Unified ID 2.0 Overview

Summary

Addressable advertising enables publishers and developers to provide the content and services consumers have come to enjoy, whether it's through mobile apps, streaming TV, or web experiences. This value exchange has not always been well understood by, or communicated to, consumers. As the industry reduces its reliance on the 3rd party cookie, there's an opportunity to move towards a new, and better, approach to identity for the open internet; an approach where content creators are empowered to have this value exchange conversation with consumers, while giving them more control and transparency over their data.

Unified ID 2.0 (UID2) is a deterministic identifier based on authenticated PII (e.g., email or phone number) with complete user transparency and privacy controls. It is tied to logged-in experiences and publishers and developers can apply it to websites as well as mobile and CTV apps. With several layers of privacy protection, UID2s can be safely distributed across the open internet. The Trade Desk is building the initial code base but, in mid-2021, operational responsibility will be migrated to an independent organization and the relevant code will be open sourced. In addition, UID2 is non-proprietary and accessible to constituents across the advertising ecosystem - including Advertisers, Publishers, DSPs, SSPs, SSOs, CDPs, CMPs, Identity Providers, and Data and Measurement Providers - if they remain in compliance with a code of conduct.

The goal of UID2 is to enable deterministic identity for advertising opportunities on the open internet with full consumer transparency and controls. With an open and interoperable approach, UID2 provides a collaborative framework for all constituents and, ultimately, a healthy open internet.

UID2 Principles

The overarching core principles of UID2:

- **Non-proprietary**: It is not a product or service exclusive to The Trade Desk in any way. All constituents in the advertising ecosystem that abide by a code of conduct can access it with minimal to no fees.
- **Independent Governance**: It will be operated by an unbiased third party, with a transition expected in mid-2021.The Trade Desk is providing the working code and framework only to get it off the ground.
- **Secure and Privacy Safe**: It leverages multiple layers of security, cryptography, and encryption to ensure user PII and data is safe.
- **Transparency and Control**: Consumers can understand where their ID is shared and what data they are associated with and have control to revoke these permissions.
- **Open Sourced**: The related code will be open sourced.
- **Interoperable**: It is accessible to all constituents in the advertising ecosystem - including DSPs, SSPs, data providers, measurement providers, and identity services - who abide by the code of conduct.

The design principles for the UID2 infrastructure:

- **Lightweight**: It is as lightweight as possible and inexpensive to operate.
- **Decentralized**: There is no centralized storage of PII to UID2's mapping (no "honey pot" for bad actors).
- **No Real-time Dependencies**: It has no reliance on external services for real-time processing of RTB data.
- **Accountability**: Accessing UID2 requires participants to abide by a code of conduct and gives the independent governing body the technical ability to remove bad actors.

UID2 Technical Design

The Identifier

UID2

The raw UID2 (unencrypted) is an identifier based on a user's verifiable PII, such as email address. It can only be accessed by members in good standing.

- A UID2 is created (via an API) by hashing and adding a secret salt to the user's PII.
- A raw UID2 is never shared in the bid stream.
- Each UID2 is in a salt bucket and the salt for a bucket rotates 1x every 6-12 months.
- UID2 holders check (via API) to know when a UID2's salt bucket has rotated.
- It is designed to be handled by advertisers, data providers, and DSPs.

UID2 Token

The UID2 Token is the encrypted and transient UID2 for bid stream facing workflows.

- After the UID2 is generated, a cryptographic nonce is generated an appended to the UID2.
- That ID is then encrypted with an encryption key.
- A timestamp (of when the ID was created) is attached as metadata to the payload.
- It is designed to be handled by publishers, SSOs, and SSPs.

With the process defined above, the UID2 Token is constantly changing and is different every time it enters the bid stream. This allows the ecosystem to be secure and prevents non-members from building profiles using UID2 Tokens.

Infrastructure Components

UID Core

The centralized service that manages access to the distributed UID2 ecosystem.

Responsibilities:

- Distributes encryption keys and salt buckets to UID2 operators.
- Distributes decryption keys so only members in good standing are able to decrypt a UID2 Token.
- Distributes user Opt-Outs to both Publishers and DSPs.
- Distributes Deletions to Advertisers, Data Provider, and DSPs.

- Audits members of the trusted ad ecosystem to determine if they are in good standing.

UID Operators

A few select actors that operate the APIs to generate and manage UID2s and UID2 Tokens.

Responsibilities:

- Receives and stores encryption keys and salt buckets from the UID Core service.
- Translates authenticated PII into UID2s (via a salt and hash process).
- Creates UID2 Tokens by encrypting UID2s.
- Provides salt bucket update management data to advertisers, data providers, and DSPs.
- Broadcasts UID2 Token (stored in 1st party cookie) updates to publishers via a refresh token.
- Sends UDI2 user opt-outs to publishers and DSPs.
- Sends UDI2 Deletion Requests to advertisers, data providers, and DSPs.
- Does not store and is not aware of PII to UID2 mappings.

Transparency and Control Service

Consumer facing website and underlying APIs that enable user transparency and control.

Responsibilities:

- Transparency and Control Portal
  - Offers transparency surrounding UID2 access and data segments.
  - Provides global opt-out of UID2.
  - Allows UID2 deletion or Subject Access Request (SAR).
- Privacy Controls APIs
  - Provisions opt-out requests to publishers (via UID Operators) and DSPs (via UID2 Core).
  - Communicates deletion requests and SAR to advertisers, data providers, and DSPs.

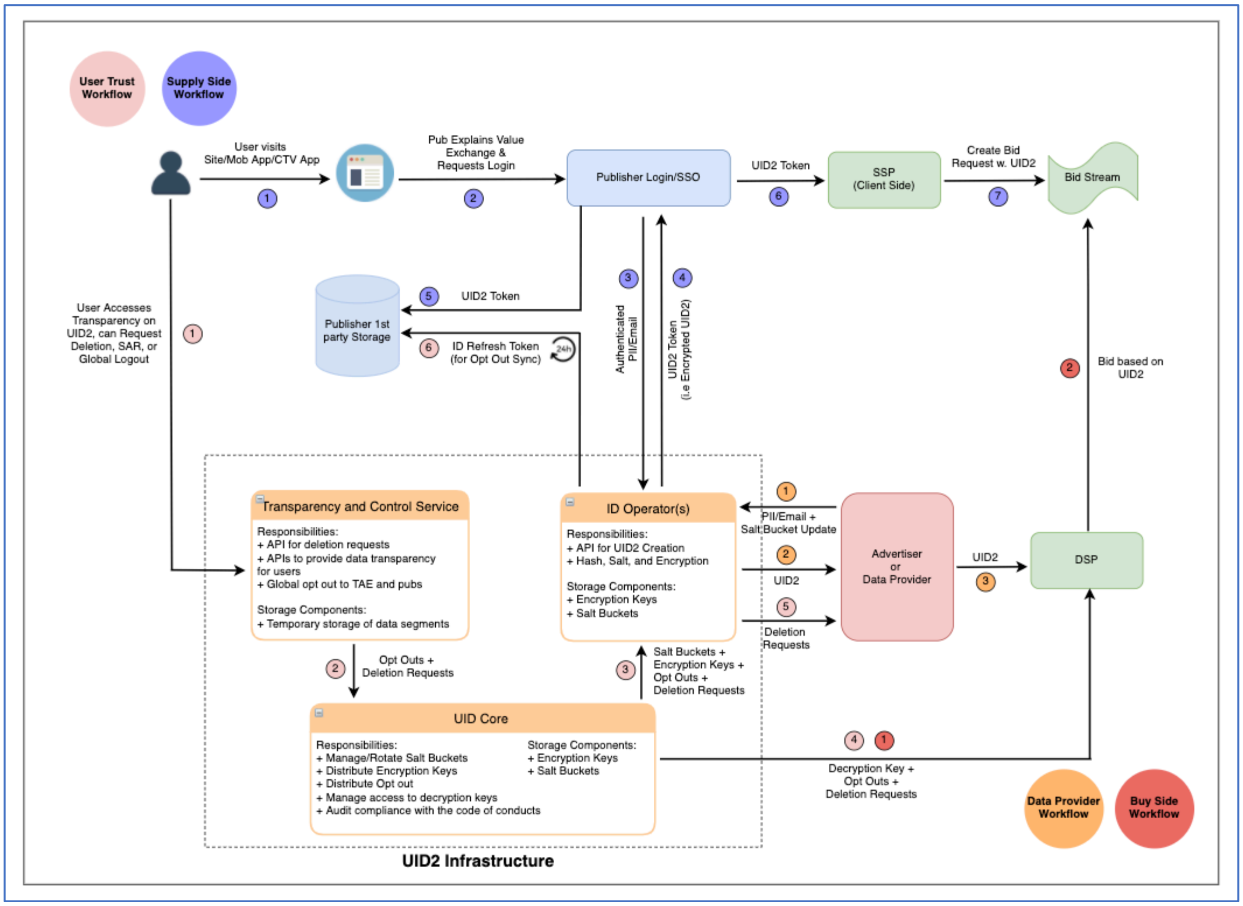
Privacy & Security Details

The UID2 and UID2 Token provide security and safety in the following ways:

- Hash – SHA256
- Secret Salt
  - Additional salt applied with 6 months to 1-year TTL.
  - Input PII is assigned a 'salt bucket' and the salt of each bucket rotates on average of 1x per year.
  - UID2 payload carries metadata with the associated salt bucket.
  - ID Service provides an API that returns all rotated salt buckets since a given timestamp.
- Cryptographic Nonce
  - A nonce is an arbitrary number(s) that can be used just once.
  - It is applied to the UID2 prior to encryption (and creation of the UID2 Token).
  - It ensures that each UID2 Token going into the bid stream is unique and cannot be used by non-members to build user profiles.
- Encryption
  - Uses AES/CBC/PKCS5P adding with 256bit keys.

- Changes on a daily basis.
- All participants have same key, not vendor specific keys.
- The UID2 Token payload has the timestamp of the encryption as metadata.

Workflow


User Trust Workflow
Supply Side Workflow
User visits Site/Mob App/CTV App
1
Pub Explains Value Exchange & Requests Login
2
Publisher Login/SSO
UID2 Token
6
SSP (Client Side)
Create Bid Request w. UID2
7
Bid Stream
User Accesses Transparency on UID2, can Request Deletion, SAR, or Global Logout
1
Publisher 1st party Storage
5
UID2 Token
6
ID Refresh Token (for Opt Out Sync)
24h
3
Authenticated PII/Email
4
UID2 Token (i.e Encrypted UID2)
2
Bid based on UID2
Transparency and Control Service
Responsibilities:
+ API for deletion requests
+ APIs to provide data transparency for users
+ Global opt out to TAE and pubs
Storage Components:
+ Temporary storage of data segments
ID Operator(s)
Responsibilities:
+ API for UID2 Creation
+ Hash, Salt, and Encryption
Storage Components:
+ Encryption Keys
+ Salt Buckets
1
PII/Email + Salt Bucket Update
2
UID2
5
Deletion Requests
Advertiser or Data Provider
UID2
3
DSP
2
Opt Outs + Deletion Requests
3
Salt Buckets + Encryption Keys + Opt Outs + Deletion Requests
UID Core
Responsibilities:
+ Manage/Rotate Salt Buckets
+ Distribute Encryption Keys
+ Distribute Opt out
+ Manage access to decryption keys
+ Audit compliance with the code of conducts
Storage Components:
+ Encryption Keys
+ Salt Buckets
4
1
Decryption Key + Opt Outs + Deletion Requests
Data Provider Workflow
Buy Side Workflow
UID2 Infrastructure

Summary Workflow

There are four simultaneous workflows.

- **Supply Side**: Publishers, Identity Providers, and SSOs generating UID2s and propagating them to the bid stream via SSPs.
- **Buy Side**: DSPs transacting on UID2s in the bid stream.
- **User Trust**: Consumers engaging with publishers, or SSOs and identity providers on their behalf, and consenting to the creation of UID2s as well as engaging with the Transparency and Consent portal on the settings and related data of their UID2s.

- **Data Providers:** Non-bid request data collectors (third-party data providers, advertisers, measurement providers/MTAs, identity graph providers, data on-boarders) that push data to DSPs.

Supply Side Workflow

This workflow applies to publishers, SSOs, CMPs, Identity Providers, and SSPs.

1. A user visits a publisher property such as a website, mobile app, or CTV app.
2. The publisher explains the value exchange of the open internet and requests a login and privacy preferences/consent.
3. The publisher, or SSO or Identity Provider on their behalf, passes the PII and corresponding privacy settings to an ID operator with first party, authenticated PII.
4. An ID Operator does the salt, hash, and encryption process and returns the UID2 Token (encrypted UID2)
5. The publisher stores the UID2 Token:
    - Server side: In a mapping table, DMP, data lake, etc…
    - Client side: In a client-side app or in browser as first party cookie.
6. At impression time, the UID2 Token is passed to the SSP.
7. The SSP passes the UID2 Token into the bid stream.
8. The publisher receives updated IDs via a refresh token. The refresh token will also include the user opt-out where applicable.

Data Provider Workflow

This workflow applies to various data collectors that are not bid request facing, e.g. advertisers, third-party data providers, CDPs, measurement providers/MTAs, identity graph providers, and data on-boarders.

1. The Data Provider sends authenticated and consented PII to the ID Operator.
2. The ID Operator generates and returns a UID2 (unencrypted UID2/raw).
3. The Data Provider sends data to a DSP using transport protocols defined in code of conduct.
4. The Data Provider checks the ID Operator for rotated salt buckets and updates UID2s as needed.

Buy Side Workflow

This workflow applies to DSPs.

1. Data Providers pass first party and third party data to DSPs in the form of UID2s (decrypted).
2. The DSP syncs with UID core to receive its decryption keys if it is in good standing.
3. The DSP accesses UID2 Tokens in the bid stream and decrypts them at bid time.
4. The DSP must listen to opt-outs from UID Core to ensure they do buy on the ID until it has been refreshed on the publisher side (via the Refresh Token mechanism).

User Trust Workflow

This workflow applies to consumers.

1. The user visits the Transparency and Consent Portal where they can:
   - Globally opt-out of their UID2 from all Publishers.
   - See all Data Segments their UID2 is included in (future state).
   - Delete their UID2 from across the ecosystem of participating companies.
   - Enact a SAR across all companies interfacing with the UID2 Infrastructure.
2. The opt-out is sent to UID Core.
3. UID Core distributes the opt-out signal to the ID Operators.
4. UID Core distributes the opt-out signal to DSPs.
5. The ID Operators distribute the deletion request signal to Data Providers.
6. The ID Operators distribute the opt-out signal to Publishers via the refresh token.

FAQs

What are the requirements for companies to access and interact with the UID2 Infrastructure?

The formal code of conduct terms are in development, but they will consist of these themes:

- Honor deletion and opt-out requests.
- Do not share API keys to access the ID Operator APIs.
- Do not share decryption keys.
- Do not share UID2s (raw/unencrypted) with parties that do not have access to the UID2 Infrastructure.
- Follow encryption guidelines for transport and storage.
- Ensure that PII has proper user consent before creating a UID2.

Note that in the current stage where TTD is operating the ID Infrastructure there is a POC Agreement available that captures these points.

Do DSPs need to access the UID2 Infrastructure?

Yes, if they want to be able to receive UID2s from Advertisers and/or Data Providers and/or access UID2s in the bid stream.

Do SSPs need to access the UID2 Infrastructure?

No, SSPs can choose to pass along the encrypted UID2 token. SSPs can choose to access the UID2 Infrastructure if they would like to use UID2 for their own purposes.

Do Advertisers need to access the UID2 Infrastructure?

If advertisers want to directly send authenticated PII (email or phone) to an ID Operator to generate UID2s they must access the UID2 Infrastructure, however, advertisers may choose to work through CDPs, data on-boarders or other service providers instead.

Do Data Providers need to access the UID2 Infrastructure?

Yes, if Data Providers want to incorporate UID2s into their products. In this definition of Data Providers, we are including providers of third party data, cross device data, measurement solutions, data onboarding, CDPs, and DMPs.

Do Publishers need to access the UID2 Infrastructure?
If publishers want to directly send authenticated PII (email or phone) to an ID Operator to generate UID2s they must access the UID2 Infrastructure, however, publishers can also choose to work with an SSO or an independent ID provider that is interoperable with UID2 instead.

What do DSPs need to do to integrate with UID2?
The typical requirements are:

- Enable capability to accept data in the form of UID2s
- Enable capability to bid on data in the form of UID2s
- Enable a daily encryption key sync with the UID2 core
- Expose API for honoring Opt Outs and Deletion requests
- Integrate with the ID Operator APIs to generate UID2s and handle salt bucket rotations (note only for DSPs with access to email or phone)
- Abide other elements of the UID2 Code of Conduct

What do Publishers need to do to integrate with UID2?
The typical requirements are:

- Integrate with ID Operator APIs to generate UID2 Tokens and access Refresh Tokens. Publishers can also use the JS SDK provided by the UID2 service to manage the refresh token.
- Enable passing of UID2 Token to SSPs or other integrations of interest.
- Abide by other elements of the UID2 Code of Conduct.

Publishers can also choose to work with an SSO or an independent ID provider that is interoperable with UID2 and can handle the integration on their behalf.

What do Advertisers need to do to integrate with UID2?
The typical requirements are:

- Expose API for deletion requests.
- Integrate with the ID Operator APIs to generate UID2s and handle salt bucket rotations.
- Abide by other elements of the UID2 Code of Conduct.

Advertisers may also choose to work through CDPs, data onboarders, or other service providers that can handle the integration on their behalf.

What do Data Providers need to do to integrate with UID2?
The typical requirements are:

- Integrate with the ID Operator APIs to generate UID2s and handle salt bucket rotations.
- Expose API for deletion requests.
- Abide by other elements of the UID2 Code of Conduct

How do companies interfacing with UID2 Tokens know which Decryption Key to apply?
Metadata with the UID2 token will disclose the timestamp of the encryption informing which decryption key applies.

How does a holder of a UID2 know when to refresh the UID2 because a salt rotation?
Metadata on a UID2s salt bucket is returned as part of the UID2 generation request. The salt bucket is persistent and assigned to the underlying input PII. There is a separate API that, for a given time stamp, returns which salt

buckets have been rotated since then. This informs the UID2 holder which UIDs to refresh. This workflow typically applies to Data Providers and Advertisers.

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.

Can a user opt-out of UID2?
Yes, the user has complete control of the UID2 tied to their PII. They can opt-out of UID2 and/or request that their UID2 is deleted by all data holders through the Transparency and Control Portal. Note that a publisher or service provider has the option to limit access to their product based on a user's participation in UID2 and this should be communicated by the publisher 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 will disclose links to the Transparency and Consent Portal in their privacy policies, as part of their login/consent flows, and/or through other means.