iab. TECH LAB

id-sources.json
Technical Specification

Draft in Public Comment as of October 13, 2021

Please email support@iabtechlab.com with feedback or questions. This document is available online at https://iabtechlab.com/standards/id-sources

Special thanks to:
Caitlin Fitzharris, Index Exchange; Brian May, Dstillery; Scott Menzer, ID5; Chris Muellenbach, LiveRamp; Mike O'Sullivan, Roku

A full list of Rearc Accountability Working Group participants is available at the following link: https://iabtechlab.com/working-groups/rearc-accountability-working-group/

IAB Tech Lab Lead:
Alex Cone, VP Privacy & Data Protection

About IAB Tech Lab
The IAB Technology Laboratory is a nonprofit research and development consortium charged with producing and helping companies implement global industry technical standards and solutions. The goal of the Tech Lab is to reduce friction associated with the digital advertising and marketing supply chain while contributing to the safe growth of an industry.

The IAB Tech Lab spearheads the development of technical standards, creates and maintains a code library to assist in rapid, cost-effective implementation of IAB standards, and establishes a test platform for companies to evaluate the compatibility of their technology solutions with IAB standards, which for 18 years have been the foundation for interoperability and profitable growth in the digital advertising supply chain. Further details about the IAB Technology Lab can be found at https://iabtechlab.com.

Disclaimer

THE STANDARDS, THE SPECIFICATIONS, THE MEASUREMENT GUIDELINES, AND ANY OTHER MATERIALS OR SERVICES PROVIDED TO OR USED BY YOU HEREUNDER (THE "PRODUCTS AND SERVICES") ARE PROVIDED "AS IS" AND "AS AVAILABLE," AND IAB TECHNOLOGY LABORATORY, INC. ("TECH LAB") MAKES NO WARRANTY WITH RESPECT TO THE SAME AND HEREBY DISCLAIMS ANY AND ALL EXPRESS, IMPLIED, OR STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AVAILABILITY, ERROR-FREE OR UNINTERRUPTED OPERATION, AND ANY WARRANTIES ARISING FROM A COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE. TO THE EXTENT THAT TECH LAB MAY NOT AS A MATTER OF APPLICABLE LAW DISCLAIM ANY IMPLIED WARRANTY, THE SCOPE AND DURATION OF SUCH WARRANTY WILL BE THE MINIMUM PERMITTED UNDER SUCH LAW. THE PRODUCTS AND SERVICES DO NOT CONSTITUTE BUSINESS OR LEGAL ADVICE. TECH LAB DOES NOT WARRANT THAT THE PRODUCTS AND SERVICES PROVIDED TO OR USED BY YOU HEREUNDER SHALL CAUSE YOU AND/OR YOUR PRODUCTS OR SERVICES TO BE IN COMPLIANCE WITH ANY APPLICABLE LAWS, REGULATIONS, OR SELF-REGULATORY FRAMEWORKS, AND YOU ARE SOLELY RESPONSIBLE FOR COMPLIANCE WITH THE SAME, INCLUDING, BUT NOT LIMITED TO, DATA PROTECTION LAWS, SUCH AS THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (CANADA), THE DATA PROTECTION DIRECTIVE (EU), THE E-PRIVACY DIRECTIVE (EU), THE GENERAL DATA PROTECTION REGULATION (EU), AND THE E-PRIVACY REGULATION (EU) AS AND WHEN THEY BECOME EFFECTIVE.

Table of Contents

1 Introduction

Many participants in the ads ecosystem, from digital properties (publishers *and* brands) to ad technologies, may choose to integrate various unique-to-user identifiers, referred to in this specification as “ID sources.” For any given ad related transmission, there may be many ID sources passed along in the supply chain both client and server-side. While it is possible to use developer tools to inspect client to server ID source transmissions there is no known standard which provides all ads ecosystem participants with a common method of disclosing which ID sources they integrate. Providing ads ecosystem participants with a standard way to disclose integrated ID sources creates a new layer of transparency which allows for more accurate analysis and understanding of companies connecting to unique-to-user identifiers.

This specification is for <u>all</u> digital ads ecosystem participants choosing to integrate with any and all unique-to-user ID sources, whether those sources are used for cross-site, cross-app, and cross-channel purposes or “first party” only. This includes:

- Publishers
- Advertising technology providers
- Agencies
- Advertisers

This specification is meant for cases when a unique-to-user identifier is ingested by or knowingly passed along between entities

1.1 Guiding Principles

- Consistency with other IAB Tech Lab supply chain transparency is helpful to industry integration and adoption (i.e., sellers.json and buyers.json)
- Simplicity of implementation is important for wide adoption
- An entity using an identity source of any flavor should be comfortable being transparent about it

2 Specification

2.1 Access Method

Participants should post the id-sources.json file on their root domain and any subdomains as needed. For the purposes of this document the “root domain” is defined as the “public suffix” plus one string in the name. Crawlers should incorporate Public Suffix list [16] to derive the root domain.

The declarations must be accessible via HTTP and/or HTTPS from the website where the instructions are to be applied under a standard relative path on the server host: "/id-sources.json" and HTTP request header containing "Content-Type: application/json". Additionally, you could use "Content-Type: application/json; charset=utf-8" to explicitly signal UTF8 support. Also, HTTPS connections over HTTP are preferred when crawling id-sources.json files. In any case, where data is available at both an HTTPS and an HTTP connection for the same URL, the data from HTTPS should be preferred.

For convenience we will refer to this resource as the "/id-sources.json" file. Despite the use of the word "file," the resource need not originate from a file system.

If the server response indicates Success (HTTP 2xx Status Code,) the advertising system must read the content, parse it, and utilize the declarations.

If the server response indicates an HTTP/HTTPS redirect (301, 302, 307 status codes), the advertising system should follow the redirect and consume the data as authoritative for the source of the redirect, if and only if the redirect is within the scope of the original root domain defined as the public suffix plus one string in the name as defined above. Multiple redirects are valid if each redirect location remains within the original root domain. For example, an HTTP to HTTPS redirect within the same root domain is valid. Only a single HTTP redirect to a destination outside the original root domain is allowed to facilitate one-hop delegation of authority to a third party's web server domain. If the third-party location returns a redirect, then the advertising system should treat the response as an error. A future version may address other delegation of authority to a third-party web server, but for now redirects to a third-party web server and any other redirect should be interpreted as an error and ignored.

If the server response indicates the resource does not exist (HTTP Status Code 404) or for any other HTTP error, the last successfully retrieved data set should be utilized.

2.2 File Format

All data in the file is serialized using JSON (JavaScript Object Notation). The parent JSON object and all child objects are written to the id-sources.json file.

2.3 Expiration

Systems that consume /id-sources.json should cache the files and periodically verify that the cached copy is fresh before using its contents.

Standard HTTP cache-control mechanisms can be used by both origin server and robots to influence the caching of the /id-sources.json file. Specifically, consumers and replicators should take note of the HTTP Expires header set by the origin server. A maximum expiry of 7 days is recommended. If no cache-control directives are present, consuming systems should default to an expiry of 7 days.

2.4 Implementation

Every digital advertising ecosystem participant which integrates with a unique-to-user identity source should publish an id-sources.json file at the following location:

https://{participantdomain}/id-sources.json

Examples of unique-to-user identity sources:

- ID sources found in Prebid's User ID Module
- Device provided advertising identifiers like mobile ad IDs
- Platform storage mechanisms like cookies

2.5 Object Specifications

Object: Parent

The Parent object is the top-level of an id-sources.json file. It is a container for all properties in an id-sources.json file.

Attribute	Type	Description
`version`	String; required	The version of this spec
`last_updated`	Datetime; required	Last time this file was updated
`sources`	Object array; required	The list of all source objects that a participant uses or integrates with. All identity sources must be included even if they are non-commercial or come standard from a platform (i.e., IDFA).
`contact_email`	String (optional)	An email address to use to contact the participant for questions or inquiries about this file (ex. integrations@partipant.com)

Object: sources

The sources object array is required by all participants who publish an id-sources file to provide transparency into the full list of unique-to-user and device ID sources they are built to support. "Support" means knowingly integrating, passing, and/or acting upon an ID source. For example, a publisher may work with two ID resolution vendors and an SSP may support two more additionally plus several device provided identifiers.

Attribute	Type	Description
`source`	String (required)	A value that references the parent domain of the source's owner. For those integrated with Prebid or OpenRTB, this should relate to what you put in the respective eids object. If multiple identifiers are sourced from the same domain, provide a different source object, that is tied to a different subdomain, i.e., abilitec.rlcdn.com, rampid.rlcdn.com for LiveRamp. Otherwise, if the source owner is a device or operating system follow the `ifa_type` convention set in IAB Tech Lab's IFA guidelines. See "How to Handle Device Identifiers" for more information.
`name`	String; required	The business name of the ID source. Examples: "RAMP ID", "UID2"
`transformation`	Boolean; required	Is the ID transformed in any way by this participant before transmitting it?
`transformation_methods`	Array of Enums; required if `transformation` true	Basic information on how the ID source is transformed if not passed through directly as received. See "Types of Transformation Methods" for more information on what to include.

How to Handle Device Identifiers

This specification provides transparency for all types of unique-to-user identity sources including those provided by the device (e.g., IDFA, AAID). When listing a device provided identity source use the list of ifa_types "Name" provided in IAB Tech Lab's IFA Guidance where applicable. This specification adds a few more types not in the IFA Guidance last published in 2018.

Name	Description	In IFA Guidance*
`dpid`	Generic "device provided id", but based on historical usage, common device type specific values can be used	Yes
`rida`	Roku ID	Yes
`aaid`	Google Android ID	Yes
`idfa`	Apple's cross app ID	Yes
`idfv`	Apple's ID for app vendors	
`afai`	Amazon Fire ID	Yes
`msai`	Microsoft ID	Yes
`sessionid`	Session ID	Yes
`tifa`	Samsung's Tizen ID	

** Last published in 2018*

Types of Transformation Methods

Participants to this specification may perform some type of transformation process on the ID sources they integrate with their properties and systems. When `sources.transformation` is true then listing the type of transformation(s) performed is required. This will allow anyone doing analysis to understand what, if anything, they might look for in further recipients of the same unique-to-user identifier in an ad related transmission.

Name (enum)	Description
`decrypt`	When a unique-to-user identifier is encrypted, some entities may decrypt it and others may simply pass along the encrypted form.
`hash`	Some ID sources may require participants to hash an ID before passing it along to other systems/entities.
`deal`	Some entities may take receipt of a unique-to-user identifier and turn it into a deal or other private marketplace ID that is then used or passed along to other systems/entities.
`segment`	Some entities may take receipt of a unique-to-user identifier and turn it into a segment ID that is then used or passed along to other systems/entities.

3 Example File

https://{participantdomain}/id-sources.json

```
{
  "version": "1.0",
  "last_updated": "2021-12-25",
  "sources": [
    {
      "source": "rampid.rlcdn.com",
      "name": "Ramp ID",
      "transformation": true,
      "transformation_methods": [
        "deal"
      ]
    },
    {
      "source": "uidapi.com",
      "name": "UID2",
      "transformation": true,
      "transformation_methods": [
        "decrypt"
      ]
    },
    {
      "source": "id5-sync.com",
      "name": "ID5 Technology",
      "transformation": false
    },
    {
      "source": "tifa",
      "name": "Samsung Tizen Identifier for Advertising",
      "transformation": false
    }
  ],
  "contact_email": "integrations@participant.com"
}
```

Notes for Public Comment

While developing this draft specification, IAB Tech Lab's Accountability Working Group considered including ID source descriptions to be shared by ID sources themselves. The Working Group agrees that is important work but should be carried out using a dedicated specification. The Working Group also spent a lot of time debating how to standardize ID source references. The draft specification lands on using domains, however the Working Group requests additional thoughts from the public on how ID sources might be commonly identified.