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

clean room if mapped against advertiser

encrypted IDs.

speed lookup and passes on publisher encrypted

ID in the bid request (KsKp).

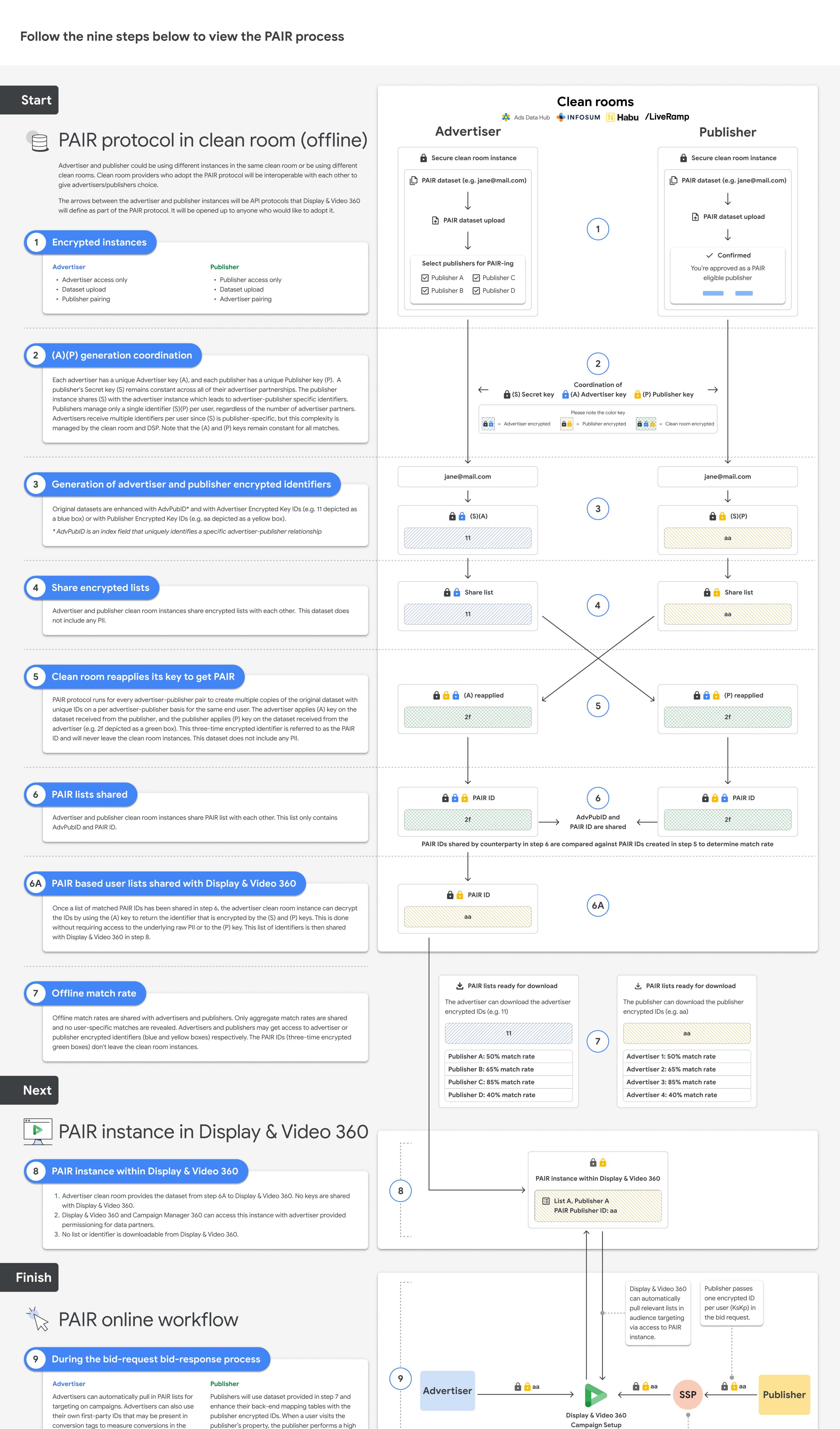
Note: Online match rates are expected to be lower than offline match rates and will be influenced by the

length of the campaign, how often the end user visits the publisher site, and the offline match rate.

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.

Why use PAIR

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



Publisher can use any

SSP of choice.