Unified iD

2.0

Technical Content

[Introduction 4](#_Toc68786500)

[Guiding Principles 4](#_Toc68786501)

[Components 5](#_Toc68786502)

[Identity Components 5](#_Toc68786503)

[UID2 5](#_Toc68786504)

[UID2 Token 5](#_Toc68786505)

[Infrastructure Components 5](#_Toc68786506)

[Technical Design Principles 5](#_Toc68786507)

[UID2 Administrator Service 6](#_Toc68786508)

[Functions 6](#_Toc68786509)

[UID2 Operator 7](#_Toc68786510)

[Functions 7](#_Toc68786511)

[Transparency and Control Service 7](#_Toc68786512)

[Functions 7](#_Toc68786513)

[UID2 Auditor 7](#_Toc68786514)

[Functions 7](#_Toc68786515)

[Workflow Summary 8](#_Toc68786516)

[Buy-Side Workflow 9](#_Toc68786517)

[Buy-Side (DSP) Workflow Overview 9](#_Toc68786518)

[Buy-Side Integration 9](#_Toc68786519)

[Data Provider Workflow 11](#_Toc68786520)

[Data Provider Workflow Overview 11](#_Toc68786521)

[Data Provider Integration 12](#_Toc68786522)

[Publisher Workflow 13](#_Toc68786523)

[Publisher Workflow Overview 14](#_Toc68786524)

[Publisher Integration 14](#_Toc68786525)

[User Trust Workflow 15](#_Toc68786526)

[User Trust Workflow Overview 15](#_Toc68786527)

[Opting Out of the UID2 16](#_Toc68786528)

[Frequently Asked Questions 16](#_Toc68786529)

# Introduction

Addressable advertising enables publishers and developers to provide the content and services consumers have come to enjoy, whether through mobile apps, streaming TV, or web experiences. This value exchange of the open internet has not always been well understood by, or communicated to, consumers. As the industry reduces reliance on the third-party cookie, we have an opportunity to improve how we identify consumers in the open internet. This improved identification empowers content creators to engage customers with value exchange conversations. Customers benefit equally by relaxing their privacy concerns--gaining more control and transparency over their data.

Unified ID 2.0 (UID2) is a deterministic identifier based on PII (e.g., email or phone number) with complete user transparency and privacy controls. The UID2 identifier ties logged-in experiences from publisher websites, mobile apps, and CTV apps. Benefitting from several layers of security and privacy measures, UID2s safely distribute across the open internet. Initially built (and maintained? --Udhaya) by The Trade Desk, stewardship of UID2 will transfer (in mid-2021) to independent organizations for open-source code management, governance, administration, and system operations. UID2 is a non-proprietary standard and accessible to constituents across the advertising ecosystem--including Advertisers, Publishers, DSPs, SSPs, SSOs, CDPs, CMPs, Identity Providers, Data Providers, and Measurement Providers--while they remain in compliance with a code of conduct.

UID2’s goal is to enable deterministic identity for advertising opportunities on the open internet with consumer transparency and controls in place. UID2 provides a collaborative framework for all constituents and a healthy, open internet by utilizing a transparent and interoperable approach.

## Guiding Principles

**Independent Government:** UID2 will be governed by unbiased third-party organizations, with the transition from The Trade Desk anticipated mid-2021.

**First-Party Relationships**: UID2 allows advertisers to easily activate their first-party data on publishers across the open internet.

**Non-Proprietary (Universal) Standard:** UID2 is accessible to all constituents who abide by the code of conduct in the advertising ecosystem. This includes DSPs, SSPs, data providers, measurement providers, and identity services. No individual company will controll access.

**Open-Source Framework:** UID2 code will be transparent via an open-source framework.

**Interoperable Solutions:** UID2 allows other identity solutions to integrate and provide UID2s with their offering.

**Secure and Encrypted Data:** UID2 leverages multiple layers of security, cryptography, and encryption to secure PII and user data.

**Transparency and Control:** Consumers understand where their ID is shared and what data is associated with it. Consumers also hold the right to revoke their consent and permissions.

# Components

## Identity Components

### UID2

The UID2 (raw UID2) is an unencrypted alphanumeric identifier created through a set of APIs or SDKs using a user’s verifiable and authenticated PII as an input. Examples of PII are an email address or phone number. Only members in good standing can access the UID2.

A UID2 is designed to be stored by advertisers, data providers, and DSPs and is never shared in the bidstream.

#### Technical Details

* The UID2 Operator API or SDK interface is used to create a UID2.
* The UID2 Operator SHA256 hashes the PII and adds a secret salt to the user’s PII to generate a UID2.
* Each UID2 is assigned a salt bucket. The salt for each bucket rotates once every 12 months. Each salt bucket has an alphanumeric designation between 1 and 1,000,000.
* Members who store UID2s monitor the UID2 Operator API to know when a UID2’s salt bucket rotated.

### UID2 Token

Encrypting raw UID2s creates UID2 tokens, which are transient for bidstream workflows. By utilizing cryptographic nonces and encryption, the UID2 token is different every time it enters the bidstream. This secures the UID2 ecosystem and prevents non-members from building profiles using UID2 tokens.

UID2 Tokens are designed to be stored by publishers, SSOs, and SSPs. DSPs decrypt them at bid request time.

#### Technical Details

* A cryptographic nonce is generated and appended to the UID2, which is then encrypted to create the UID2 tokens.
  + A nonce is an arbitrary number that may only be used once.
  + AES/CBC/PKCS5P with 256-bit keys are used for encryption and rotate on a daily basis.
* The UID2’s encryption timestamp is attached as payload metadata.

## Infrastructure Components

### Technical Design Principles

**Accountability:** Access to UID2 depends on members’ adherence to a code of conduct governed by an independent body. Incompliant members can lose their membership if decided by the governing authority.

**Distributed Integration:** Multiple certified integration paths provide options for publishers and advertisers to generate UID2s.

**Decentralized Storage:** Centralized location with PII-to-UID2 mapping has been eliminated to block malicious actors.

**Lean Infrastructure:** Infrastructure is light and inexpensive to operate.

**Self-Reliant:** No reliance on external services for real-time processing of RTB data.

Diagram

Description automatically generated

## UID2 Administrator Service

The centralized service manages access to the distributed UID2 ecosystem.

### Functions

* Distribute encryption keys and salt buckets to UID2 Operators.
* Distribute decryption keys to compliant members for use in decrypting UID2 tokens.
* Send UID2 user opt-out requests to Operators and DSPs.

## UID2 Operator

Organizations that operate the API to generate and manage UID2s and UID2 tokens. Multiple operators comprise the UID2 infrastructure. Participants have the option to select an Operator or become Operators themselves.

### Functions

* Receive and store encryption keys and salts from the UID2 Administrator service.
* Salt and hash authenticated PII to return a UID2.
* Encrypt UID2s to generate UID2 tokens.
* Broadcast UID2 token updates (includes--handling opt outs and salt bucket rotations) to publishers utilizing the refresh token.

## Transparency and Control Service

This service provides a user-facing website and an underlying API to enable user Transparency and Control management. Refer to the [User Trust Workflow](#_User_Trust) section for more information.

### Functions

* Offers transparency to users about their UID2 usage.
* Provides users a way to globally opt-out of UID2, which triggers opt-out requests to all UID2 data holders.

## UID2 Auditor

Organization that audits all the participant UID2 parties for compliance against a stated code of conduct.

### Functions

* Audit members of the trusted UID2 ecosystem to determine their compliance.
* Relay compliance information to UID2 Administrators and UID2 Operators.

# Workflow Summary

Four key workflows make up the UID2 ecosystem as shown in the overview diagram below:  
Diagram

Description automatically generated

In the above diagram, I recommend putting an *either-or* fork for **UID Core** at steps 3 and 4 to either send **Deletion Requests/Opt outs** or **Salt Buckets** and **Encryption Keys** (this could be a diamond in the flowchart with a Yes going one route and No going the other route). It’s further complicated that the **Deletion Requests** go from **UID Core** to **ID Operators** and also in parallel to the **DSP**s. A decision fork with three outputs; or two for Yes and one for No.

--Udhaya

The following sections drill down on each workflow separately to further illuminate their place in the entire UID2 process.

* [Buy-Side Workflow](#_Buy-Side_Workflow)
* [Data Provider Workflow](#_Data_Provider_Workflow)
* [Publisher Workflow](#_Supply-Side_Workflow)
* [User Trust Workflow](#_User_Trust_Workflow)

## Buy-Side Workflow

This workflow is for DSPs who transact on UID2s in the bidstream.

Graphical user interface, application

Description automatically generated

### Buy-Side (DSP) Workflow Overview

1. Data providers pass first party and third-party data to DSPs in the form of raw UID2s.
2. DSPs sync with UID2 Administrator to receive decryption keys.
3. DSPs access UID2 tokens in the bidstream and decrypt them at bid time.
4. DSPs listen to opt-out requests from UID2 Administrator.
5. DSPs block buying on any UID2 that has opted-out.

### Buy-Side Integration

DSPs integrate with UID2 to receive UID2s from brands (as first-party data) and data providers (as third-party data) and leverage them to inform bidding on UID2s in the bidstream.

##### Requirements

* Accept data in the form of UID2s
* Bid on data in the form of UID2s
* Build a webhook for honoring opt-out requests
* Sync encryption keys daily with the UID2 Administrator

##### Optional

If a DSP wants to generate UID2s themselves from email, see the [Data Provider](#_Data_Provider_Workflow) section on how to generate UID2s.

## Data Provider Workflow

This workflow is for organizations that collect user data and push it to DSPs. Data collectors include advertisers, data on-boarders, measurement providers, identity graph providers, third-party data providers, and other organizations who push data to DSPs.

Diagram

Description automatically generated

### Data Provider Workflow Overview

1. Data provider sends a user’s consented PII to the UID2 Operator.
2. UID2 Operator generates and returns a raw UID2.
3. Data provider stores the UID2 and salt bucket.
   1. Server-side: The data provider stores the UID2 in a mapping table, DMP, data lake, or other server-side application.
4. Data provider sends the UID2 to a DSP using permitted transport protocols defined in the code of conduct.
5. Data provider monitors the UID2 Operator for rotated salt buckets and updates UID2s as needed.

### Data Provider Integration

To generate UID2s from authenticated PII, data providers must access the UID2 Operator APIs. Some advertisers may choose to work through CDPs, data on-boarders, or other service providers instead.

##### Requirements

* Integrate with the UID2 Operator to generate UID2s and handle salt bucket rotations

## 

## Publisher Workflow

This workflow is for organizations that propagate IDs to the bidstream via SSPs. The term Publisher also covers identity providers and SSOs.

Diagram

Description automatically generated

Kanishk had mentioned that SSP should be changed to Publisher, however in the **SSP Workflow** both Publisher and SSP show up as separate agents performing together, so I’m a bit confused here!

--Udhaya

### Publisher Workflow Overview

1. A user visits a publisher website, mobile app, or CTV app.
2. The publisher explains the value exchange of the open internet and requests the user log in.
3. Once the user authenticates, the publisher sends the first-party authenticated PII and corresponding privacy settings to the UID2 Operator via an SDK or direct API integration. A publisher may authorize a SSO provider or identity provider to pass PII and privacy settings on their behalf.
4. The UID2 Operator performs the salt, hash, and encryption process and returns the UID2 Token.
5. The publisher stores the UID2 Token to share with SSPs during real-time bidding.
   1. Server-side: The publisher stores the token in a mapping table, DMP, data lake, or other server-side application.
   2. Client-side: The publishers store the token in a client-side app or in the user’s browser as a first-party cookie.
6. The publisher sends the UID2 token to the SSP at the time of impression.
7. The SSP places a bid request using the UID2 token, capturing it in the bidstream.
8. The publisher requests updated UID2 tokens using a refresh token. When applicable, the Refresh Token includes a user’s opt-out request.

### Publisher Integration

#### Publisher Direct Integration

Publishers who want to send authenticated PII and generate UID2s need to access the UID2 Operator API.

##### Requirements

* Integrate with UID2 Operator API to generate UID2 tokens
* Maintain refresh tokens or use the JavaScript client-side SDK provided by UID2 to manage the refresh token.
* Enable sending the UID2 token to SSPs and other integrating organizations.

#### Publisher Integration Through SSO or Identity Providers

Publishers may choose to work with an SSO or an independent ID provider who is interoperable with UID2. The provider may handle the UID2 integration on their behalf.

## User Trust Workflow

This workflow is for users engaging with publishers or publisher-related SSOs and identity providers. This workflow allows a user to consent to the creation of a UID2 and manage their UID2 consent and privacy settings in the Transparency and Control Portal.

Diagram

Description automatically generated

### User Trust Workflow Overview

Users visit the **Transparency and Control Portal** where they can:

1. Globally opt-out of UID2 for all publishers.
2. Opt-out requests are sent to UID2 Administrator.
3. UID2 Administrators distribute the request to DSPs.
4. UID2 Operators distribute the request to publishers utilizing the refresh token.

### Opting Out of the UID2

There are two ways for a user to opt out of the UID2. One is to send the opt out deletion key request to the DSP. That is a backup option to the preferred solution: the ID Refresh Token program.

The idea behind the ID Refresh Token is to *zero the ID* right where the user is (right on the device for the Publisher and browser) to avoid any errors. The other benefit of the ID refresh token is that this ID Refresh Token keeps the encryption constantly changing which makes it more secure and hard to breach.

# Frequently Asked Questions

## Identity

### How does a holder of UID2 know when to refresh the UID2 due to salt rotation?

Metadata supplied with the UID2 generation request indicates the salt bucket used for generating the UID2. Salt buckets are persistent and assigned to the underlying PII. Use the API provided to return which salt buckets rotated since a given timestamp. The returned rotated salt buckets inform the UID2 holder which UID2s to refresh. This workflow typically applies to data providers.

### How does a holder of a UID2 token know when to refresh it?

The UID2 token is automatically refreshed as part of the refresh token. This workflow typically applies to publishers and SSOs.

### How do companies interfacing with UID2 tokens know which decryption key to apply?

Metadata supplies with the UID2 token discloses the timestamp of encryption, which informs which decryption key applies.

## User Trust

### Can a user opt-out of targeted advertising tied to their UID2?

Yes, through the Transparency and Control Portal, a user can opt-out of being served targeted ads tied to their UID2. The request will be distributed through UID2 Administrator and UID2 Operators to all relevant members.   
  
Some publishers and service providers have the option to limit access to their products based on a user’s participation in UID2 and it is the publisher’s responsibility to communicate this as part of their value exchange dialogue with the user.

### How does a user know where to access the Transparency and Control Portal?

Publishers, SSOs, or consent management platforms disclose links to the Transparency and Control portal in their login/consent flows, privacy policies, and other means.

### Why do advertisers/data providers not need to integrate with the opt-out feed?

Opt-outs relate to opting out of targeted advertising, which is handled through the publisher and DSP opt-out workflows. If the consumer wishes to disengage with a specific advertiser, they need to contact the advertiser directly. <The T&C Portal will link to an advertiser privacy policy where they can request deletion of their data.>