要求的特定用户交互应该对于广告自身内容及其展示环境都恰到好处, 并且这些交互应该在实践中证明了其能强有力的表示广告可见。每种类型的合格用户交互都应当由测量组织进行完整公开。此外, 在提供报告时, 强用户交互规则(此规则并非 50%的像素阈值和一秒持续时间的规则)带来的可见度效果应当和可见曝光分开说明。即使广告不符合以上像素和时间要求, 对视频广告的合理点击也可能产生可见效果。此处需要注意的是, 简单的点击开始播放视频按钮, 不算强用户交互, 只有当视频渲染好以后, 开始在用户的浏览器界面播放后才能开始进行测量, 视频播放过程中的用户点击才可以算是强用户交互。

2) 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, 也可以辅助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, 可以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”。

3) 对于展示广告内嵌有视频广告的特殊情况来说, 通常我们以展示广告的可见性标准进行测量。还需要注意的是, 这里指的是整个广告的 50%像素, 如果被用来测可见性的标准是视频播放器像素的 50%, 而不是整个广告的, 这时需要提前将该测量方法确定, 并且对该测量方法在报告中说明。而且需要提供证据证明, 以播放器的尺寸而不是整个广告的尺寸进行测量对测量结果不会有实质性的影响。

6.4.3 广告可见性验证指南

6.4.3.1 综述

可见性曝光的验证与广告投放数测量有根本区别, 因为后者在客户端计数时不考虑广告曝光是否出现在浏览器的可见界面上并满足一定的时间要求。所以, 不是所有被投放的广告曝光都有机会被用户看到。

本标准鼓励广告可见性验证服务商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。这样的信息会为阅读报告的各方产生更大的价值, 并帮助卖方优化操作环境和广告位排版。

6.4.3.2 技术机制

广告可见性验证是通过验证代码或 UM SDK 与被验证创意一同投放到广告位后, 执行脚本从浏览器/客户端中获取各种参数来判断当前被验证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。

6.4.3.3 最低验证频率

为了使各个可见性验证服务商之间保持一定的一致性, 本标准规定以下的验证测量时间间隔进行了要求: 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。这些频率数据表示在验证并确定每一次以上两种广告类型的曝光可见性, 需要至少连续 10 次相同的测量结果。验证方不需要保存这些区间测量结果。

例如: 如某验证服务提供商表示其经验可保证使用比本标准规定的最低验证展示类广告频率 100 毫秒一次更低的频率(但不应低于 200 毫秒一次)对最终的曝光可见性验证结果并无影响, 应被认为是在可允许范围内的操作方式。

6.4.3.4 投放控制

由于广告验证服务商对广告可见性在投放前已有大规模的分析，因此可以应对广告供需方在广告投放前或投放中基于广告可见性的历史统计结果，并结合当前可获的投放参数为依据做控制。本着对品牌资产的保护以及事前预防优先的原则，本标准建议广告投放前基于广告验证结果做流量筛选，在广告投放中基于广告验证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）。

6.4.4 可见曝光验证技术规范

数字广告的验证主要集中在两种技术环境下——桌面或移动设备的网页端以及移动应用端（以下分别简称网页环境和应用APP内环境）。网页环境在桌面以及移动设备上的运行环境类似效果相仿，且在HTML5的大力推行下技术框架更趋于统一。而应用APP内环境由于移动操作系统的底层差异导致广告运行的技术环境不统一，因此在验证时需要广告供应方尽最大可能提前支持技术框架和协议。例如网页环境，根据广告类型的不同，媒体供应方需提供验证代码的运行环境（如Javascript、VAST、VPAID、等）；类似的，对应用APP内环境，媒体供应方需提供广告验证技术运行环境（如MRAID、广告验证 SDK等）。

6.5 广告品牌安全验证

6.5.1 品牌安全的定义

品牌安全是通过技术和其他手段保证数字广告不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以在投放中实时进行，也可以在后置测量过程中执行。

6.5.2 品牌安全验证的一般要求：

关于品牌安全验证，应遵循广告测量的基本要求，详见6.4.2.2 一般要求的内容。

6.5.3 广告环境验证

广告验证方应提供技术手段，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：

- 成人内容
- 协助非法活动
- 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）
- 侵犯版权
- 药物/酒精/管制药品
- 极端的图像/明显暴力内容
- 诱导对测量进行操纵
- 仇恨/亵渎
- 骚扰/间谍软件/恶意软件/ 盗版软件
- 政治/宗教
- 未经认证的由用户生成的内容
- 在广告主媒介计划以外的媒体点位

广告验证应关注潜在规避类别，以对各种情况进行规避。广告验证服务提供商应遵循潜在规避类别并清楚地向客户披露设定参数细节，以便客户对投放情况有所了解并设置预期。

广告验证服务可在维护潜在规避类别的过程中做更详细的子类别区分，以进一步细化和区分所提

供的服务。

6.5.4 执行规范

广告验证服务应维持一个流程，即定期对媒体、网络和广告交易中心进行预评估，有助于卖方能在潜在规避内容类别相关错误出现之前提前接到广告验证服务提供商的通知。

对广告品牌安全的验证可采用如下方法来执行：

1. 在广告展示页执行能够可见页面内容的监测方法。
2. 爬虫方法。但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。
3. 抽样执行验证方法。使用上述 1 或 2 的方式进行验证时，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、计算方法论必须完整披露给媒体及广告主。
4. 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。

6.5.4.1 广告投放控制

由于广告验证机构对广告环境在投放前已有大规模的分析，因此可以应对广告供需方在广告投放前或投放中基于广告品牌安全的历史统计结果，并结合当前可获的投放参数为依据做控制决策。本着对品牌资产的保护以及事前预防优先的原则，本标准建议广告投放前基于广告验证结果做流量筛选决策，在广告投放中基于广告验证结果做实时广告阻挡控制（即环境判断安全时投放，判断为风险时基于供需双方的合约做阻挡、退还、跳过和替换等广告投放控制）。

6.5.4.2 注意事项

如品牌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被认为是品牌不安全的。类似的，移动应用 APP 内广告投放时需要有机制返回 APP 包名以确认投放地点。如应用 APP 属于品牌不安全分类，应阻止广告投放至该 APP。

广告投放中有时为了特殊需要会使用 iFrame 来投放，这是允许的，但 iFrame 嵌套(nested iFrame)则会对广告验证带来困难，因此当活动中验证发现有大量的 iFrame 嵌套甚至恶意反复嵌套现象应当谨慎分析 并归入品牌安全问题流量。广告网络和广告交易平台等应依据最小化原则使用跨域 iFrame。

附 录 A
(规范性附录)
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 对于 OTT 设备: 20-Android 21-tvOS 22-0thers 23- aliyunOS | 是 | 移动、OTT | SDK/API |
| IMEI | 用户终端的 IMEI, md5 加密 | 取 md5sum 摘要 | OS=0 时, IMEI/MAC/MAC1 /AAID/OAID 至少一项必填; OS=1 时, MAC/MAC1/IDFA 至少一项必填 | 移动 | SDK/API |
| MAC | 用户终端的 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 md5sum 摘要 | OS=0 时, IMEI/MAC/MAC1 /AAID/OAID 至少一项必填; OS=1 时, MAC/MAC1/IDFA 至少一项必填 | 移动、OTT | SDK/API |
| MAC2 | OTT 终端的有线 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 md5sum 摘要 | 否 | OTT | SDK/API |
| MAC3 | OTT 终端的无线 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 md5sum 摘要 | 否 | OTT | SDK/API |
| MAC4 | OTT 终端的蓝牙 | 去除分隔符":", (保 | 否 | OTT | SDK/API |

| | | | | | |
|------|---|---|--|-----------|-------------------|
| | MAC 地址(大写去除冒号分隔符), md5 加密 | 持大写) 取 md5sum 摘要 | | | |
| MAC1 | 用户终端的 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 md5sum 摘要 | OS=0 时, IMEI/MAC/MAC1 /AAID/OAID 至少一项必填; OS=1 时, MAC/MAC1/IDFA 至少一项必填 | 移动、OTT | SDK/API |
| IDFA | iOS IDFA 适用于 iOS6 及以上 | 保留原始值 | OS=0 时, IMEI/MAC/MAC1 /AAID/OAID 至少一项必填; OS=1 时, MAC/MAC1/IDFA 至少一项必填 | 移动、OTT | SDK/API |
| AAID | Android Advertising ID | 保留原始值 | OS=0 时, IMEI/MAC/MAC1 /AAID/OAID 至少一项必填; OS=1 时, MAC/MAC1/IDFA 至少一项必填 | 移动 | SDK/API |
| DUID | Windows Phone 用户终端的 DUID, md5 加密 | 取 md5sum 摘要 | OS=2 时, 是 | 移动 | SDK/API |
| OAID | 用户终端的 OAID, 适用于 Android 系统 | 保留原始值 | OS=0 时, IMEI/MAC/MAC1 /AAID/OAID 至少一项必填; OS=1 时, MAC/MAC1/IDFA 至少一项必填 | 移动 | 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 | A.B.C.D(4 段点分), 如 12.34.56.78 | 是 | 桌面、移动、OTT | 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%3BGT-I9220%20Build%2FIMM76D) | 否 | 桌面、移动、OTT | 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、移动、OTT | SDK/API |
| EVNT | 用于区分监测的 | 英文数字下划线, | 否 | 桌面、移 | 输入 |

| | | | | | |
|-----------|-----------------------------|---|---|-----------|---------|
| | 事件,如:播放开始或者播放完成 | 如“Start” | | 动、OTT | |
| 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、移动、OTT | 输入 |
| MUID | 媒体分配的浏览器 Cookie ID 或用户 ID | 字符串,需 URLEncode | 否 | 桌面、移动、OTT | 输入 |
| LBS | 用户终端设备的经纬度地理坐标 | 十进制保留 6 位小数,西经南纬保留负数,用字母 x 分割纬度与精度(先纬后经,最后精度),如 35.758134x-122.406722x100.0 | 否 | 移动 | SDK/API |
| GEO | 用户终端设备的经纬度地理坐标 | 十进制保留 1 位小数,西经南纬保留负数,用字母 x 分割纬度与精度(先纬后经,最后精度),如 35.7x-122.4x100.0 | 否 | 移动 | SDK/API |
| OSVS | 用户终端的操作系统版本 | 字符串,需 URLEncode | 否 | 桌面、移动、OTT | SDK |
| TERM | 用户终端的机型 | 字符串,需 URLEncode | 否 | 移动、OTT | 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、OTT | SDK |
| WIFIBSSID | 客户端使用 wifi 的 MAC 地址 | 去除分隔符":", (保持大写)取 md5sum 摘要 | 否 | 移动、OTT | SDK |
| WIFISSID | 客户端使用 wifi 的名称 | 字符串, wifi 名称做 encode 处理 | 否 | 移动、OTT | SDK |
| SCWH | 用户终端的屏幕分辨率 | 宽 x 高,用字母 x 分割 | 否 | 移动、OTT | 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、OTT | SDK |
| AKEY | 媒体 APP Key | 字符串,需 URLEncode | 是 | 移动、OTT | SDK |
| ANAME | 媒体 APP Name | 字符串,需 URLEncode | 否 | 移动、OTT | SDK/API |

| | | | | | |
|----------------|---|----------------------|---|---------------|-----|
| | | ode | | | |
| SDKVS | SDK 版本 | 字符串, 需 URLenc ode | 是 | 移动、OTT | SDK |
| SIGN | 签名串 | 字符串, 需 URLenc ode | 否 | 移动、OTT | SDK |
| ImpressionType | 在曝光监测中, 标志是否满足广告 开始渲染 (Bt R) 的要求 | 0=不满足 1=满足 | 否 | 桌面、移 动、OTT | 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 URLenc ode | 是 | 移动、OTT | SDK |
| isRoot | 标志设备是否 R OOT/越狱 | 0-否, 1-是, 2-未知 | 否 | 移动 | SDK |
| isSimulator | 标志设备是否是 模拟器 | 0-否, 1-是, 2-未知 | 否 | 移动 | SDK |
| isHook | 设备是否被 hoo k, | 0-否, 1-是, 2-未知 | 否 | 移动 | SDK |
| isADB | 是否处于, 仅用 于 Android 设备 | 0-否, 1-是, 2-未知 | 否 | 移动 | SDK |

下表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, 不应受到下表约束。可见曝光参数可应用于桌面端、移动端、OTT端。

| 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 | 仅能等于 1 | 否 | 预先配置 |

| | | | | |
|---------------------------------|--|--|---|-----------|
| | 数据 (AdviewabilityEvents) 上报 | | | |
| 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%3a1561956276826%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 | 否 | SDK |
| 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：

第三方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。

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：

下：

OS _IMEI_ _MAC_ _MAC1_ _IDFA_ _AAID_ _DUID_ _OAID_ _IP_
UA _TS_。

非必选的媒体输入参数，输入空值表示该值缺省。

SDK获取的可禁用的参数，可以通过修改XML配置文件实现禁用。

附 录 B

（规范性附录）

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互联网APP（应用程序）内嵌广告的监测，方案定义了一种通用可配置的、供移动APP广告媒体平台与第三方广告监测或验证平台完成数据通信SDK（下文中统称为“广告监测及验证统一SDK”，即UM SDK）。本方案不适用于其它媒体形式或其他监测方式（如 移动网页、电脑网页类广告）。

广告监测及验证统一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第三方监测或验证公司、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，至少存储有以下三种文档和信息：

- a. 监测参数配置文档，XML 格式文档，用于定义各个媒体已经接入的各家第三方监测或验证公司的参数配置规则，由媒体广告系统技术部门定期更新维护监测参数配置文档，维护的内容包括：
 1. 已接入的第三方监测或验证公司及其参数配置。
 2. 可监测的播放时点和交互事件。
- b. 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，由媒体的运营人员上传到投放系统。

监测URL，由第三方监测或验证公司提供，跟随素材设置到一般包括曝光监测和点击监测两段HTTP URL，在上传广告素材时，由媒体的运营人员设置到投放系统。

B.2.2 媒体APP

安装于浏览者(个人用户)移动终端的软件(如视频、游戏、工具、阅读等移动应用)，除了正常的 APP 内容和场景外，还包含以下模块：

- a. 广告监测及验证统一 SDK（UM 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；并在断网时，将未提交成功的监测请求及其发送失败时间存放于未成功队列，在重新联网是一并发送。
- b. UM 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。
- c. 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(素材加载、播放、播放完成等事件、点击、滑过、关闭、重播、展开等交互)时触发 UM SDK 内相应的监测提交方法。

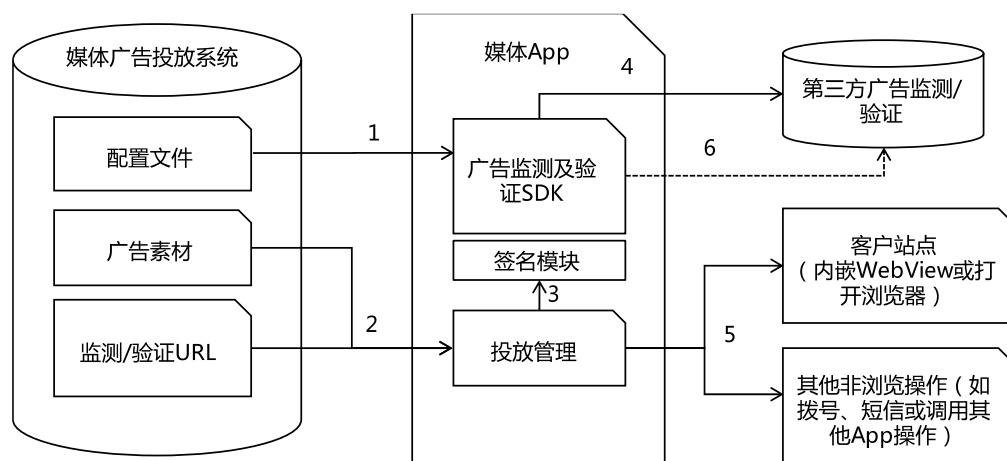
媒体 APP 运行被用户运行时，会加载并初始化 UM SDK。初始化时，媒体 APP 可以选择禁用部分参数

模块，如禁止获取经纬度坐标，未加密 MAC 地址等。

B.2.3 第三方监测和验证系统

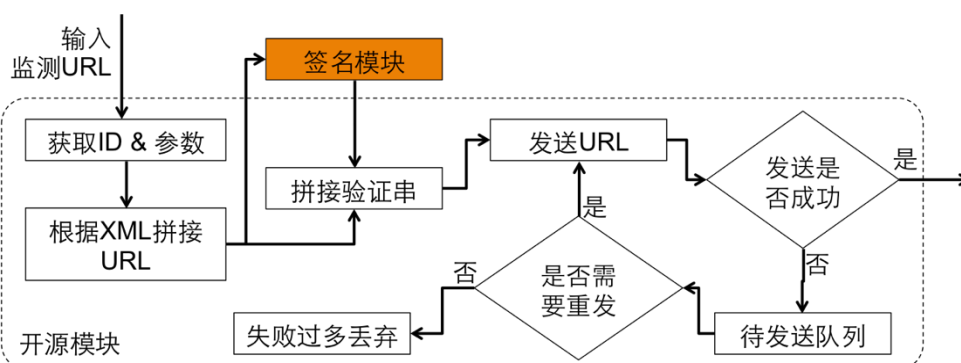
第三方监测或验证公司部署的服务器，用于记录数据并向广告主提供统计报告。

B.3 数据通信流程



图B.1 广告监测及验证统一 SDK (UM SDK) 架构设计

1. SDK 远程动态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第三方监测 URL，一般包含曝光监测 URL、点击监测 URL。
3. 媒体 APP 内的投放管理模块调用广告监测及验证统一 SDK 的“提交监测”方法(包括提交曝光监测、提交点击监测、提交事件或交互监测)，并传递监测 URL，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. 广告监测及验证统一 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 URL 后拼接 SDK 额外获取的参数(如：机型和操作系统、屏幕分辨率、加密的 MAC 地址等参数)，向第三方监测或验证系统服务器提交监测请求。
广告监测及验证统一 SDK 中的签名模块可以对监测 URL 进行签名校验。广告监测及验证统一 SDK 根据输入 URL 生成签名校验串并拼接在 URL 尾部，发送到监测系统，第三方监测或验证公司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，符合广告监测或验证标准建议的监测方式。
6. 如果用户处于断网状态，广告监测及验证统一 SDK 将暂时无法提交的监测请求存放待发送队列。广告监测及验证统一 SDK 会定时检查(定时间隔为每 10 秒~5 分钟，可由媒体 APP 初始化 SDK 时定义，默认为 60 秒)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 广告监测及验证统一SDK (UM 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。（参见B. 5.1 初始化配置更新策略）

B.4.2 广告行为数据发送策略

为了确保请求发送成功，因此在配置文件中，还包含三个可配置的值，分别是：

- 待发送队列缓存的长度
- 失败队列的重试时间间隔
- 发送请求的超时时间

当程序内部通过调用 SDK 中的方法发起监测请求时，该请求不会被立即发送，而是记录在一个待发送队列中，当监测请求个数达到长度值，或者距离上次发送请求时间间隔超过 1 小时时，SDK 会自动发送待发送队列中的请求。

为了减少网络调用，通过监测 SDK 可以配置监测日志达到一定数量时再进行批量发送，通过修改配置文件中的 长度参数进行设置，比如 长度值设定为 5 时，本地监测条数大于 5 条时，本地的监测日志才会批量发送给远程的服务器，如果要保证监测实时发送，请将配置文件中的 长度参数设定为 0。

监测请求如果发送成功，该请求会被从待发送队列中删除，如果发送失败，该请求会进入失败队列。

联网情况下，失败队列中的请求每隔重试间隔的时间会发送一次，如果发送成功，该请求会被删除，如果发送失败，该请求继续保留在失败请求队列中，如果失败次数超过 3 次，该记录会被移除。

B.5 广告监测及验证统一SDK (UM SDK) 初始化与安全校验

B.5.1 初始化配置更新策略：

- 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 广告监测及验证统一SDK（UM SDK）安全校验相关

a) iOS 编译、解包、校验

签名模块统一编译为静态连接库.a 文件

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（经过静态连接库的整合后，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）

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

签名模块采用 C 语言 NDK 方式独立编码为 .so 资源文件

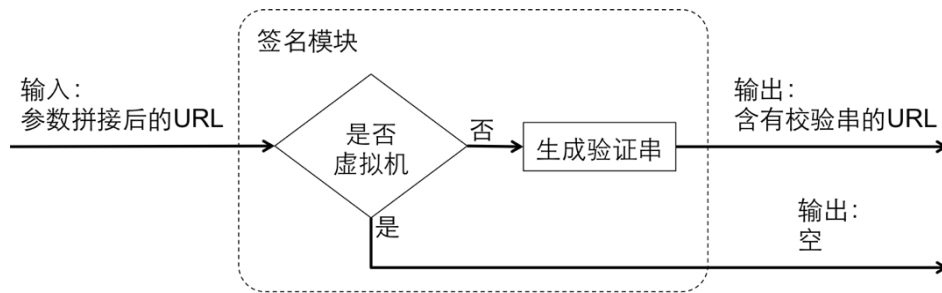
编译方法：开源代码部分各媒体单独编译，并嵌入签名模块 .so 资源文件后，发布 APP。

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。

c) 签名模块机制流程 (如下图):

检查运行环境是否是虚拟机，当检查到虚拟机时返回特殊字符串。

按照输入生成校验串后返回给开源模块



附 录 C
(规范性附录)
无效流量监测字段

C.1 无效流量监测字段

在无效流量监测中首先要甄别出一般无效流量监测字段,从而识别出其中非经正常用户产生、无效、多余、重复或无法识别的数据流量字段。如表D.1所列。

表C.1 一般无效流量监测字段

| 序号 | 字段 | 说明 | 是否必须 |
|----|----------------|--|------|
| 1 | 事件类型 | 描述业务或转化的信息,例如曝光、点击等 | 是 |
| 2 | 广告系列 ID | 包括广告活动、媒体、广告位等信息,至少包含广告唯一 ID | 是 |
| 3 | 时间戳 | 格林威治时间 1970 年 01 月 01 日 00 时 00 分 00 秒(北京时间 1970 年 01 月 01 日 08 时 00 分 00 秒)起至现在的总秒数 | 是 |
| 4 | IP 地址 | 用户端 IP 地址,不能为直接用户通过接入互联网服务商所获得的互联网 IP 地址以外的 IP | 是 |
| 5 | 请求方式 | HTTP 协议中的请求方式,如 GET、POST 和 HEAD 等 | 是 |
| 6 | 用户代理信息 | 网页为包含浏览器和操作系统的 User-Agent 完整字符串,PC 客户端(如视频客户端)和移动 App 应含有 App 名称、App 版本及操作系统等基本信息 | 是 |
| 7 | COOKIE/设备唯一标识符 | 用户的唯一标识,需满足网页端可读写 COOKIE 或移动端可获取到设备唯一标识的情况下可用 | 是 |
| 8 | 预加载 HEADERS | 如 X-MOZ/FireFox, X-Purpose/Safari 等 | 否 |
| 9 | 适用的 OpenRTB 属性 | 投标唯一标识、广告位类型、请求安全协议标识符等 | 否 |
| 10 | 广告页面 URL | 当广告展示在网页、移动网页或任何通过浏览器使用 http 或 https 协议可以访问的页面时 | 是 |
| 12 | App 程序完整包名 | 仅当广告展示在移动 APP 内部时 | 是 |
| 13 | 位置信息 | 需注明所使用的坐标系规格 | 否 |
| 14 | 请求状态码 | HTTP 请求返回的状态码,如 200、302、400 等 | 否 |
| 15 | 视频/音频广告开始播放的标志 | 仅当视频/音频广告需要被用户点击后开始播放的场景 | 是 |