

# PAIR

## Publisher Advertiser Identity Reconciliation

### What is PAIR

PAIR is a secure and privacy-forward way for enabling advertisers and publishers to reconcile their first-party data for marketing use cases via advanced data encryption methods without the reliance on third-party cookies.

### How PAIR works

The PAIR protocol leverages an encryption process wherein an input string has consecutive encryption keys applied on it (e.g. 'A' and 'P'). Regardless of the order of the application of the keys, the output is the same for a given input (jane@mail.com\*A\*P = jane@mail.com\*P\*A = xxx). This method is called commutative ciphers.

### Follow the nine steps below to view the PAIR process

### Start

#### PAIR protocol in clean room (offline)

Advertiser and publisher could be using different instances in the same clean room or be using different clean rooms. Clean room providers who adopt the PAIR protocol will be interoperable with each other to give advertisers/publishers choice.

The arrows between the advertiser and publisher instances will be API protocols that Display & Video 360 will define as part of the PAIR protocol. It will be opened up to anyone who would like to adopt it.

#### 1 Encrypted instances

- |   |  |
|---|--|
| <b>Advertiser</b> <ul style="list-style-type: none"> <li>Advertiser access only</li> <li>Dataset upload</li> <li>Publisher pairing</li> </ul> | <b>Publisher</b> <ul style="list-style-type: none"> <li>Publisher access only</li> <li>Dataset upload</li> <li>Advertiser pairing</li> </ul> |
|---|--|

#### 2 (A)(P) generation coordination

Each advertiser has a unique Advertiser key (A), and each publisher has a unique Publisher key (P). A publisher's Secret key (S) remains constant across all of their advertiser partnerships. The publisher instance shares (S) with the advertiser instance which leads to advertiser-publisher specific identifiers. Publishers manage only a single identifier (S)(P) per user, regardless of the number of advertiser partners. Advertisers receive multiple identifiers per user since (S) is publisher-specific, but this complexity is managed by the clean room and DSP. Note that the (A) and (P) keys remain constant for all matches.

#### 3 Generation of advertiser and publisher encrypted identifiers

Original datasets are enhanced with AdvPubID\* and with Advertiser Encrypted Key IDs (e.g. 11 depicted as a blue box) or with Publisher Encrypted Key IDs (e.g. aa depicted as a yellow box).

*\*AdvPubID is an index field that uniquely identifies a specific advertiser-publisher relationship*

#### 4 Share encrypted lists

Advertiser and publisher clean room instances share encrypted lists with each other. This dataset does not include any PII.

#### 5 Clean room reapplies its key to get PAIR

PAIR protocol runs for every advertiser-publisher pair to create multiple copies of the original dataset with unique IDs on a per advertiser-publisher basis for the same end user. The advertiser applies (A) key on the dataset received from the publisher, and the publisher applies (P) key on the dataset received from the advertiser (e.g. 2f depicted as a green box). This three-time encrypted identifier is referred to as the PAIR ID and will never leave the clean room instances. This dataset does not include any PII.

#### 6 PAIR lists shared

Advertiser and publisher clean room instances share PAIR list with each other. This list only contains AdvPubID and PAIR ID.

#### 6A PAIR based user lists shared with Display & Video 360

Once a list of matched PAIR IDs has been shared in step 6, the advertiser clean room instance can decrypt the IDs by using the (A) key to return the identifier that is encrypted by the (S) and (P) keys. This is done without requiring access to the underlying raw PII or to the (P) key. This list of identifiers is then shared with Display & Video 360 in step 8.

#### 7 Offline match rate

Offline match rates are shared with advertisers and publishers. Only aggregate match rates are shared and no user-specific matches are revealed. Advertisers and publishers may get access to advertiser or publisher encrypted identifiers (blue and yellow boxes) respectively. The PAIR IDs (three-time encrypted green boxes) don't leave the clean room instances.

### Next

#### PAIR instance in Display & Video 360

#### 8 PAIR instance within Display & Video 360

- Advertiser clean room provides the dataset from step 6A to Display & Video 360. No keys are shared with Display & Video 360.
- Display & Video 360 and Campaign Manager 360 can access this instance with advertiser provided permissioning for data partners.
- No list or identifier is downloadable from Display & Video 360.

### Finish

#### PAIR online workflow

#### 9 During the bid-request bid-response process

- |   |  |
|---|--|
| <b>Advertiser</b> <p>Advertisers can automatically pull in PAIR lists for targeting on campaigns. Advertisers can also use their own first-party IDs that may be present in conversion tags to measure conversions in the clean room if mapped against advertiser encrypted IDs.</p> <p><i>Note: Online match rates are expected to be lower than offline match rates and will be influenced by the length of the campaign, how often the end user visits the publisher site, and the offline match rate.</i></p> | <b>Publisher</b> <p>Publishers will use dataset provided in step 7 and enhance their back-end mapping tables with the publisher encrypted IDs. When a user visits the publisher's property, the publisher performs a high speed lookup and passes on publisher encrypted ID in the bid request (KsKp).</p> |
|---|--|

### Why use PAIR

- Improve reach for existing audience amid industry privacy shifts
- Control of first-party data:
  - No pooling of data
  - No leakage of data
  - No leakage of insights
- Durable for the future using secure encryption methods
- Use across SSPs
- No tracking across the web

