Standardising Measurement: Attribution Data Matching Protocol

The challenge

Advertisers struggle to accurately measure campaign performance across multiple publishers, ad networks, and platforms without exposing sensitive user data. The fragmented attribution landscape lacks standardised protocols for matching ad exposures to conversions while maintaining privacy, making it difficult to compare campaign effectiveness and optimise media spend. Current solutions often require sharing personally identifiable information or rely on proprietary systems that create data silos.

The solution

ADMaP (Attribution Data Matching Protocol) is a privacy-centric Data Clean Room protocol that enables advertisers and publishers to securely collaborate on attribution reporting without disclosing users' personal information. By establishing standardised methods for matching user conversions with ad engagements through encrypted identifiers, ADMaP allows parties to measure campaign attribution across different environments while maintaining strict privacy controls and preventing direct data exposure between participants.

Value to the industry

For advertisers

- Measure and compare campaign performance across multiple publishers without exposing customer data
- Achieve consistent attribution methodology across all media partners
- Reduce discrepancies and gain transparent, privacy-safe measurement insights
- Ensure and demonstrate compliance with privacy-safe measurement standards

For publishers & platforms

- Demonstrate advertising effectiveness without sharing audience data
- Participate in cross-platform attribution with privacy protection
- Support advertiser measurement needs while maintaining data control
- Ensure and demonstrate compliance with privacy-safe measurement standards

For the industry

- Enable interoperability between different Data Clean Room providers
- Establish privacy-first attribution standards for the evolving ecosystem
- Support regulatory compliance while maintaining measurement capabilities

Key capabilities

Privacy-preserving matching

Privacy Enhancing Technology (PET)
Uses cryptographic techniques like Private Set Intersection (PSI) to match datasets without revealing unmatched user identities to either party

Two-protocol architecture

Separates mapping (creating common identifiers) from attribution (matching conversions to exposures) for enhanced security and flexibility

Flexible attribution methods

Supports multiple attribution methodologies including last-touch, first-and-last, time decay, and custom models based on advertiser needs

Multiple engagement types

Tracks different ad interactions with configurable priorities: clicks, engaged views, standard views, and audio listens

Trusted execution environment

Privacy Enhancing Technology (PET)
Reference implementation using TEE ensures computation occurs in secure, attestable environments that prevent data leakage

Aggregated reporting

Applies thresholding, rounding, and noise to attribution outputs to prevent re-identification while maintaining measurement utility

iab UK

Real world applications

Cross-publisher campaign attribution

An advertiser running campaigns across multiple publishers uses ADMaP to measure which publisher exposures led to conversions, attributing credit appropriately while keeping customer lists encrypted. Each publisher receives performance reports filtered to their inventory only.

Multi-touch attribution analysis

A brand evaluates its omnichannel campaign by matching ad exposures from display, video, and audio channels to purchase conversions using ADMaP's flexible attribution models, enabling data-driven budget optimisation without sharing PII across media partners.

Privacy-compliant CTV measurement

CTV platforms and advertisers implement ADMaP to attribute streaming ad exposures to online conversions in privacy-preserving Data Clean Rooms, supporting measurement in cookie-less and identifier-constrained environments while maintaining regulatory compliance.

Technical overview

Matching methods: Private Set Intersection (PSI) using elliptic-curve cryptography, TEE-based secure computation

Key types supported: Email addresses, phone numbers (E.164), IP addresses, advertising IDs, universal ID providers

Privacy features: Encrypted identifiers, aggregation thresholds, differential privacy noise, secure enclaves

Current version: v1.0 (2024)

Get started with ADMaP

Learn more: iabtechlab.com/admap

Support: support@iabtechlab.com

Documentation: iabtechlab.com/admap

Working group: Rearc Addressability

iab UK