OVERVIEW AND KEY CONCEPTS

UNIVERSAL IDs

SKELETON KEY

UNIVERSAL IDS (UIDs) ARE **UNIQUE IDENTIFIERS** THAT ALLOW ADVERTISERS AND PUBLISHERS TO **RECOGNIZE USERS** CONSISTENTLY **ACROSS DEVICES** AND **ENVIRONMENTS**.

WHY DO THEY EXIST?

THESE PRIMARY CATALYSTS...

01

INCREASED FOCUS ON USER PRIVACY

Consumers are more in tune with how their data is being used, demanding greater transparency to maintain trust & advocacy

02

DRAMATIC PRIVACY PARADIGM SHIFTS

Leading to greater regulation, incentivising platforms to implement technical changes and reduce data interoperability

03

DECLINE OF TRADITIONAL 3P IDs

Marketers must navigate regulations and shifting consumer expectations in an industry without legacy third party identifiers

…LED TO THESE SECONDARY DRIVERS

01

SHIFT TO 1PD AND USER AUTHENTICATION

With 3P IDs being less viable, brands and publishers had to focus on authenticated 1PD (e.g., email addresses, logins).

02

CROSS-ENVIRONMENT CONNECTIVITY GAPS

3P IDs historically enabled cross-site/app racking, and their removal increased identity fragmentation across the industry.

03

DATA INTEROPERABILITY CHALLENGES

Data interoperability challenges from fragmentation led to demand for privacy compliant cross environment “universal” IDs.

ADVERTISERS AND PUBLISHERS ARE THE **ULTIMATE BENEFICIARIES** OF UIDs.

ADVERTISERS

→ More precise audience targeting

→ Cross-device and cross-platform identity enablement

→ Improved attribution and measurement

PUBLISHERS

→ Higher ad revenue via more addressable inventory

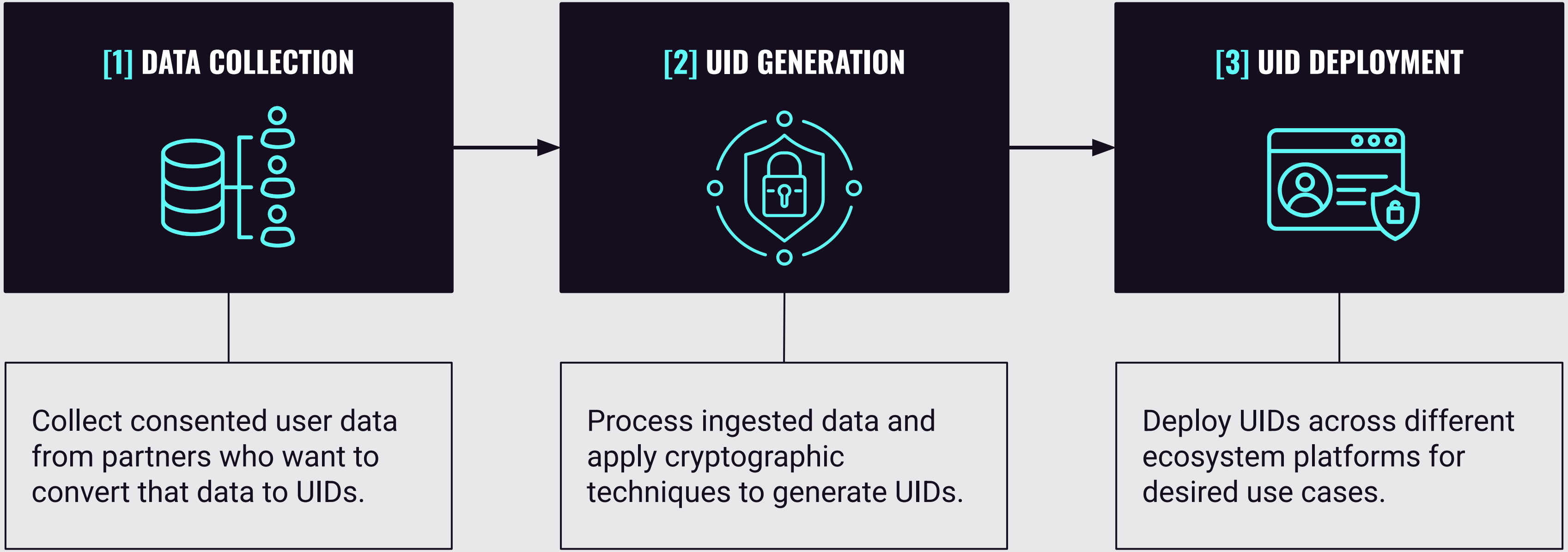
→ Improved 1P data monetization

→ Improved control over identity and audience data

UIDs AS SYSTEMS

IT’S HELPFUL TO THINK OF UIDs AS A “SYSTEM” OF INTEROPERABLE COMPONENTS RATHER THAN JUST STANDALONE IDENTIFIERS.

THIS SYSTEM DOES THREE THINGS (on a high level)



[1] DATA COLLECTION

Collect consented user data from partners who want to convert that data to UIDs.

[2] UID GENERATION

Process ingested data and apply cryptographic techniques to generate UIDs.

[3] UID DEPLOYMENT

Deploy UIDs across different ecosystem platforms for desired use cases.

DATA COLLECTION

DATA TYPES

UID systems rely on specific types of data to build identifiers. These can largely divided into two categories:

DETERMINISTIC (primary)

User-provided data that directly identifies an individual and is persistent across sessions and devices. These are the core inputs for UID systems and form their respective identity “spines”.

Examples

- ➔ Emails
- ➔ Phone numbers
- ➔ Account/Customer IDs
- ➔ Browser cookies
- ➔ Mobile device IDs

PROBABILISTIC (secondary)

Indirect or inferred signals used to identify users based on likelihood rather than certainty. Generally serve to supplement deterministic data to extend the reach of UID systems.

Examples

- ➔ Device characteristics - Browser, OS, screen resolution, etc.
- ➔ Network signals - IP address, network provider, etc.
- ➔ Environmental context - Page URLs, categories, KWs, time of day, etc.
- ➔ Digital behavioral patterns

DATA SOURCES

UID systems collect data from various sources including but not limited to the following:

WEBSITES

- **Data types**
  - Registration or login forms (deterministic)
  - Cookies, JavaScript tags, or SDKs (probabilistic)
- **Example**: News publisher passes UID provider subscriber emails along with browsing information from 1P cookies

MOBILE APPS

- **Data types**
  - App logins or account creation (deterministic)
  - App SDKs for device data (probabilistic)
- **Example:** Streaming app passes UID provider emails captured during registration and device properties from installed SDK

DATA SOURCES

UID systems collect data from various sources including but not limited to the following:

CRM/DATA WAREHOUSE/CDP

➔ **Data types**
  - 1P customer data e.g. emails, phone numbers, purchase data (deterministic)

➔ **Examples:** A retailer uploads its loyalty program data to a UID provider

ADTECH PLATFORMS*

➔ **Data types**
  - Bidstream data e.g. IP address, user agent, device type (probabilistic)
  - 3rd party audience segments (mostly probabilistic)

➔ **Examples:** SSPs share bidstream data with UID provider via API

**Data collected from adtech platforms generally used to enrich existing UIDs or identity graph*

COLLECTION MECHANISMS

CLIENT-SIDE COLLECTION

Description: User IDs are collected via SDKs or JavaScript tags placed on websites/apps.

Use case: Common for publishers collecting 1P data directly from users (e.g., login-based platforms).

REAL-TIME API INGESTION

Description: Data is sent via APIs in real-time, often integrated into publisher, advertiser, or adtech systems

Use case: Ideal for dynamic environments like programmatic advertising or real-time audience activation.

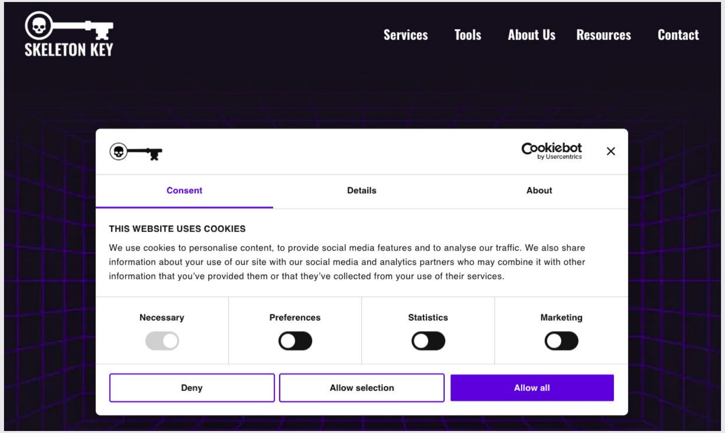
SECURE BATCH UPLOADS

Description: Bulk hashed PII is uploaded via secure channels like SFTP or encrypted cloud storage.

Use case: Used for CRM onboarding or large-scale audience matching.

USER CONSENT VERIFICATION

Consent verification is critical to comply with privacy regulations, build user trust, and enable data legitimacy. If consent is not verified, data collection stops and the user's data is excluded from the UID generation process.



THIS WEBSITE USES COOKIES

We use cookies to personalise content, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media and analytics partners who may combine it with other information that you've provided them or that they've collected from your use of their services.

Consent verification process is managed Consent Management Platforms

Consent Management Platforms (CMPs) = Tools integrated into websites/apps to capture and manage user consent preferences

Industry examples - OneTrust, TrustArc, Quantcast Choice

Example workflow

1. User visits a website and is presented with a consent banner managed by the CMP
2. User selects preferences (e.g. opt-in to personalised ads)
3. The CMP records preferences and stores as a first-party cookie and/or a server-side record linked to a deterministic ID
4. UID provider queries CMP through API to validate consent before proceeding with UID creation

UID GENERATION

UIDs ARE GENERATED USING A COMBINATION OF DETERMINISTIC AND PROBABILISTIC METHODS

DETERMINISTIC

Uses authenticated, PII like email addresses, phone numbers, or login credentials to generate IDs

PROBABILISTIC

Leverages non-PII signals (e.g., device attributes, IP addresses, browsing patterns) to infer user identity statistically

DETERMINISTIC METHODS ARE GENERALLY USED TO CREATE THE PRIMARY UID FOUNDATION WHILE **PROBABILISTIC APPROACHES** PROVIDE SUPPLEMENTAL OR FALLBACK MECHANISMS WHEN AUTHENTICATED DATA IS UNAVAILABLE.

DETERMINISTIC METHODS

Deterministic methods involve preparing the raw data, hashing the prepared data to generate UIDs, and securing the UIDs using encryption. This is to:

1. **ENSURE DATA CONSISTENCY AND ACCURACY**: Standardizing input data for reliable UID creation

2. **PROTECT USER PRIVACY**: Applying techniques like hashing and encryption to pseudonymize data.

3. **ENABLE INTEROPERABILITY**: Transforming data into a format compatible with the UID provider’s infrastructure and downstream systems.

KEY STEPS

NORMALISATION

Clean/Standardise collected data

HASHING

Apply cryptographic algos to pseuduonymize deterministic data

ENCRYPTION

Secure hashed data for sharing/storage

DATA NORMALISATION

This refers to **cleaning** and **standardising** the collected data in preparation for the upcoming cryptographic processes. This is generally performed by the data provider..

CONVERT DATA INTO COMMON FORMAT

- Examples
  - Emails - Convert to lowercase, trim whitespace
  - Phone numbers - Format to include country codes, remove special characters

REMOVE DISCREPANCIES AND DUPLICATES

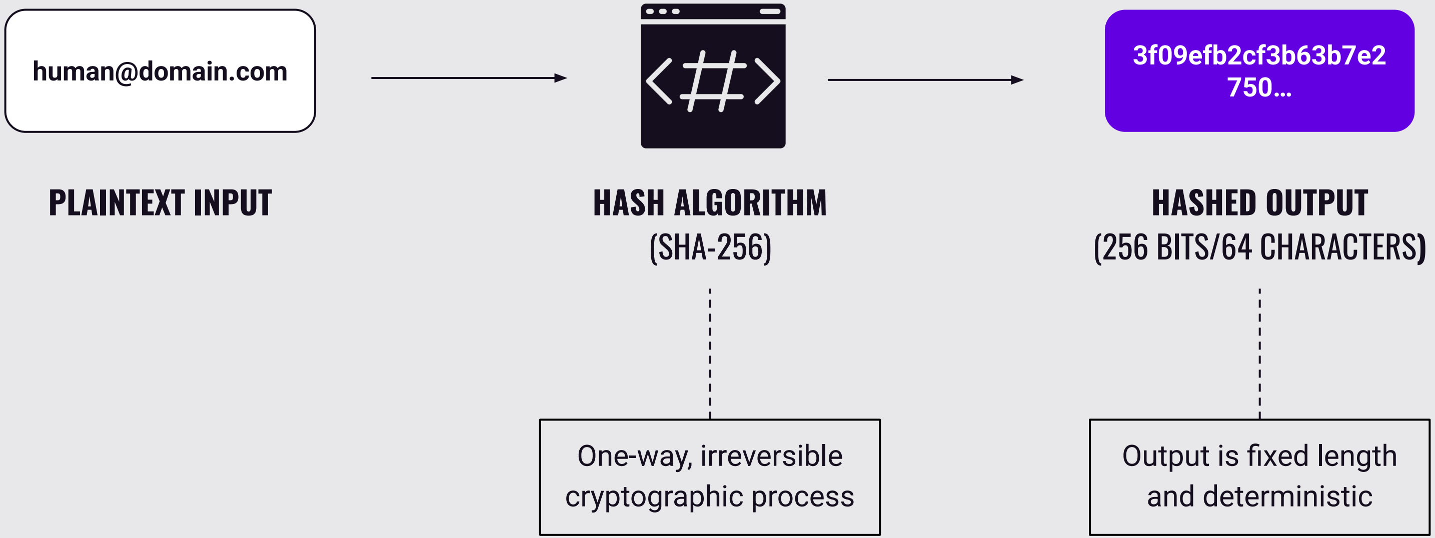
- Examples
  - Remove instances of users submitting personal details multiple times

STANDARDISE DATA POINTS

- Examples
  - Emails - Check for valid syntax (e.g. human@domain.com)
  - Phone numbers - Confirm numbers conform to standards

DATA HASHING

Hashing is a **one-way** cryptographic process that converts raw user data (e.g., an email address) into a **fixed-length, deterministic** pseudonymous string. This can be performed by the data or UID provider depending on the system.



human@domain.com

PLAINTEXT INPUT

HASH ALGORITHM
(SHA-256)

One-way, irreversible cryptographic process

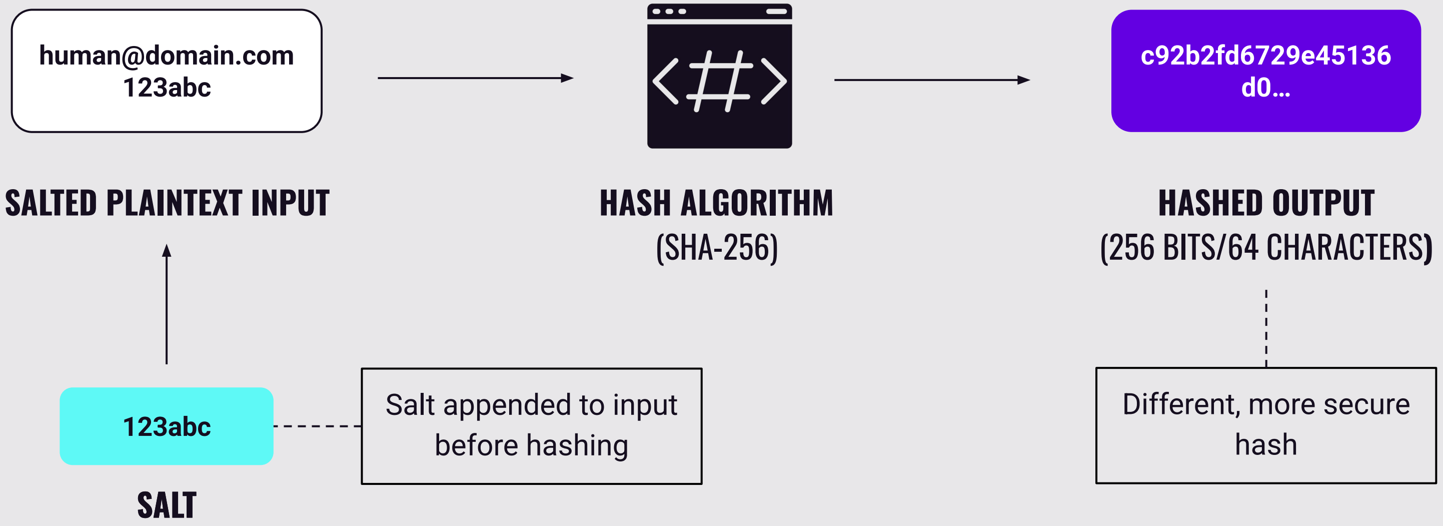
3f09efb2cf3b63b7e2
750...

HASHED OUTPUT
(256 BITS/64 CHARACTERS)

Output is fixed length and deterministic

DATA HASHING WITH SALTING

Salting **enhances the security of hashing** by appending a random or unique value (salt) to the input. This adds randomness to the input, adds complexity to the hash, and prevents identical inputs from producing the same hash.



human@domain.com
123abc

SALTED PLAINTEXT INPUT

HASH ALGORITHM
(SHA-256)

c92b2fd6729e45136
d0...

HASHED OUTPUT
(256 BITS/64 CHARACTERS)

123abc

SALT

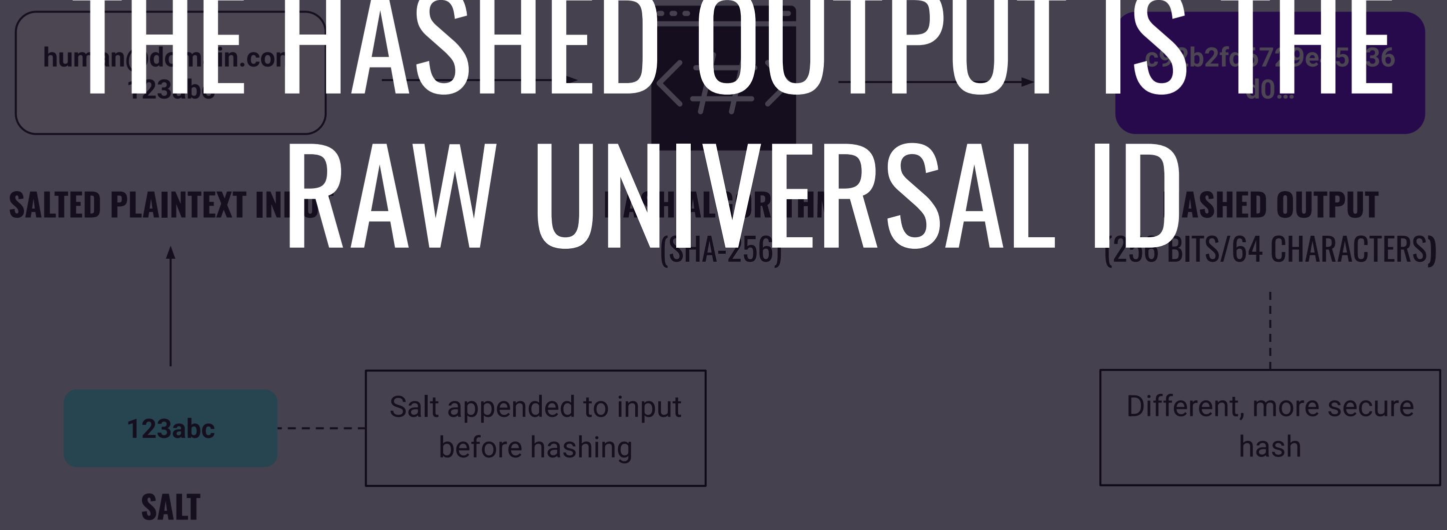
Salt appended to input before hashing

Different, more secure hash

DATA HASHING WITH SALTING

Salting enhances the security of hashing by appending a random or unique value (salt) to the input. This adds randomness to the input, adds complexity to the hash, and prevents identical inputs from producing the same hash.

THE HASHED OUTPUT IS THE RAW UNIVERSAL ID



human@domain.com 123abc

SALTED PLAINTEXT INPUT

HASH ALGORITHM (SHA-256)

c92b2fc6729e45 36 d0...

HASHED OUTPUT (256 BITS/64 CHARACTERS)

123abc

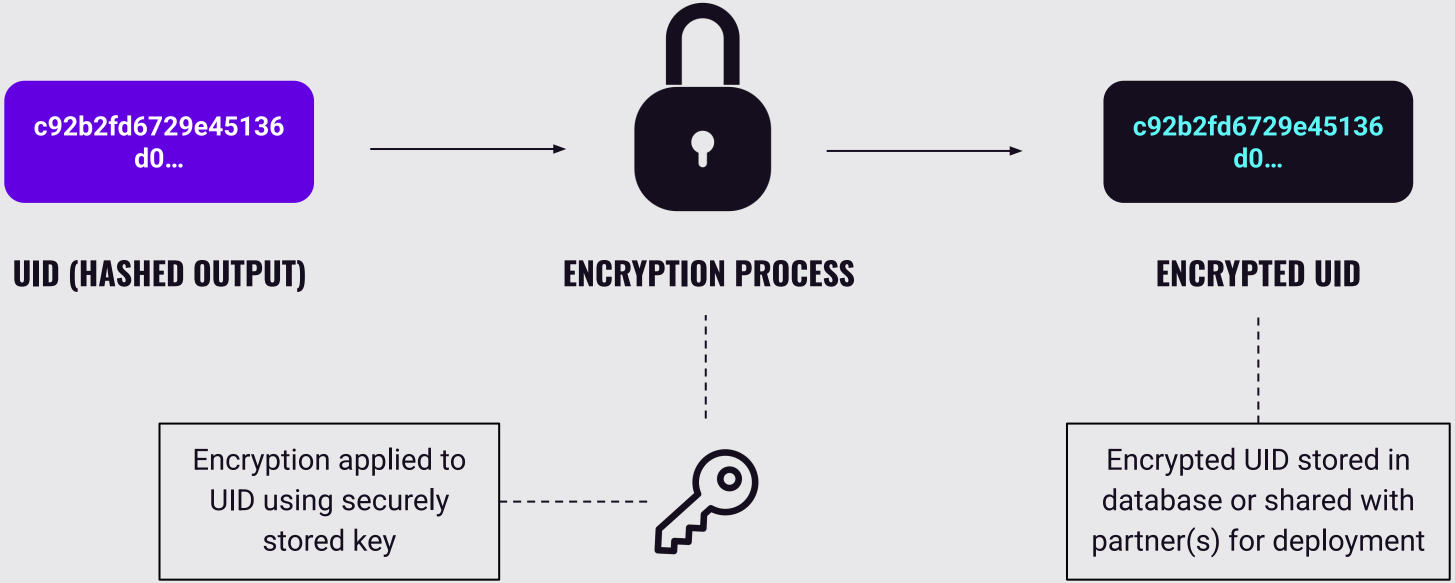
SALT

Salt appended to input before hashing

Different, more secure hash

DATA ENCRYPTION

Encryption is used to secure hashed or salted data during **storage** or **transmission**, ensuring privacy and compliance with data protection regulations. This is typically performed by the UID provider.

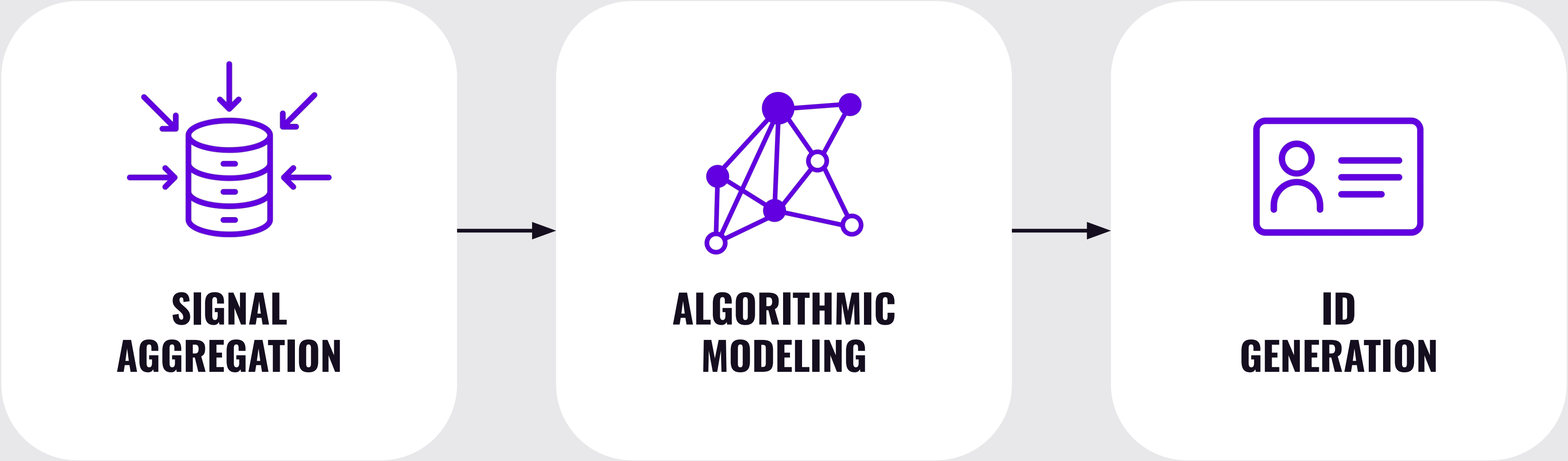


Encryption applied to UID using securely stored key

Encrypted UID stored in database or shared with partner(s) for deployment

PROBABILISTIC METHODS

PROBABILISTIC UID CREATION

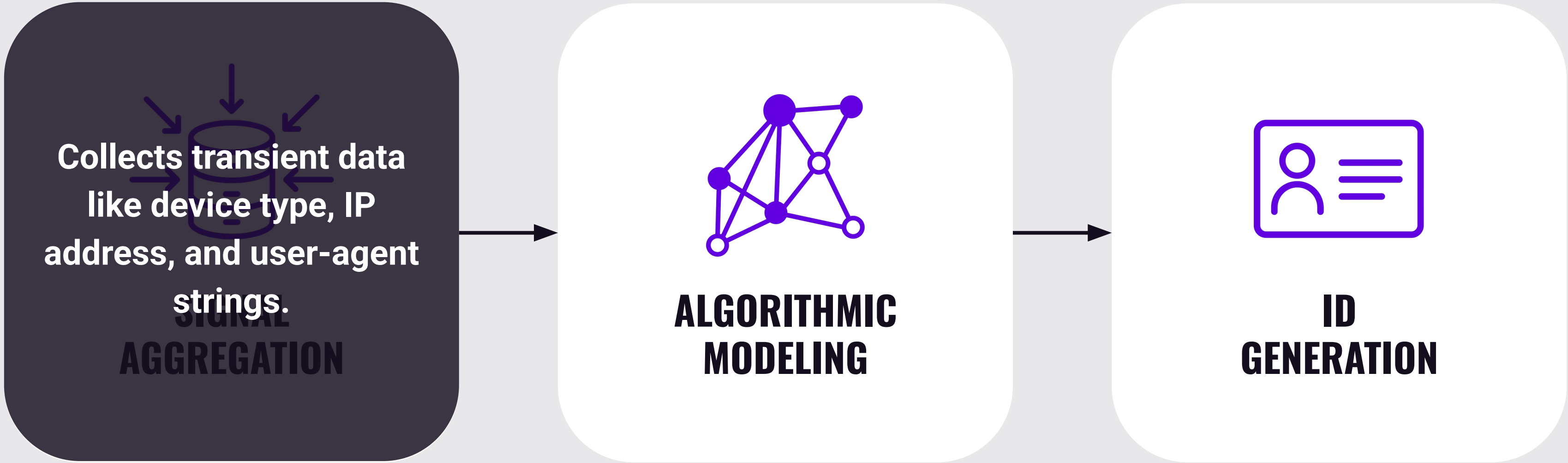


SIGNAL AGGREGATION

ALGORITHMIC MODELING

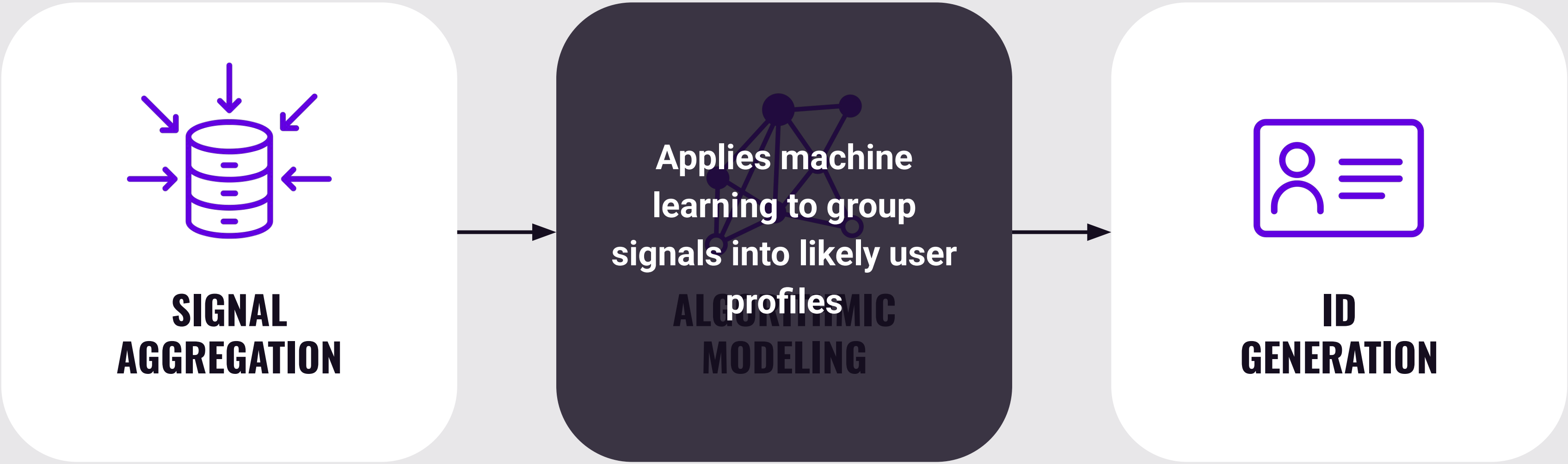
ID GENERATION

PROBABILISTIC UID CREATION



Collects transient data like device type, IP address, and user-agent strings.

PROBABILISTIC UID CREATION



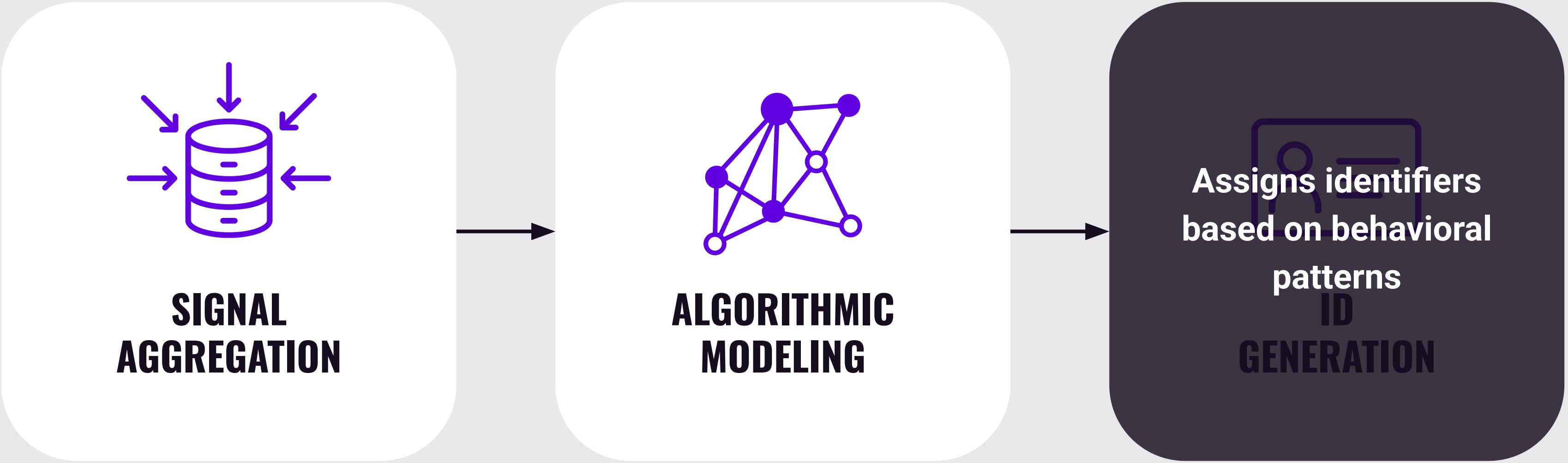
SIGNAL AGGREGATION

ALGORITHMIC MODELING

Applies machine learning to group signals into likely user profiles

ID GENERATION

PROBABILISTIC UID CREATION



SIGNAL AGGREGATION

ALGORITHMIC MODELING

Assigns identifiers based on behavioral patterns

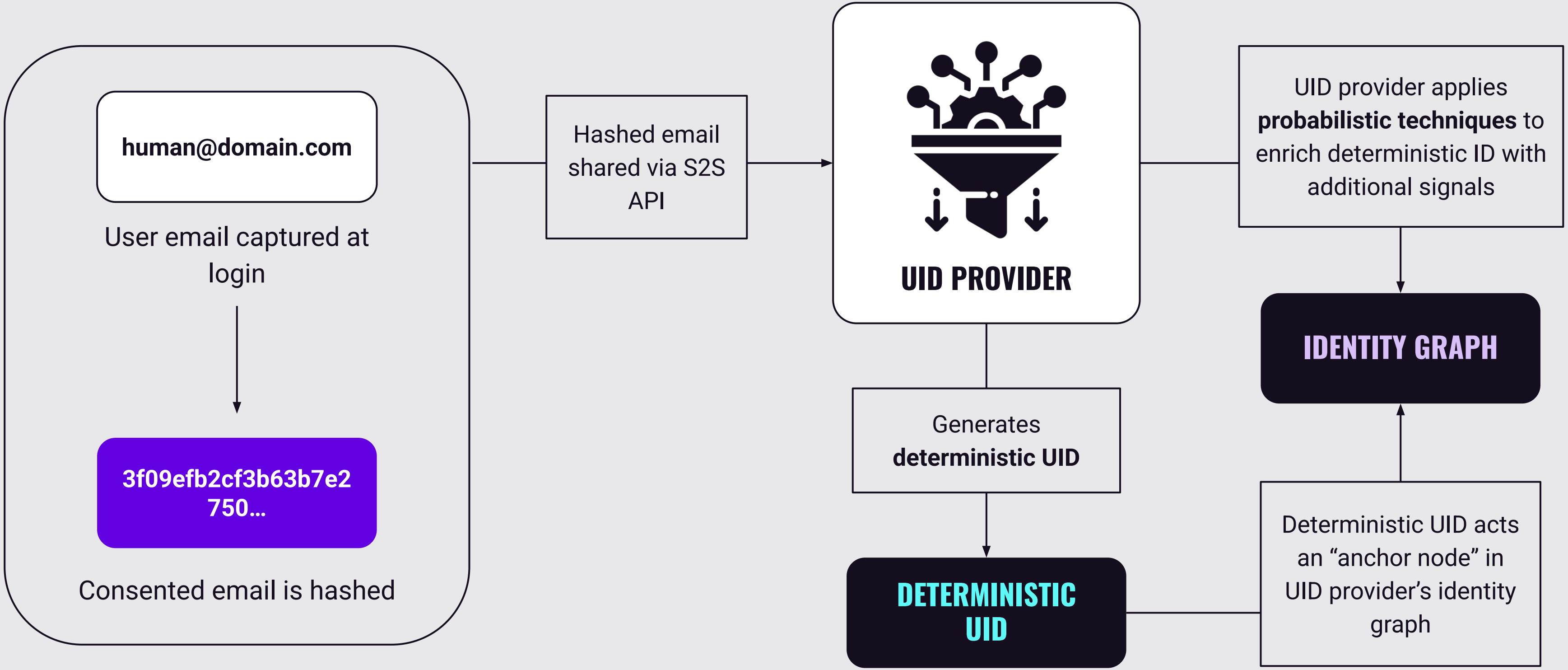
ID GENERATION

PROBABILISTIC METHODS ARE **MOST OFTEN** USED AS A **SUPPLEMENT** OR **FALLBACK** TO DETERMINISTIC IDENTITY RATHER THAN FOR STANDALONE UID CREATION.

ROLE	USE CASE EXAMPLE(S)
SUPPORT To enhance coverage of deterministic methods	**Cross-device linking** - When deterministic UIDs exist, but additional device connections need to be made. **ID graph validation/extension** - When deterministic data is incomplete or fragmented across platforms.
FALLBACK To infer identity when deterministic UID is unavailable	**Bid request ID bridging** - When deterministic IDs are missing on one or both sides of the bidstream **Multi-touch attribution with missing data** - When deterministic tracking is interrupted or incomplete.
AMPLIFICATION To amplify scale beyond directly known users	**Lookalike modeling / Audience expansion** - When an advertiser needs to expand targeting beyond known UID-matched users.

HYBRID WORKFLOW EXAMPLE

HYBRID WORKFLOW



human@domain.com

User email captured at login

3f09efb2cf3b63b7e2750...

Consented email is hashed

Hashed email shared via S2S API

UID PROVIDER

Generates **deterministic UID**

DETERMINISTIC UID

UID provider applies **probabilistic techniques** to enrich deterministic ID with additional signals

IDENTITY GRAPH

Deterministic UID acts an "anchor node" in UID provider's identity graph

UID DEPLOYMENT

UIDs ARE DEPLOYED ACROSS ADTECH AND MARTECH SYSTEMS TO PROVIDE A **PRIVACY COMPLIANT** WAY TO EXECUTE **IDENTITY** AND **AUDIENCE** BASED USE CASES.

SYSTEM TYPE	USE CASES ENABLED (examples)
DEMAND-SIDE PLATFORMS (DSPs)	→ Audience targeting & retargeting → Cross-environment tactics → Lookalike modeling → Frequency capping
SUPPLY-SIDE PLATFORMS (SSPs)	→ Identity-based programmatic enablement → Sell-Side curation (custom deals leveraging UIDs) → Frequency management → Publisher monetization

SYSTEM TYPE	USE CASES ENABLED (examples)
DATA & IDENTITY PLATFORMS	→ Identity resolution → First-party data activation (e.g. via DSPs) → Lookalike modeling → Data enrichment → Data collaboration (ie. data clean rooms)
MEASUREMENT & ANALYTICS (sometimes as part of other systems)	→ Conversion tracking → Multi-touch attribution → Incrementality testing → Cross-channel measurement → Offline-to-online attribution

UIDs CAN BE **ACTIVATED** IN A **VARIETY OF WAYS** DEPENDING ON THE DATA PROVIDER, UID SYSTEM, AND USE CASE. MANY OF THESE **MIRROR** HOW UID PROVIDERS INGEST DATA.

HOW UIDs ARE ACTIVATED

BID STREAM - UID tokens are passed in real-time bid requests via SSPs/DSPs during ad auctions.

- ➔ Process
  - ◆ Publishers include UID tokens in ad requests (e.g., via OpenRTB).
  - ◆ SSPs forward tokens to DSPs in bid requests.
  - ◆ DSPs decrypt tokens to resolve UIDs for targeting/attribution.
- ➔ Use case(s) - Real-time targeting and frequency in programmatic auctions
- ➔ Example - A DSP decrypts a UID token from a bid request to match a user to 1PD for retargeting.

SERVER-TO-SERVER APIs - UIDs are shared directly between systems via APIs

- ➔ Process - UID providers return UID tokens to data providers for deployment.
- ➔ Use case(s)
  - ◆ CRM onboarding (e.g., uploading hashed emails to build audiences).
  - ◆ Closed-loop measurement (linking offline sales to ad exposures).
- ➔ Example - A publisher’s server uses a UID provider’s API to convert hashed emails UIDs to pass in bid requests

HOW UIDs ARE ACTIVATED

BATCH FILE TRANSFERS - Bulk UID datasets are uploaded/downloaded via secure channels (SFTP, cloud).

- Process
  - Advertisers upload hashed PII files to UID providers for batch UID generation.
  - Providers return UID-enriched files for activation in DSPs/CDPs.
- Use cases
  - Offline audience onboarding (e.g., loyalty program emails), historical attribution analysis.
- Example - A retailer uploads a CSV of hashed emails to a DSP for audience activation.

CLEAN ROOM ENRICHMENT- UIDs are resolved in privacy-safe data clean rooms without raw data sharing.

- Process
  - Advertisers/publishers upload hashed data to a clean room.
  - The clean room resolves hashes to UIDs via integration with UID providers.
- Use cases
  - Privacy-compliant data collaboration (e.g., brand-publisher partnerships).
- Example - A CPG brand matches its CRM data to a publisher's UIDs in a data clean room.

IN PRACTICE, UID SYSTEMS UTILISE **MULTIPLE** SHARING METHODS IN MOST WORKFLOWS TO MAXIMISE **COVERAGE**, **USABILITY**, AND **EFFICIENCY** ACROSS ADTECH AND MARTECH SYSTEMS.

CONSENT PROPAGATION

Ensures that user privacy preferences travel with UIDs throughout the adtech/martech ecosystem and associated workflows. This process is crucial for maintaining compliance with regulations like GDPR and CCPA.

INITIAL COLLECTION

Consent collected by CMP and can be stored in:

- 1P cookies
- Server-side databases
- User account settings
- Local storage or SDK frameworks

ENCODING CONSENT

User consent preference is encoded and attached to UID in one of the following ways:

- Embedded inside UID token
- Stored separate and sent alongside UID
- Via API lookups

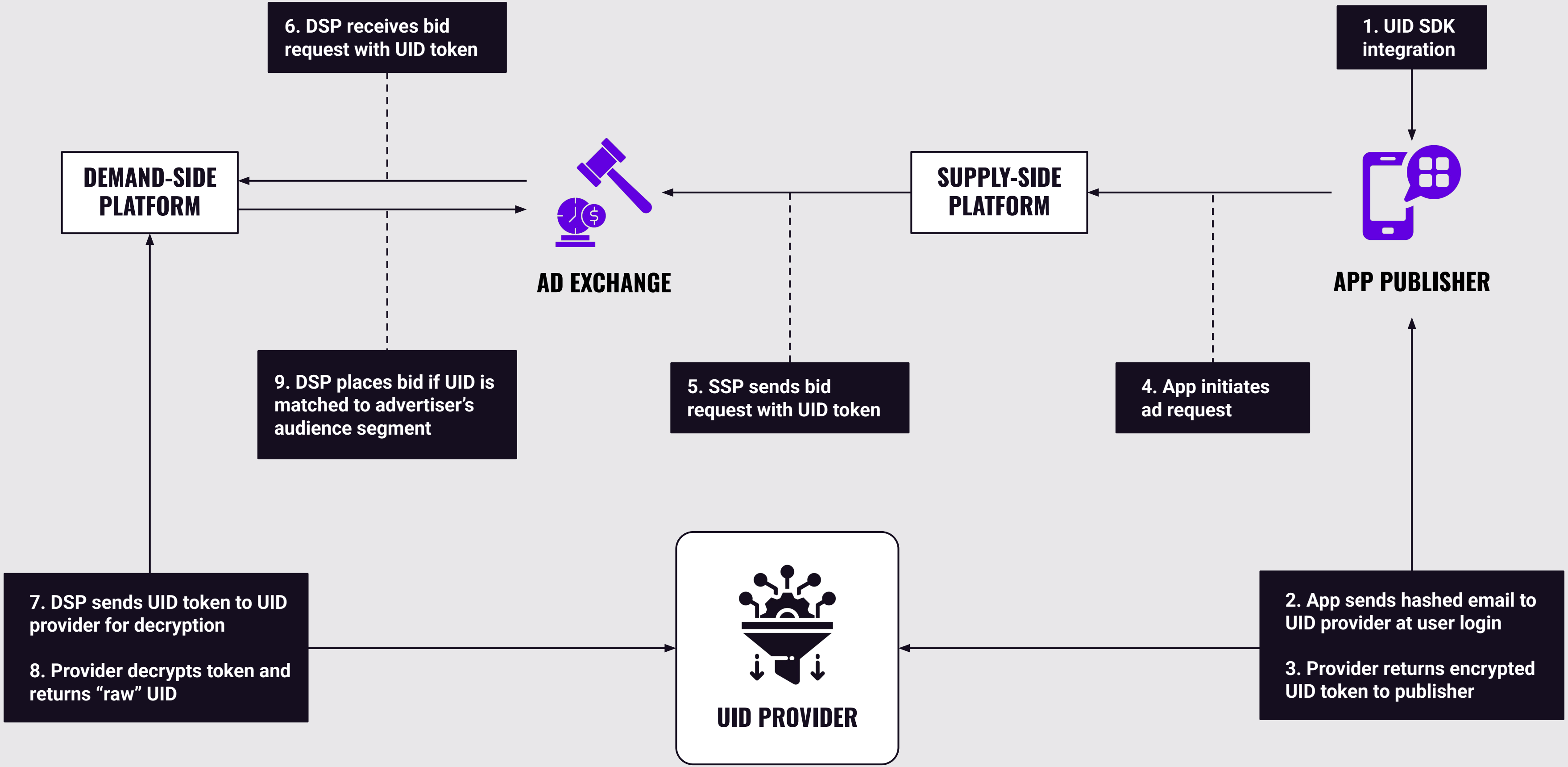
CONSENT PROPAGATION

Created UID + consent metadata can now be sent across ecosystem

- Publisher → SSP
- SSP → DSP
- DSP → Advertisers
- Measurement/Attribution

PUTTING IT ALL TOGETHER

PROGRAMMATIC ADVERTISING



6. DSP receives bid request with UID token

1. UID SDK integration

DEMAND-SIDE PLATFORM

AD EXCHANGE

SUPPLY-SIDE PLATFORM

APP PUBLISHER

9. DSP places bid if UID is matched to advertiser's audience segment

5. SSP sends bid request with UID token

4. App initiates ad request

7. DSP sends UID token to UID provider for decryption

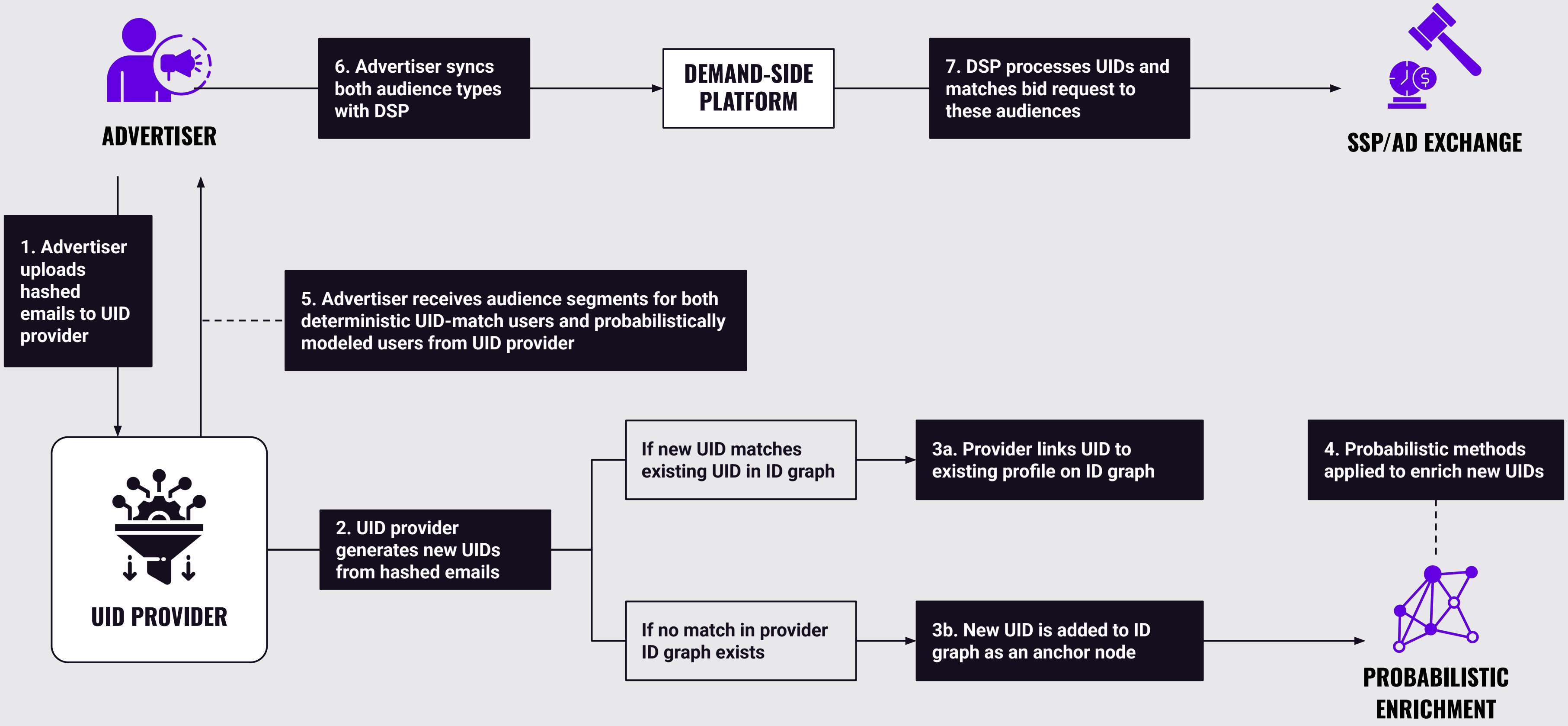
8. Provider decrypts token and returns "raw" UID

UID PROVIDER

2. App sends hashed email to UID provider at user login

3. Provider returns encrypted UID token to publisher

ACTIVATING CRM DATA



ADVERTISER

6. Advertiser syncs both audience types with DSP

DEMAND-SIDE PLATFORM

7. DSP processes UIDs and matches bid request to these audiences

SSP/AD EXCHANGE

1. Advertiser uploads hashed emails to UID provider

5. Advertiser receives audience segments for both deterministic UID-match users and probabilistically modeled users from UID provider

If new UID matches existing UID in ID graph

3a. Provider links UID to existing profile on ID graph

4. Probabilistic methods applied to enrich new UIDs

2. UID provider generates new UIDs from hashed emails

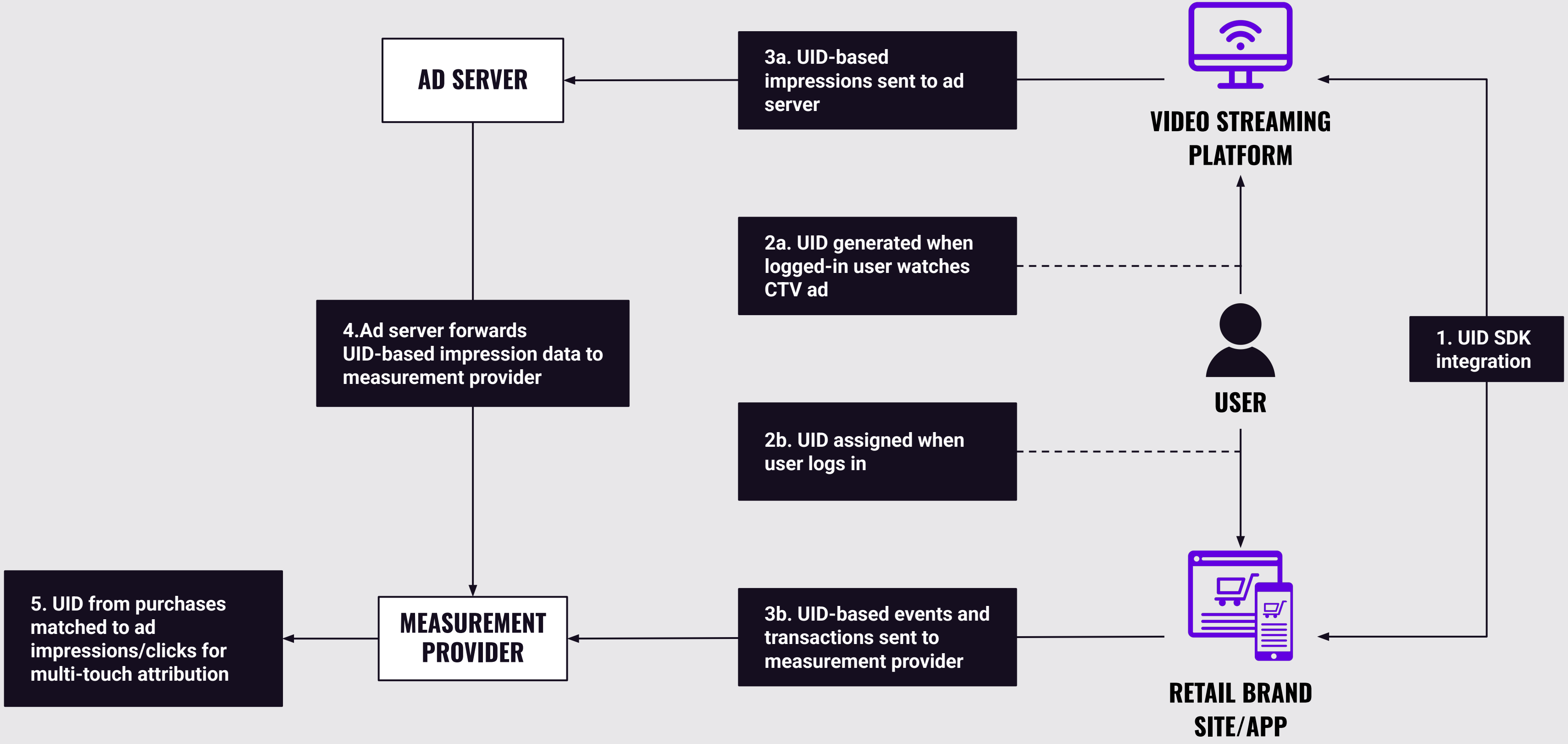
UID PROVIDER

If no match in provider ID graph exists

3b. New UID is added to ID graph as an anchor node

PROBABILISTIC ENRICHMENT

CTV ATTRIBUTION



AD SERVER

3a. UID-based impressions sent to ad server

VIDEO STREAMING PLATFORM

2a. UID generated when logged-in user watches CTV ad

4.Ad server forwards UID-based impression data to measurement provider

USER

1. UID SDK integration

2b. UID assigned when user logs in

5. UID from purchases matched to ad impressions/clicks for multi-touch attribution

MEASUREMENT PROVIDER

3b. UID-based events and transactions sent to measurement provider

RETAIL BRAND SITE/APP

SOME OF THE PRIMARY PROVIDERS

UID SOLUTIONS **DIFFER ACROSS SEVERAL AREAS**, INCLUDING DATA SOURCE, PRIVACY COMPLIANCE STRICTNESS, TECHNICAL APPROACH, AND ADOPTION STRATEGY.

PROVIDER	TYPE	DESCRIPTION	ADOPTION
Unified ID 2.0 (UID2)	Deterministic	Open-source framework using hashed emails for ID resolution.	Widely adopted in NA and growing in APAC; slower uptake in EMEA due to stricter GDPR requirements.
ID5	Hybrid	An independent solution that leans on probabilistic methods, but also incorporates deterministic 1P signals.	Highly adopted among EMEA publishers & expanding globally as a top choice among alternative IDs.
LiveRamp RampID	Hybrid	A people-based ID linking 1P data (e.g. emails) with 3P data.	Strong adoption in the US; expanding in EU and APAC with a robust identity graph for offline-to-online matching.
Lotame Panorama ID	Hybrid	A people-based identifier linking 1P data (e.g. emails) with 3P data.	Global reach across the open web, with usage in multiple ad tech ecosystems.
PreBid Shared ID	Deterministic	A community-driven, open-source solution primarily used in header bidding.	Widely implemented by publishers as a fallback in header bidding setups, across various regions.
Criteo SPUID	Deterministic	Criteo’s shopper UID created from retailer and login data for targeted advertising.	Primarily within the Criteo network, offering global reach within its ecosystem for retargeting.

FOR UP-TO-DATE STATS ON UID DEPLOYMENT ACROSS PUBLISHERS ON THE OPEN WEB, CHECK OUT SINCERA’S FREE DASHBOARDS

PROVIDER	TYPE	DESCRIPTION	ADOPTION
Unified ID 2.0 (UID2)	Deterministic	Open source framework using hashed emails for ID resolution.	Widely adopted in NA and growing in APAC; slower uptake in EMEA due to stricter GDPR requirements.
ID5	Hybrid	An independent ID solution that uses both 1P signals and device/browser data.	Highly adopted among EMEA publishers & expanding globally as a top choice among alternative IDs.
LiveRamp RampID	Hybrid	A people-based ID linking 1P data (e.g. emails) with 3P data.	Strong adoption in the US, expanding in EU and APAC with a robust identity graph for offline-to-online matching.
Lotame Panorama ID	Hybrid	A people-based identifier linking 1P data (e.g. emails) with 3P data.	Global reach across the open web, with usage in multiple ad tech ecosystems.
PreBid Shared ID	Deterministic	A community-driven, open-source solution primarily used in header bidding.	Widely implemented by publishers as a fallback in header bidding setups, across various regions.
Criteo SPUID	Deterministic	Criteo's shopper ID created from retailer and login data for targeted advertising.	Primarily within the Criteo network, offering global reach within its ecosystem for retargeting.

WATCHOUTS AND LIMITATIONS

UIDs CAN BE A POWERFUL SOLUTION TO MAINTAIN AND ENABLE IDENTITY-BASED USE CASE IN A PRIVACY-FIRST LANDSCAPE. HOWEVER, THEY ARE NOT A PERFECT, ONE-SIZE-FITS-ALL SOLUTION AND COME WITH THEIR OWN CAVEATS AND CHALLENGES.

01 FRAGMENTATION & INTEROPERABILITY

Despite the name “universal” ID, there is no single standard as dozens of competing UID solutions exist. This forces publishers and ad platforms to juggle multiple IDs undermining interoperability.

02 SCALE AND ADOPTION CHALLENGES

As UIDs rely heavily on authenticated users, their coverage and scale is limited compared to 3P cookies. In addition, adoption has been mixed across the different UID solutions, particularly in Europe due to GDPR concerns.

03 IMPLEMENTATION COMPLEXITY & COST

The cost and complexity of implementing multiple UIDs (to maximise addressability) create operational burdens for publishers, requiring ongoing technical and compliance efforts. This is especially a challenge for smaller publishers .

04 WALLED GARDENS & COVERAGE GAPS

UIDs are not supported by major walled gardens (e.g. Google, Meta, TikTok). This limits their utility in enabling cross-platform use cases mainly to the open web.

05 DATA LEAKAGE & PRIVACY RISKS

The potential for data leakage with UIDs remain a concern, as widely shared identifiers could allow unauthorized parties to aggregate and misuse user data. Also, lack of transparency with some UID providers create trust issues for customers.

06 FINGERPRINTING CONCERNS

Some UIDs providers supplement deterministic methods with probabilistic fingerprinting techniques to increase match rates. These are heavily regulated under privacy laws and most device/browsers are blocking or limiting their vectors, placing it in an ethically grey area, shaky legal ground, and at risk for shut down by future tech changes.

SO... ARE UIDs ACTUALLY PRIVACY-SAFE AND FUTURE RESILIENT?

UIDs ARE AN IMPROVEMENT OVER 3RD-PARTY COOKIES...

EXPLICIT USER CONSENT

UIDs are generally built on a foundation of authenticated data (e.g. user logins) rather than passive tracking

CRYPTOGRAPHIC TECHNIQUES

UIDs are hashed and encrypted, meaning no raw PII is passed. Most providers apply additional techniques such as salting and ID rotation for further protection.

IMPROVED TRANSPARENCY & CONTROL

UID solutions offer comparatively clear consent flows with centralised opt-out portals and privacy settings.

PRIVACY LAW ALIGNMENT (IN PRINCIPLE)

Generally speaking, UIDs are designed to comply with global privacy laws by requiring explicit consent for advertising use and options for opt-out.

...BUT THEY ARE NOT WITHOUT CHALLENGES

UIDs ARE STILL PERSISTENT IDENTIFIERS

Hashing is a deterministic process, meaning that hashing a given ID always returns the same output. This means that UIDs can still be used to link user activity across websites.

DATA LEAKAGE POTENTIAL

Since UIDs are broadly shared across open web platforms, they can theoretically be combined with other datasets to re-identify users.

REGULATORY UNCERTAINTY

While UIDs are "letter of the law" compliant with privacy laws, some regulators warn that they may recreate 3P cookie tracking under a different name.

FINGERPRINTING RISKS

Some UIDs supplement deterministic matching with probabilistic signals. This creates the potential for fingerprinting, which is prohibited by privacy laws.

THUS, ADVERTISERS AND PUBLISHERS SHOULD NOT VIEW UIDs AS A PANACEA, BUT INSTEAD ONE OF MANY SOLUTIONS IN THEIR TOOLBOX FOR ENABLING IDENTITY-BASED USE CASES IN TODAY’S INDUSTRY LANDSCAPE.

THANK YOU