

Unified ID Adoption Guidelines for DMPs

March 2019

Contents

- A Device ID Equivalent Designed for the Open Web..... 2
- Solution Overview 2
- Set-Up Procedure..... 2
 - Step 1 – Adsrvr.org Setup 2
 - Step 2 – DMP Partner Page Setup..... 3
- Migration Strategies..... 4
 - DMPs Already Storing the Cookie Map to TDID..... 4
 - DMPs Requiring The Trade Desk to Store the Cookie Map to TDID..... 5
 - DMPs with No Integration with The Trade Desk 5
- Advantages of TDID Integration..... 5
- General Note on Disabled Third-Party Cookies..... 5
- Privacy and Compliance 5
 - Opt-Out 5
 - GDPR 6
 - Changes to this Specification 6

A Device ID Equivalent Designed for the Open Web

Adserver.org and its sister ad-serving domain Adsvr.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 DMPs can use adsvr.org as an ID issuing service allowing them 100% match rate data portability with all adopting SSPs, DSPs, and other DMPs.

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 adsvr.org's cookie mapping endpoint which will either extract the existing TDID from adsvr.org cookies or issue a new TDID and redirect back to the partner's configured endpoint.

Essentially, partners will leverage the adsvr.org endpoint as an ID issuing service. Adsvr.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 – Adsvr.org Setup

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

(If you are already set up with a standard cookie mapping to Adsvr.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%%&ttd_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 – DMP Partner Page Setup

The DMP 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/cmfgeneric  
?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 adsvr.org at the TTL interval specified on the query string.

Note: If you are a partner DMP already using a customized version of the cookie mapping URL to Adsvr.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, Adsvr.org will infer the `<cookiePartnerId>` from the path of the endpoint itself.

Migration Strategies

The migration strategy for DMPs moving to the TDID depends on the level of current integration with The Trade Desk. There are three primary scenarios:

- DMPs already storing the cookie map to TDID
- DMPs requiring The Trade Desk to store the cookie map to TDID
- DMPs with no integration to The Trade Desk.

DMPs Already Storing the Cookie Map to TDID

DMPs with an existing integration with The Trade Desk already storing match tables which map the DMP user ID to The Trade Desk user ID already have a TDID (which is the standard Trade Desk ID) in their match tables.

They can start to offer their existing data segments, in terms of the TDID, almost instantly to any party adopting the TDID by looking up the DMPID→TDID map.

New users created after the switch to using TDID will only have data in terms of the TDID.

As the DMPs migrate existing users over to TDID, they should update all references to their legacy ID with the TDID in the data segments, as well as in any cookie maps that they store which map their legacy ID to another party's ID.

For example, if a DMP is working with The Trade Desk and another DSP, it would start with having data segments in terms of DMPID and cookie maps for both DMPID→TDID and DMP→DSPID. As new users get created and existing users get migrated the DMPID→DSPID map will gradually transition to being an TDID→DSPID map.

Any adopting party can then lookup the DMPID→TDID map and return data segments in terms of the TDID.

Any segments that contain a mix of DMPID and TDID (due to new users being added to the segment along with a gradual migration of old users to TDID) would look up the DMPID/TDID→DSPID map to be able to send the segment in terms of the DSPID to the other DSP with whom they are working.

DSPs that store a DMPID→DSPID cookie map will need to start receiving data segments with the TDID. They will need to also ingest the DMPID→TDID map in bulk so they can update their DMPID→DSPID map before they can start receiving data segments in terms of the TDID.

DMPs Requiring The Trade Desk to Store the Cookie Map to TDID

DMPs that require The Trade Desk to store the TDID cookie map will need to ingest the DMPID→TDID map from Adsvr.org to offer data segments in terms of TDID. They will also gradually start migrating their legacy user IDs to the TDID.

Existing users can be looked up in the DMPID→ID map. New users should be redirected to Adsvr.org to issue TDIDs as described in the previous section.

DMPs with No Integration with The Trade Desk

DMPs with no current integration with The Trade Desk will need to start a cookie mapping process and gradually migrate users over to the TDID. They may need to wait until their existing users are mapped before they can begin to offer data segments in terms of TDID.

New users will get TDIDs directly from Adsvr.org, yielding results the same as for those DMPs that store the cookie map from their ID to the TDID, as described above.

Advantages of TDID Integration

After you have integrated the TDID standard, you will, of course, experience improved match rates with The Trade Desk. But you will also see enhanced performance with any other DSP that has integrated the TDID standard. You can easily exchange your data with these DSPs. As your experience with TDID-supporting DSPs grows and your confidence increases, you can drop ID synchronization with these DSPs and realize significant infrastructure and processing savings.

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.