

Data Platform

01/09/2025 10:49 am EST

Core Value Proposition

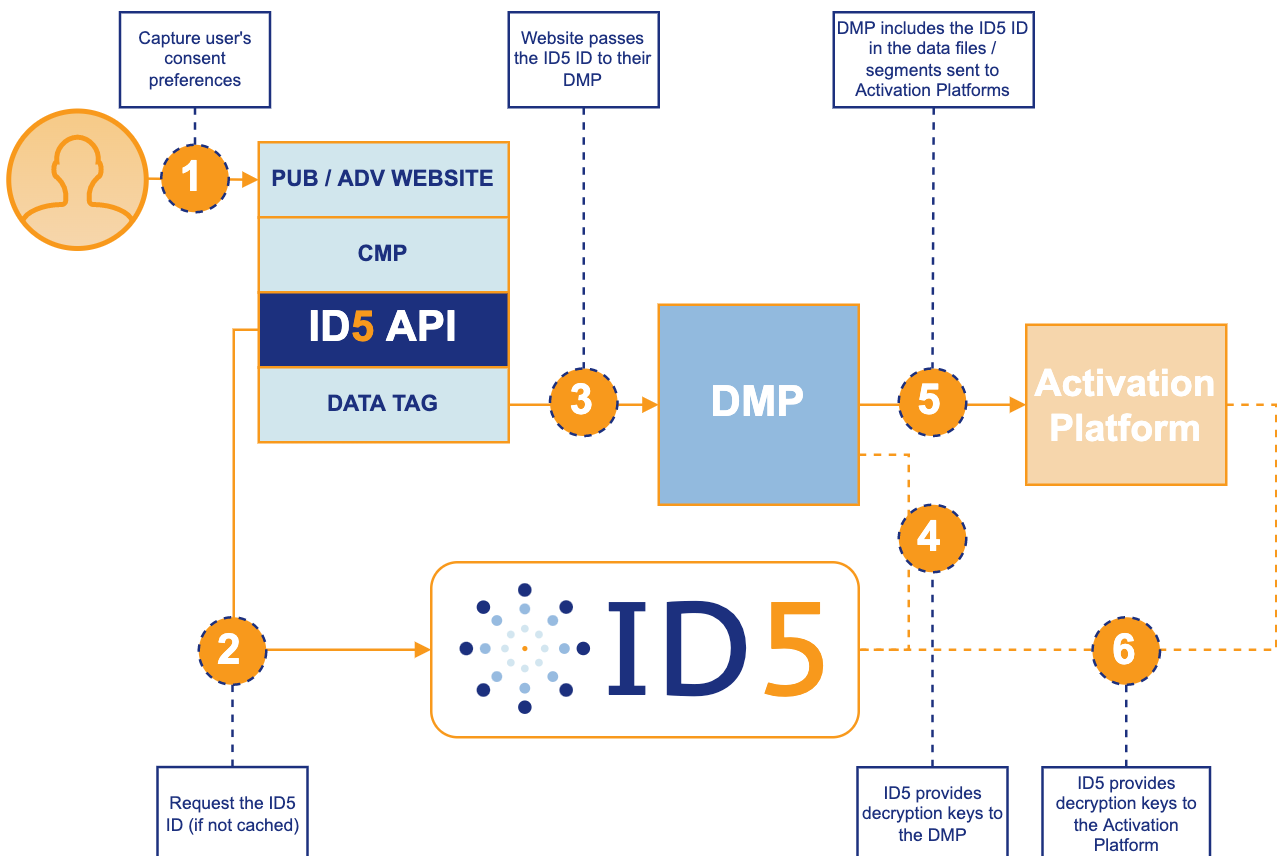
1. Improve user identification with the Partner Graph and maximize the availability of first and third-party data in activation platforms such as Ad Servers, SSPs and DSPs
2. Future-proof your business with the ID5 ID by enabling clients to activate audiences in cookieless environments
3. Improve efficiency and privacy compliance by outsourcing identity infrastructure to a specialized solution provider

ID5 ID Overview

The ID5 ID is a shared, neutral identifier that publishers and ad tech platforms can use to recognise users even in environments where 3rd party cookies are not available or blocked. ID5 enables publishers to create and distribute a shared 1st party identifier to the entire ecosystem. Ad tech platforms that connect with ID5 can decrypt the ID5 ID and improve their user recognition capabilities. The ID5 ID is designed to respect users' privacy choices and publishers preferences throughout the advertising value chain.

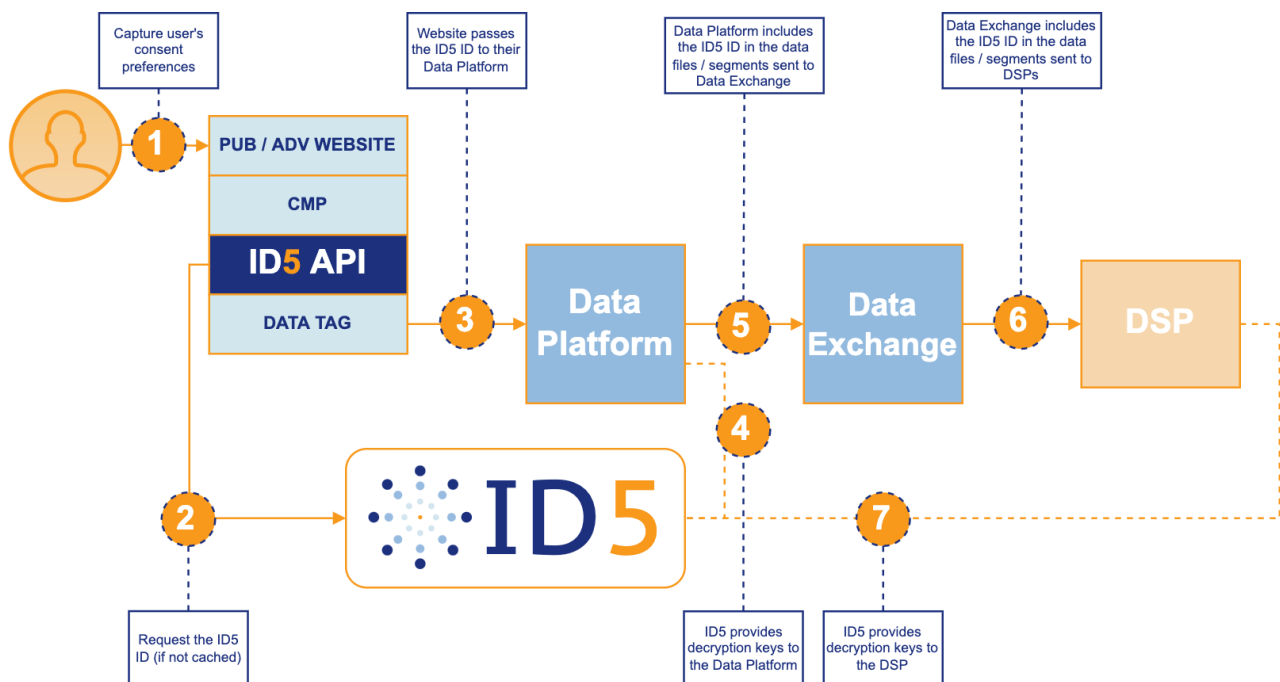
Solution Overview

Data Provider to DMP Integration



1. Publisher first loads its CMP and captures the user's consent preferences. This is essential before any IDs or ads are requested or delivered
2. The ID5 API checks in cache (local storage, 1P or 3P cookies) for an ID5 ID and ensures it is still fresh. If necessary, a request to ID5 is made for a new/refreshed ID, which is then placed in cache to avoid unnecessary http requests on future page views.
3. The DMP tag on the publisher's page retrieves the ID5 ID from the API and passes it, along with any other data signals they normally send, to the DMP servers for processing
4. In order to aggregate data and build segments, the DMP must decrypt the ID5 ID with keys provided by ID5, which happens outside of the data ingestion process.
5. The DMP pushes the generated data segments to Activation Platforms (Data Exchanges, DSPs, SSPs, etc) and includes the ID5 ID in addition to, or instead of, the normal user IDs they pass
6. Outside of the data ingestion process, the Activation Platform decrypts the ID5 ID and matches the ID5 ID to their internal ID

Data Exchange Integration



1. Publisher first loads its CMP and captures the user's consent preferences. This is essential before any IDs or ads are requested or delivered
2. The ID5 API checks in cache (local storage, 1P or 3P cookies) for an ID5 ID and ensures it is still fresh. If necessary, a request to ID5 is made for a new/refreshed ID, which is then placed in cache to avoid unnecessary http requests on future page views.

3. The DMP tag on the publisher's page retrieves the ID5 ID and passes it, along with any other data signals they normally use, to its servers for processing
4. In order to aggregate data and build segments, the DMP must decrypt the ID5 ID with keys provided by ID5, which happens outside of the data ingestion process.
5. The DMP pushes the generated data segments to Data Exchange and includes the ID5 ID in addition to, or instead of, the normal user IDs they pass
6. The Data Exchange pushes the DMP's data segments to DSPs and includes the ID5 ID in addition to, or instead of, the normal user IDs they pass
7. Outside of the data ingestion process, DSPs decrypt the ID5 ID and match the ID5 ID to their internal ID

ID5 Integration Overview

Phase 1: Collect & Log

- Integrate calls to ID5 API in data collection tags
- Listen to the ID5 ID in calls to your platform
- Log IDs for analytics purposes

Phase 2: Read & Measure

- If applicable, pass through the still-encrypted ID5 ID in raw data feeds to other platforms
- Measure potential uplift v. proprietary IDs, broken down by browser type (Chrome v. Safari/Firefox), countries, devices, etc.

Phase 3: Use & Share

- Add ID5 ID to ID graph and implement real-time decryption
- Enable analytics and audience building with the ID5 ID
- Use ID5 ID (in addition to existing IDs) when sending data segments to other platform

Integration Details

ID5 Partner Creation

Before getting started with the ID5 ID, we need to make sure you have an ID5 Partner account. If you are not already integrated with ID5, reach out to contact@id5.io and we'll get you set up right away.

Passing or Receiving the ID5 ID in Data Integrations

Data integrations between platforms are custom with no industry standards to go by. As such, you will need to work with your inbound or outbound data partner to determine the best way to receive or pass the ID5 ID with them. However, we've experienced some of these integrations and have the following tips and best practices to share.

If you'd like to hear more about how other platforms have addressed this or would like to seek advice, reach out to ID5 at contact@id5.io and we'd be more than happy to provide you some best practices and

consulting to help make your integration work.

JSON Object

If data is passed using JSON, rather than just pass a field called "id" (which could contain the inbound or outbound partner's UID), we recommend using (or creating) a user ids array that can contain multiple ids: the receiving partner's, the sending partner's, and shared IDs like ID5. An example may look like this:

```
{
  "user_ids": [
    {
      "source": "RECEIVING_PARTNER",
      "uids": [
        {
          "id": "RECEIVING_PARTNER_UID"
        }
      ]
    },
    {
      "source": "id5-sync.com",
      "uids": [
        {
          "id": "ID5-abc123"
        }
      ]
    }
  ],
  ... // additional data fields
}
```

Flat Files

If data is passed using flat files, typically it is agreed ahead of time whether to use the receiving partner's or the outbound partner's UID for all rows of data received, along with a file format for passing data. We suggest adding a field in the file format to accept a shared ID like ID5, in addition to, or instead of, the existing UID being used.

ID5 ID Decryption

ID5 encrypts the ID in order to enforce the privacy preferences of the consumer and the publisher. To learn more about how to decrypt the ID, please visit [Decrypting the ID5 ID](#) (login required).

Privacy & Regulations

Privacy-by-Design

ID5 has built a privacy-by-design shared ID service for publishers and ad tech vendors. Our service leverages the IAB's [Transparency and Consent Framework \(TCF\)](#) and [US Privacy Framework](#) to capture the user's privacy preferences.

As a shared ID provider, ID5 acts as a Controller of the ID5 ID, and thus, we must receive a valid legal basis to process requests. When we receive a request for the ID5 ID, we check that we have a legal basis to store

our user ID in a cookie before proceeding; if we don't have one, we do not read our cookie or write to it as part of the HTTP response.

When ID5 returns an ID to the page, the value is encrypted in such a way that only platforms that have authorization to process data (based on the consumer's and publisher's privacy preferences) are able to decrypt the string back to a stable ID. By doing so, ID5 enforces privacy preferences and regulations, ensuring that no downstream party can understand the ID without the proper legal basis to do so. When the ID is non-decryptable, the request is truly anonymized, preventing any personal data from being retrieved or processed.

Privacy Policy

For our Platform Privacy Policy, please visit <https://id5.io/platform-privacy-policy>.
