Unified ID Adoption Guidelines for DSPs

May 2019

Contents

A Device ID Equivalent Designed for the Open Web

Adserver.org and its sister ad-serving domain Adsrvr.org were created to enable ad tech companies to collaborate on the foundation of anonymous identity that our industry relies on to deliver a personalized advertising experience to customers and great results to advertisers. The Trade Desk, Inc. (NASDAQ:TTD) has been using this domain for eight years. We write an ID called TDID into the top-level cookie in this domain along with the metadata describing the status of mapping that cookie to partners. In H2 2017, TTD started making the TDID available for other parties to use it as their primary ID to better reflect the collaborative intent of the domain. The implementation is identical, and TTD continues to own and operate the domain. It is a Google AdX-approved fourth-party domain, it is included in the National Advertising Initiative (NAI) opt-out tool, and it has a privacy policy to which all adopters must adhere.

Solution Overview

Adopting demand-side platforms (DSPs) can use adsrvr.org as an ID issuing service allowing them 100% match rate data portability with all adopting SSPs, DMPs, and other DSPs.

Currently, any partner setup to do cookie mapping with TTD issues their own user ID and fires cookie sync pixels across their footprint. The end result of the cookie mapping is that they can store a map of their user ID to the TDID in a server side match table and/or a cookie. For SSPs, this allows the TDID to be looked up at bid time and included in the bid request. For DMPs, it allows them to upload data segments to TTD keyed by TDID instead of their own ID.

Going forward, TTD will start allowing the use of the TDID the primary user ID for any partners that would like to participate in this initiative. Partners will be able to use the existing cookie mapping endpoints that they're already using to extract the TDID and then simply use it as their own ID. When a partner identifies a new user they can redirect the user to adsrvr.org's cookie mapping endpoint which will either extract the existing TDID from adsrvr.org cookies or issue a new TDID and redirect back to the partner's configured endpoint.

Essentially, partners will leverage the adsrvr.org endpoint as an ID issuing service. Adsrvr.org in turn will work towards propagating new users across participants so that we improve the coverage and match rate for all partners that are using TDID as their primary ID.

Set-Up Procedure

Step 1 – Adsrvr.org Setup

All adopting parties will need to be configured as a partner in Adsrvr.org system. This is the same setup for a standard cookie mapping to Adsrvr.org.

(If you are already set up with a standard cookie mapping to Adsrvr.org, you can skip this section and move to Step 2.)

Adopting parties will provide URLs (`http` and `https`) to their server with two required query string parameters, one for the TDID and another for the TTL. These will be stored internally in the database in Adsrvr.org with macros that are substituted with the values before being redirected back to the partner's endpoint.

Here is an example of one such URL.

```
http(s)://partnername.com/pixel?tdid=%%TDID%%&ttl=%%TTL%%
```

where:

- `%%TDID%%` is substituted with the TDID generated by Adsrvr.org, and
- `%%TTL%%` is substituted with timestamp of the expiration time, at which point the adopting party will need to refresh the TDID. The expiration time is in terms of the seconds elapsed since 5/11/2011, which is referred to as TTD Epoch.

As mentioned above, Adsrvr.org supports the federation of alternative consortiums user IDs. If Adsrvr.org has a consortium user ID available at the time it receives the call from a partner's cookie sync pixel, it will be added onto the partner's URL as another query string parameter; for example, `appnexus_id`**.** Any additional user IDs that we federate in the future will be available as additional query string parameters. We will provide a table of these query string parameter names, so that code may be added at the partner's server to parse them out and use them as appropriate.

Note: Adopting parties will receive a Cookie Mapping Partner ID, created in the Adsrvr.org system. This ID is required in step 2.

Step 2 – DSP Partner Page Setup

The DSP partner page needs to immediately redirect any new users to the Adsrvr.org endpoint. For users who are also new to adsrvr.org, a new TDID will be issued. For users new to the partner who already exist on Adsrvr.org, the existing TDID will be returned.

Format the cookie mapping URL for Adsrvr.org like this:

```
http(s)://match.adsrvr.org/track/cmf/generic
?ttd_pid=<cookiePartnerId>&ttd_tpi=1
```

where:

- `<cookiePartnerId>` is the Cookie Mapping Partner ID received at the time of Adsrvr.org setup, and
- `ttd_tpi` indicates that this is a cookie mapping request initiated by the partner. Adsrvr.org will then redirect the user's browser to the partner URL provided at the time of setup and substitute the `%%TDID%%` macro with the TDID for the user and the `%%TTL%%` macro with the expiration time, as described in Step 1.

The partner can then parse the TDID value received in the query string and use it as their primary user ID. Partners are encouraged to re-sync the ID with adsrvr.org at the TTL interval specified on the query string.

Note: If you are a partner DSP already using a customized version of the cookie mapping URL to Adsrvr.org, that will mapping continue to function as before. We do not require you to switch to the format outlined in the example above. If you do use a customized version, Adsrvr.org will infer the `<cookiePartnerId>` from the path of the endpoint itself.

Using the TDID

To use TDID, DSPs need to start logging and bidding against some additional identifiers contained within bid requests. These identifiers are located within the user object inside a standard OpenRTB bid request, as shown in this example:

```
{
    "user": {
        "id": "... unchanged ...", #index exchange identifer
        "buyerid": "... unchanged ...", #dsp specific identifier
        "ext": {
            "eids": [{
                "source": "adserver.org",
                "uids": [{
                    "id": "uid123", #id received from request
                    "ext": {
                        "rtiPartner": "TDID" #outgoing name
                }]
            }]
        }
    }
}
```

The available values in the TDID are summarized in this table:

Value	Example	Description
t	`1531859913100`	UNIX timestamp of when the TDID was retrieved
d.response	`"match"`	Result of the call to the adsrvr.org endpoint
e	`1537184912609`	UNIX timestamp that indicates when the local object will expire
d.data.TDID_LOOKUP	`"TRUE"`	Boolean result of whether or not an existing or new ID was returned (successful server-side lookup)
d.data.TDID_CREATED_AT	`2018-08-10T11:48:32`	Timestamp indicating when the user ID was created on the server
d.data.TDID	`4e555440-e1ba-460a-bf59-24599c187221`	User ID that the adsrvr.org endpoint returned

General Note on Disabled Third-Party Cookies

If third-party cookies are disabled in a user's browser, as they are by default in Safari, the cookies set by an SSP, DSP, or DMP will be rejected because these are set on the response to a pixel firing in a page that's running in a different top level domain, such as the publisher's or the advertiser's domain. If cookies can't be set and used at ad serving time, it is impossible to have any reliable notion of identity.

Privacy and Compliance

The EULA (www.thetradedesk.com/general/uid-eula) sets out requirements to which adopters must adhere.

Opt-Out

All adopters must honor user preferences. Adopters should check for the opt-out state at least every 14 days.

A list of opted-out IDs will be available via service, details are TBD.

The opt-out state is also available on resync; an opted-out client will return 0s on resync.

Once an opt-out is received, it should be honored accordingly. This includes no further use of the opted-out ID, and may include passing it on to other parties, depending on your circumstances.

If the ID has changed between re-syncs, you must update the ID. You must not tie together data with different IDs for the same device from the ID service across deletion or opt-out events. For example, if a user clears cookies, and subsequently gets a new ID, you should not try to merge data from the pre-cookie clearing ID with data from the post-cookie clearing ID.

You should treat data associated with expired IDs according to your retention policies and other legal requirements.

GDPR

The ID issuing service supports the IAB Transparency & Consent Framework (TCF) and will expect to receive an appropriate TCF legal basis signal with a GDPR-applicable ID request. When you receive IAB TCF signals you should honor them according to IAB TCF policy.

Changes to this Specification

The service and this specification may be updated from time to time. Upon such updates, adopters' integrations must be updated to conform within a commercially reasonable time.