

Market Research zum Advertising-Identity-Ökosystem

Market Research zum Advertising-Identity-Ökosystem

Management Summary	2
Hintergrund	3
Research	3
Ergebnisse	4
Kurzvorstellung der Anbieter	4
ID5 – Universal ID	4
The Trade Desk – Unified ID Solution	4
Roq.ad	4
Digitrust	4
Advertising ID Consortium	4
LiveRamp	4
Mapp	4
NetID	4
Adbrain	4
Flashtalking – Ftrack	5
Zeotap	5
Funktionsweise, Vor- und Nachteile	5
Einführung in die zugrundeliegenden Technologien	5
Summary	9
Die Anbieter im Detail	11
Sicherheit	16
Summary	16
Die Anbieter Im Detail	16
Neutralität	19
Summary	19
Vergleich der Anbieter	19
Qualität	21
Einführung	21
Vergleich der Anbieter	21
Relevanz	24
Die Anbieter im Detail	24
Appendix	26
Erhebungszeitraum	26
Kosten und Abrechnungsmodelle	26
Summary	26
Die Anbieter im Detail	26
Über uns	28
Impressum	29

Management Summary

Regulatorische¹, und technische² Entwicklungen entziehen dem etablierten technischen Fundament (3rd-Party-Cookies) für gezielte Aussteuerung digitaler Werbung die Grundlage.

Die Branche muss sich daher auf einen neuen Standard verständigen, durch den Werbetreibende, Medienunternehmen und ihre Technologiepartner an bestehenden Geschäftsmodellen festhalten und gleichzeitig dem Bedürfnis der Verbraucher nach Datensouveränität nachkommen können. Dabei bleibt die zentrale Frage für alle Marktteilnehmer bestehen: Wie können wir die Adressierbarkeit digitaler Werbung aufrecht erhalten?

Das vorliegende BVDW-Whitepaper zum Advertising-Identity-Ökosystem basiert auf einer von der OVK Unit Programmatic & Data Ende 2019 beauftragten Untersuchung der am weitesten verbreiteten Technologien und Anbietern von Identity-Lösungen.

Da mehrere Browser-Hersteller (Firefox, Safari) 3rd-Party-Cookie/Fingerprinting für das webseiten-übergreifende Tracking von Nutzern künftig nicht mehr unterstützen bzw. eine solche Einschränkung (Chrome) angekündigt haben, lag ein besonderer Schwerpunkt der Studie auf der Beurteilung der Basistechnologien relevanter am Markt verfügbarer Anbieter.

Ziel der Untersuchung war es, ein bis dahin möglichst vollständiges Bild der verschiedenen technologischen Ansätze unter Aspekten wie Funktionsweise, Sicherheit, Zukunftsfähigkeit, Qualität der Adressierbarkeit, Skalierbarkeit und Neutralität der Anbieter zu generieren und damit eine Entscheidungsgrundlage für Nutzer der Technologien bereitzustellen.

Die aktuell hohe Marktdynamik in diesem Bereich lässt erwarten, dass es künftig weitere Ansätze und Anbieter im Markt geben wird. Da der Untersuchungszeitraum des Whitepapers zwischen November 2019 und Februar 2020 liegt, ist es möglich und wahrscheinlich, dass der Leistungsumfang einiger der betrachteten Anbieter sich zügig erweitern wird. Auch im Hinblick auf die im Anhang genannte Preisübersicht sind Veränderungen zu erwarten.

Weitere Entwicklungen und vertiefende Konzepte rund um die Advertising Identity, z.B. zu browser-basierten Targeting-Möglichkeiten („Google Sandbox“) oder der Initiative des IAB - Project Rearc, werden ggfs.in Folgepublikationen vertiefend behandelt sobald hinreichend konkret und in Produkten verfügbar. Auch sind die technischen Details zur Übermittlung der Advertising Identity innerhalb der programmatischen Prozesskette und die Möglichkeiten zur Verknüpfung von Einwilligungsmanagement und persistenter Advertising Identity (Consented Identity) nicht Schwerpunkt der vorliegenden Auswertung.

¹ DSGVO, ePrivacy Richtlinie, EuGH/BGH Urteile, Datenschutzbehörden

² Browser als Gatekeeper: Firefox Enhanced Tracking Protection, Safari Intelligent Tracking Prevention:
<https://www.bvdw.org/themen/publikationen/detail/artikel/warum-advertising-identity-die-zukuenftige-antwort-fuer-zielgerichtete-auslieferung-von-werbung-ist-1/>

Hintergrund

Seit mehreren Jahren bahnt es sich an und es wird dieser Tage konkret: Das 3rd-Party-Cookie als großflächige Basis für eine zielgruppenbasierte Auslieferung digitaler Werbeformen wird sterben. Die Browserhersteller begleiten die rechtlichen Entwicklungen mit technischen Hürden, die immer höher werden. Das Ziel scheint zu sein, das Publisher-übergreifende Tracking von Nutzern über Cookies und ähnliche browserseitige Speicherverfahren letztlich zu verhindern.

Ein besonderes Augenmerk gilt bei dieser Entwicklung den für die Vermarktung eingesetzten Technologien: den diversen für die Auslieferung eingesetzten Adservern, den damit verbundenen Targeting-Systemen und den programmatischen Systemen.

Auch schon mit Cookies galt es, eine Möglichkeit der pseudonymisierten Wiedererkennung über die Barrieren Publisher, Browser und Gerät hinweg zu finden. Die bisher gängige, weil weithin akzeptierte 3rd-Party-Cookie-Variante war nie ausgereift. Mit dem kommenden Wegfall eröffnet sich neben vielen Unbekannten die Chance einer weitergreifenden Lösung, die mehr Barrieren überspringen kann. Offen bleibt, wie sich die Zielgruppen-Reichweiten und TKPs in und nach der Phase des Übergangs entwickeln werden.

Research

Im Rahmen dieses Dokuments wurden relevante und ausgereifte Anbieter von Identity-Lösungen analysiert. Hierbei wurden mit den Anbietern Gespräche geführt.

Ziel ist es, einen Überblick über das Universum dieser Anbieter zu schaffen. Was zeichnet sie aus, wo spielen sie zusammen und wie können die Lösungen am besten für die Zwecke der BVDW-Mitglieder genutzt werden? Darüber hinaus gilt es auch tiefer einzutauchen. Welche technischen Lösungen wurden für die Produkte genutzt und welchen technischen Zwängen der aktuellen Entwicklungen sind diese geschuldet?

Die Ergebnisse wurden in die großen Themenblöcke aufgeteilt, in die dieses Dokument gegliedert ist:

- Wer sind die Anbieter der Lösungen?
- Wie funktionieren die Lösungen?
- Wie steht es um die Sicherheit?
- Wie ist die Qualität einzuschätzen?
- Welche Skalierung wurde erreicht und wie entwickelt sie sich?
- Wie ist die Lösung am Markt positioniert?
- Welche Kosten sind mit der Nutzung für die Marktteilnehmer verbunden?

Ergebnisse

Kurzvorstellung der Anbieter

ID5 – Universal ID

ID5 ist ein vor über zwei Jahren gegründetes Start-up. Angetreten mit der Mission, das ineffiziente Cookie Syncing zu optimieren. Mittlerweile versucht ID5 das Problem der Advertising Identity zu lösen. Hierzu wird am Produkt „Universal ID“ gearbeitet.

The Trade Desk – Unified ID Solution

Als eine der größten DSPs bietet The Trade Desk mehrere Lösungen im Bereich der Advertising Identity an. Unter anderem die Unified ID Solution, eine Cookie-basierte Identity-Lösung auf Basis der eigenen Advertising-Infrastruktur. The Trade Desk hat sich entschieden, nicht an diesem Research teilzunehmen.

Roq.ad

Roq.ad wurde 2015 in Deutschland mit der Mission gegründet, das geräteunabhängige targetieren von Personen und Zielgruppen im digitalen Marketing zu ermöglichen.

Digitrust

Digitrust wurde als Non-Profit-Organisation gegründet, welche sich die Optimierung des Cookie Syncing als Aufgabe gestellt hat. Später wurde die Firma inklusive der Lösung und Infrastruktur vom IAB Techlab übernommen. Die strategische Ausrichtung sowie die konkrete Roadmap wurden dabei in die Hände der Mitglieder der Digitrust Commit Group innerhalb des IAB Techlab gelegt. Mitglieder dieser Gruppe sind immer auch Nutzer von Digitrust.

Advertising ID Consortium

Das Advertising ID Consortium wurde 2017 mit dem Ziel gegründet, Teilnehmer des programmatischen Werbegeschäfts im Rahmen der Advertising Identity dabei zu unterstützen, die Anzahl der Cookie Syncs zu minimieren. Die Mitglieder des Consortiums kommen sowohl von der Demand als auch von der Supply Side. Seit 2018 können auch Vermarkter und Publisher Mitglied werden.

LiveRamp

Gestartet 2011 mit der Mission, die Reichweitenverluste durch ineffizientes Cookie Syncing zu minimieren, hat LiveRamp eine deterministische, People- und Graph-basierte Lösung implementiert. Eigenen Angaben zufolge hat das Unternehmen nach Facebook und Google den drittgrößten Graphen aufgebaut.

Mapp

Vor 15 Jahren als Start-up gegründet, gehört Webtrekk seit Mitte 2019 zu Mapp, einem Marketing-Cloud-Anbieter. Mapp ist im Bereich der Website Analytics positioniert und hier mit einer breiten Kundenbasis nicht mehr wegzudenken.

NetID

Der Single-Sign-on-Anbieter European netID Foundation wurde im März 2018 gegründet. Er wurde in Form einer Stiftung ins Leben gerufen. Ziel der Stiftung ist es, eine unabhängige Alternative zu den SSO-Angeboten von Google und Facebook zu bieten.

Adbrain

Adbrains Mission ist es, eine Adressierung und Messbarkeit von Individuen und Haushalten im digitalen Marketing zu ermöglichen. 2017 wurde Adbrain von The Trade Desk übernommen. The Trade Desk hat sich entschieden, mit Adbrain nicht an diesem Research teilzunehmen.

Flashtalking – FTrack

Flashtalkings Mission ist es, eine vom Mediageschäft unabhängige Ad-serving- und Ad-Analytics-Plattform für Werbetreibende anzubieten. Mit FTrack hat Flashtalking eine Cookie-unabhängige ID, auf deren Basis Flashtalking die Auslieferung der Werbung für Advertiser misst.

Zeotap

Ende 2014 gegründet und ursprünglich mit Datenpartnern aus der Telekommunikationsbranche gestartet, kann Zeotap heute auch auf Daten von E-Commerce- und App-SDK-Anbietern zurückgreifen. Die Customer Intelligence Plattform stellt eine agnostische ID für das Martech Ecosystem und die Publisherseite zur Verfügung. Diese Lösung ist eine Erweiterung der bereits für das CRM Onboarding genutzten Zeotap-Identity-Lösung.

Funktionsweise, Vor- und Nachteile

Einführung in die zugrundeliegenden Technologien

Die in diesem Dokument betrachteten Lösungen basieren alle auf einer der aktuell verfügbaren technischen Möglichkeiten oder auf einer Kombination dieser. Im Folgenden eine funktionale Erklärung:

Cookies

Ein Cookie speichert eine Kombination aus einem Key und einem Value. Der Value kann dabei eine beliebige Information sein, verschlüsselt oder im Klartext. Häufig ist es eine pseudonymisierte ID zur Wiedererkennung. Wird ein Cookie geschrieben, wird immer auch die Domain, unter der er geschrieben wurde, mit in den Cookie aufgenommen. Man unterscheidet bei Cookies, wie und in welchem Kontext sie geschrieben/gelesen werden:

Wie: **Serverseitig**, Kontext: **1st Party**

Beim Aufbau der Seite www.PublisherA.com gehen diverse Anfragen vom Browser an den Server. Der Server beantwortet diese mit der HTML-Seite und z. B. Bildern und CSS-Dateien. In jeder dieser Antworten kann der Server dem Browser eine Anweisung zum Schreiben eines Cookies geben. Solange der Server das unter www.PublisherA.com macht, spricht man von einem 1st-Party-Cookie, welches serverseitig geschrieben wurde.

Wie: **Serverseitig**, Kontext: **3rd Party**

Zusätzlich zu den Bestandteilen, die beim Aufruf von www.PublisherA.com von diesem Server geladen werden, sind auch Drittsysteme wie z. B. die SSP www.SSP.com eingebunden. Hierzu sind in der HTML-Seite von www.PublisherA.com Bestandteile enthalten, die auf dem Server unter www.SSP.com erreichbar sind. Der Browser ruft diese Bestandteile ab. Beantwortet www.SSP.com eine dieser Anfragen mit der Anweisung, ein Cookie zu schreiben, spricht man von einem serverseitigen Cookie, welches im 3rd-Party-Kontext geschrieben wird. 3rd Party, da der User www.PublisherA.com aufgerufen hat und www.SSP.com aus Usersicht eine Drittpartei ist.

Wie: **Clientseitig**, Kontext: **Nur 1st Party**

In JavaScript gibt es die Möglichkeit, Cookies zu schreiben. www.PublisherA.com hat ein JavaScript-Skript auf seiner Seite integriert, welches von diesem Server kommt. Zudem hat www.PublisherA.com ein Skript von www.SSP.com integriert. Beide Skripte

sind in der Lage, Cookies zu lesen und zu schreiben. Alle diese Cookies sind 1st-Party-Cookies. Das Cookie, welches vom Skript von www.SSP.com geschrieben wurde, kann also von SSP nicht auf www.PublisherB.com gelesen werden. Alle Cookies bleiben bei PublisherA.

In Firefox ist der Zugriff auf Cookies im 3rd-Party-Kontext für Tracker, die auf der disconnect.me-Liste gelistet werden, blockiert.

Safari blockiert den Zugriff auf Cookies im 3rd-Party-Kontext für Tracker. Tracker werden durch eine AI anhand bestimmter Muster erkannt.

Chrome/Chromium wird im Rahmen der Umstellung auf die Privacy Sandbox den Zugriff auf Cookies im 3rd-Party-Kontext ebenfalls beschränken.

eTag

eTag steht für „Entity Tag“. Es handelt sich dabei um ein Datenfeld, welches in Webressourcen wie HTML-Seiten, Skripten oder Bildern im Cache des Browsers gespeichert werden kann. Ähnlich einem serverseitigen Cookie steuert der Server über eine Anweisung in der Antwort das Befüllen des eTag im Cache. Das eTag wird für die Cache-Validierung genutzt. Anhand des eTag, das der Server zuvor gesetzt hat, kann er die Version der schon im Cache vorhandenen Ressource erkennen. Er entscheidet, ob er eine neuere HTML-Seite oder ein neueres Bild an den Browser senden muss. Wenn nein, kann er die Bandbreite schonen und die Meldung „not modified“ senden.

Das (unsichtbare) Bild www.SSP.com/tracker/1x1.gif ist auf www.PublisherA.com eingebunden. Über diesen Weg kann die SSP eine pseudonyme ID „ABCDEF“ in den eTag und damit in den Cache eines Browsers legen. Mit diesem Browser wird www.PublisherB.com aufgerufen, auf dem ebenfalls www.SSP.com/tracker/1x1.gif eingebunden ist. Hierbei wird der Wert des eTag aus dem Cache „ABCDEF“ in der Anfrage des Browsers an den Server gesendet. Der Server ist mittels dieses Datenfeldes in der Lage zu bestimmen, dass es sich um denselben Browser handelt. Das Verfahren ähnelt in der Funktion der eines 3rd-Party-Cookies. Da hier ein Bild als Speicherort des eTag genutzt wird, wird dieses Verfahren auch als Image Cache bezeichnet.

Eine Demonstration findet sich hier: <https://lucb1e.com/rp/cookielesscookies/>

Authentication Cache

Das HTTP-Protokoll bietet eine sogenannte Basic Authentication an. Dabei sendet der Browser auf Nachfrage des Servers eine Username-Passwort-Kombination zur Authentifizierung an den Server. Für den ersten Aufruf einer so geschützten Ressource (z. B. Pixel auf dem Server) fragt der Browser den User mittels eines Dialogs. Für alle weiteren Aufrufe wird die Username-Passwort-Kombination aus dem Cache genutzt. Mittels einer Kombination aus serverseitiger Implementierung und JavaScript kann der Dialog für den User unterdrückt und als Username-Passwort-Kombination eine eindeutige ID genutzt werden. Diese kann dann im weiteren Verlauf wie eine Cookie-basierte ID genutzt werden. Diese Methode kann auch in einem 3rd-Party-Kontext und damit über Publisher hinweg genutzt werden.

Diese Methode ist davon abhängig, wie lange die Zugangsdaten im Cache des Browsers vorgehalten werden.

mobile iOS IDFA / Android GAID

Mobile Geräte auf Basis von iOS oder Android bieten sogenannte Advertising Identifier. Die Advertising Identifier werden vom Betriebssystem bereitgestellt. Der User des Geräts kann den Identifier abschalten oder zurücksetzen, um bisher gesammelte Daten unbrauchbar zu machen.

App-Entwickler können die Identifier im App-Code abfragen und den geltenden iOS- und Android-Richtlinien folgend zum Tracking nutzen.

Die Identifier sind gerätespezifisch. Das bedeutet, dass alle Werbenetzwerke in allen Apps, die auf demselben Gerät laufen, dieselbe ID erhalten.

In mobilen Browsern sind die Advertising IDs nicht nutzbar.

Local Storage

Seit der Unterstützung von HTML5 durch die relevanten Browser gibt es die Möglichkeit, in einem sogenannten Local Storage Daten im Browser abzulegen. Geschieht dies im 3rd-Party-Kontext, wird es analog zu Cookies für Publisher-übergreifendes Tracking nutzbar.

In Firefox wird Local-Storage-Zugriff für Tracker, die auf der disconnect.me-Liste gelistet werden, generell blockiert.

Safari hat die Lebenszeit von Local-Storage-Daten im Kontext von Tracking-Methoden stark eingeschränkt.

Chrome/Chromium wird im Rahmen der Umstellung auf die Privacy Sandbox den Zugriff auf Local Storage ebenfalls einschränken.

Fingerprinting

Für das Fingerprinting werden Merkmale im System des Nutzers gesammelt und kombiniert. Ziel ist es, eine handhabbare, aber hohe Zahl von Attributen zu sammeln. Sind die Attribute auf unterschiedlichen Systemen ausreichend variantenreich, ergibt sich ein Fingerabdruck des Systems.

Konkret werden für das Fingerprinting im Kontext des Trackings per JavaScript Merkmale wie

- Browser und Version
- Installierte Plugins
- Bildschirmauflösung
- Betriebssystem und Version
- Installierte Schriften

genutzt.

Die Genauigkeit, mit der ein und derselbe Browser sicher wiedererkannt werden kann, hängt dabei davon ab, wie viele Browser die gleiche Kombination dieser Attribute aufweisen.

Abgebildet auf eine Kampagne kann dies bedeuten:

- Der Frequency Cap der Kampagne ist auf „4 Einblendungen pro User pro Tag“ eingestellt.
- Zwei Browser, genutzt von zwei völlig unterschiedlichen Usern, haben dieselben Attribute.
- Bei korrekter Identifizierung könnten die zwei User 8 Ad Impressions erzeugen.
- Beide erzeugen in der Kampagne an einem Tag aber maximal 4 Ad Impressions, da sie als ein Gerät erkannt werden.

Mozilla plant für Firefox eine Einschränkung der Attribute, die für das Fingerprinting genutzt werden können.

Für Chrome/Chromium wurden im Rahmen der Privacy Sandbox Änderungen angekündigt, die das Fingerprinting beschränken werden, ohne dabei bisher spezifisch zu werden.

Apple hat für Safari bisher keine konkreten Pläne angekündigt, es ist aber davon auszugehen, dass auch hier weitere Entwicklungen folgen werden.

Login

Für eine Wiedererkennung ist ein Login eine hochgradig sichere Methode. Ein Login wird als deterministisch angesehen.

Beim Login wird eine direkte Interaktion des Nutzers mit dem für den Login genutzten System initiiert. Eine Einwilligung des Nutzers vorausgesetzt, kann der Login pseudonymisiert als ID genutzt werden, um den Nutzer in angeschlossenen Drittsystemen wiedererkennen zu können. Beispiele für Login-basierte Webangebote sind Browser-basierte E-Mail-Dienste und soziale Netzwerke. Diese Dienste nutzen den Login direkt auf ihren Angeboten und können ihn unter den entsprechenden rechtlichen Voraussetzungen auch für die Vermarktung durch ihre Partner nutzen.

Eine weitere Form des Logins ist der Single Sign-on (SSO). Hierbei wird der Login vom Anbieter auf weitere teilnehmende Websites weitergetragen. Aus der Nutzerperspektive muss nur noch ein Login angelegt werden. Mit diesem kann sich der Nutzer dann problemlos auf allen Angeboten einloggen, die den SSO unterstützen. Aus Anbieterperspektive skaliert eine solche Lösung besser, da die Hürde des Anlegens eines Accounts durch wenige bestätigende Klicks beim erstmaligen Login über den SSO ersetzt werden.

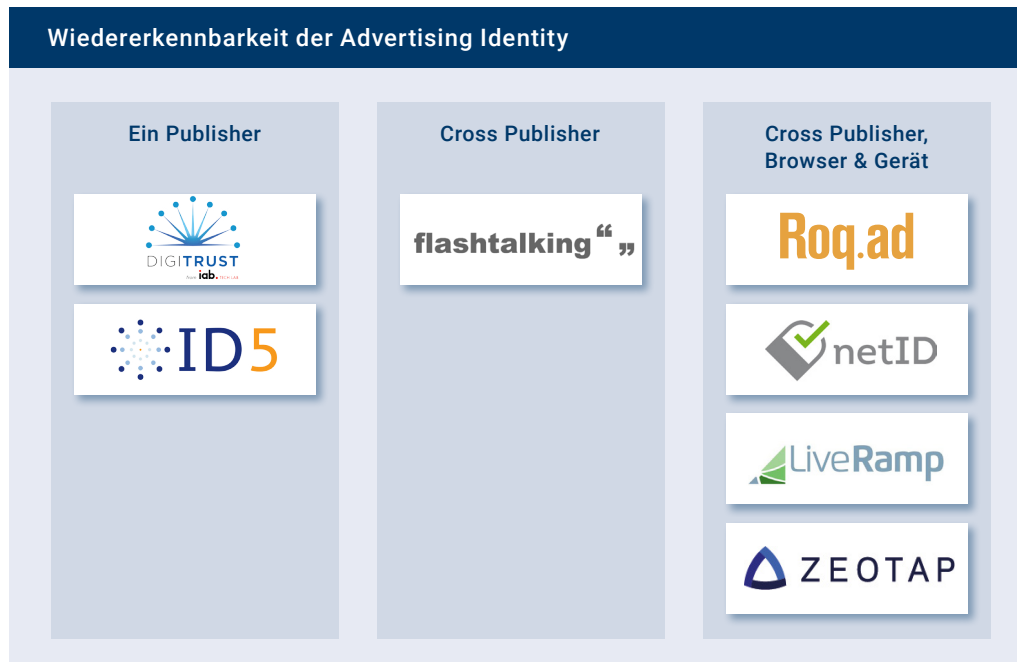
Beispiele von SSO-Anbietern sind Facebook und Google sowie der deutsche Anbieter NetID, der in diesem Dokument behandelt wird.

Summary

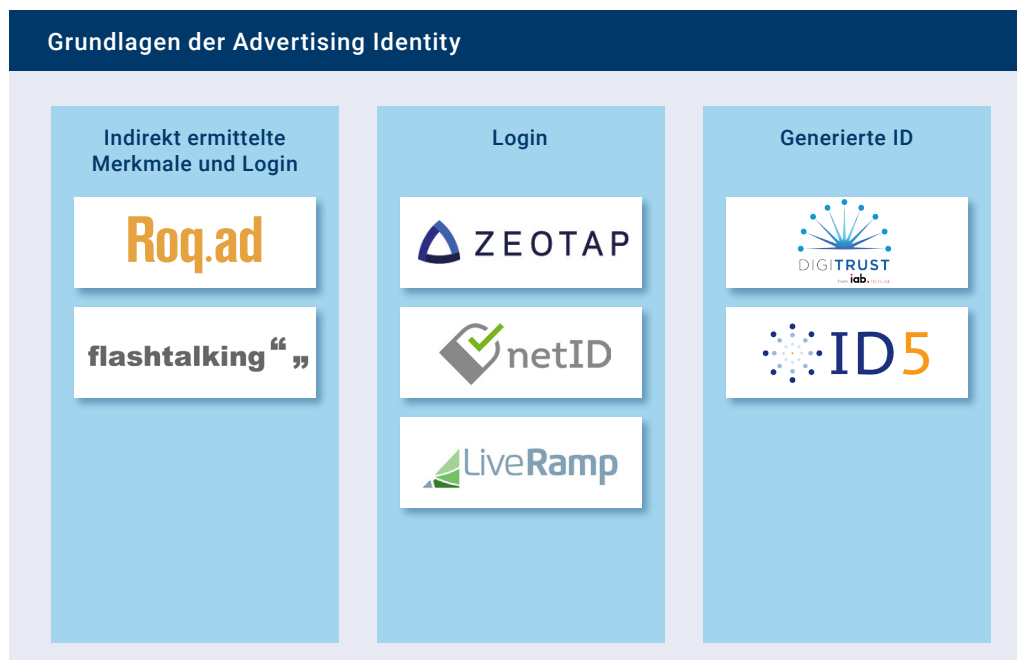
Ein wichtiger Aspekt bei der Betrachtung der Funktionsweise ist die Frage, in welcher Breite die Lösungen eine Wiedererkennbarkeit bieten:

1. Publisher / Website / Domain Level
2. Cross Publisher Level
3. Cross Browser und Geräte Level über Publisher hinweg

Hier ist das Feld der betrachteten Anbieter breit gefächert.



Die den Lösungen zugrundeliegenden Daten lassen sich in drei Gruppen gliedern.



Wesentliche Merkmale der Lösungen im Überblick.

	ID5	Roq.ad	Digitrust	LiveRamp	NetID	Flashtalking – FTrack	Zeotap
Im Prebid User ID Modul integriert*	Ja	Nein	Ja	Ja	Ja	Nein	Ja
Funktion von 3rd-Party-Cookies abhängig	Ja	Nein	Ja	Nein	Nein	Nein	Nein
Entwickelt Lösung für 3rd-Party-Cookie-Problematik	Ja	-	Nein	-	-	-	Ja
Identifikation in Safari möglich	Nein	Ja	Nein	Ja	Ja	Ja	Ja
Identifikation in Firefox möglich	Nein	Ja	Nein	Ja	Ja	Ja	Ja
CMP zur Reichweitensteigerung (Soft Login) integriert	Nein	Nein	Nein	Ja	Ja	Nein	Mittels Partnerschaften
Ermöglicht Frequency Capping im Programmatic-Umfeld	Ja	Ja	Ja	Ja	Indirekt	Ja	Ja
Ermöglicht Cross Device Targeting im Programmatic-Umfeld	Nein	Ja	Nein	Ja	Indirekt	Nein	Ja
Nutzt Fingerprinting	Nein	Nein	Nein	Nein	Nein	Ja	Nein

* neben Prebid unterstützen marktgängige Header Bidding-Lösungen anderer SSP-Anbieter die Integration der verschiedenen Identity-Anbieter und entsprechende Weitergabe der Advertising Identity an angeschlossene Technologiepartner

Die Anbieter im Detail

ID5 – Universal ID

Für ihr Produkt Universal ID setzt ID5 auf clientseitige und 3rd-Party-Cookies. Sie generieren eine ID und schreiben diese clientseitig als 1st-Party-Cookie unter der Publisher-Domain und als 3rd-Party-Cookie unter der ID5-Domain.

Die 3rd-Party-Cookies sind in Safari und Firefox blockiert und werden potenziell auch in Chrome Einschränkungen erfahren. Für ID5 bedeutet dies heute schon, dass sie in Safari und Firefox nur innerhalb eines Publishers wiedererkennen können. Auf Chrome auch über Publisher hinweg.

Auf diese Einschränkung reagieren sie mit einer Erweiterung ihres Produkts, welche aktuell entwickelt wird und laut Aussage des Hersteller im ersten Halbjahr 2020 in einer ersten Version verfügbar sein wird. Publisher können mit der für sie generierten ID weitere Signale mit-senden, z. B. eine gehashte E-Mail-Adresse oder eine Publisher-ID. Findet ID5 dieses Signal in ihren Datensätzen wieder, können sie deterministisch davon ausgehen, dass es sich um denselben Browser handelt.

Darüber hinaus entwickeln sie ein probabilistisches Modell, welches auf Basis von weniger eindeutigen Informationen eine möglichst genaue Wiedererkennung ermöglichen soll. Um das Cookie-Problem übergreifend zu lösen, sind sie zudem in Gesprächen mit Login-Allianzen, deren ID sie ebenfalls als Signal nutzen könnten. Sie planen Ende 2019 eine erste Version dieser Produkterweiterung zu testen.

Eine Device-übergreifende Nutzung der Universal ID ist abhängig von den Partnern, von denen ID5 Signale zur Wiedererkennung erhält.

Die Integration beim Publisher kann über das Prebid User ID Modul erfolgen. Es existieren auch Skripte für eine Prebid-unabhängige Integration.

Roq.ad

Die zugrundeliegende Technologie basiert auf einem proprietären, von Roq.ad entwickelten Cross-Device-Graphen. Auf Basis von Cookies, Mobile-Advertising-IDs und weiteren Attributen in jedem Geräte-Request werden in diesem Graphen verschiedene Geräte unter einer Roq.ad User ID zusammengeführt. Hierfür werden deterministische und probabilistische Daten verwendet.

Deterministisch werden z. B. verschlüsselte Nutzernamen oder E-Mail-Adressen verwendet. Für das probabilistische Verfahren werden Attribute wie z. B. verschlüsselte und verkürzte IP-Adressen, Zeitstempel, Geo-Location-Datensätze, Internet Service Provider und viele weitere verwendet. Auf deren Basis werden Annahmen getroffen, mit welcher Wahrscheinlichkeit es sich bei mehreren Geräte-Identifiern um dieselbe Person handelt. Hierbei werden Online-, Mobile- und auch Offline-Daten verwendet. Auch im Gespräch mit anderen Marktteilnehmern wird der probabilistische Ansatz generell als sehr stabil gewertet, wenn der Wahrscheinlichkeitsschwellenwert hoch genug angesetzt wird.

Roq.ad verfügt über Tags, welche Web- und Mobile-Apps eine Identifizierung ermöglichen. Primär wird Roq.ad auf der Advertiser-Seite eingesetzt. Publisher-Integrationen und die Übermittlung der Roq.ad ID im Bidstream vom Publisher über die SSP zur DSP sind seltener zu sehen.

Anwendungsfälle wie Cross-Device (i) Remarketing, (ii) Audience Amplification und (iii) Storytelling im Programmatic Advertising werden via Roq.ads Partnerintegrationen in marktführenden Demand-Side-Plattformen und Adservern wie The Trade Desk, Xandr, ActiveAgent, Addition, Flashtalking und viele weitere vollständig unterstützt.

Als Graphen-basiertes System ist die Roq.ad ID weniger stark von den Cookie-Einschränkungen betroffen. Dies gilt jedoch nur, solange ausreichend Daten im Graphen für das Zusammenführen der Geräte vorhanden sind.

Digitrust

Digitrust hat eine Lösung entwickelt, die auf einem Device mit den Einschränkungen der Browser (Cookies) eine Publisher-übergreifende Identifizierung von Usern ermöglicht. Hierdurch werden durch Digitrust die klassischen Anwendungsfälle des Programmatic Advertising unterstützt. Eine Cross-Device-Erkennung ist jedoch nicht möglich, da ein entsprechender Graph nicht angeboten wird.

Mittels der Digitrust ID kann das sehr aufwendige Cookie Syncing weiter eingeschränkt werden. Der bisher noch weit verbreitete Cookie Sync wird über eine Vielzahl an Requests vom Browser zu den Technologieanbietern der Vermarktungskette durchgeführt. Diese hohe Anzahl an Requests erhöht die Ladezeiten von Websites erheblich. Darüber hinaus ist das Verfahren ineffizient, wodurch sich die adressierbare Zielgruppe bzw. die Reichweite verringert.

Digitrusts Verfahren verspricht im Gegensatz zum Cookie Syncing schnellere Ladezeiten und weniger Reichweitenverluste.

Digitrust nutzt eine bei den meisten Publisher-Integrationen clientseitig generierte und im Cookie abgelegte 64-bit-ID. In selteneren Fällen wird die ID auf Serverseite generiert. Der Inhalt der ID ist zufällig generiert. Das Besondere an der ID ist, dass sie verschlüsselt im Cookie abgelegt wird. Es existieren für jeden Publisher dedizierte Public Keys, mit denen die IDs verschlüsselt werden. Im 1st-Party-Cookie zweier Publisher im selben Browser liegen somit unterschiedliche verschlüsselte Inhalte, die dieselbe ID enthalten. Da beide Publisher unterschiedliche Public Keys für die Verschlüsselung nutzen, sind sie ohne den Private Key nicht zusammenzuführen. Der Publisher gibt die verschlüsselte DigiTrust ID an die SSP bzw. an die eigene Ad-serving-Technologie weiter. Erst hier auf der Serverseite wird die ID mit dem privaten Schlüssel entschlüsselt und z. B. in den Bidrequest als 4th-Party-Identifizier mitgegeben.

Digitrusts Lösung basiert zu 100 % auf 3rd-Party-Cookies. Im Firefox ist Digitrust geblockt (disconnect.me-Liste). Im Safari ist Digitrust mit hoher Wahrscheinlichkeit auch oft geblockt. Digitrust fokussiert sich bei der Weiterentwicklung auf die Geräte und Browser, auf denen weiterhin 3rd-Party-Cookies verfügbar sind. Eine z. B. Graph-basierte Lösung für das Cookie-Problem ist nicht in Planung.

Digitrust kann über das UserID Modul in prebid genutzt werden. Darüber hinaus bietet Digitrust eine direkte proprietäre Einbindung mittels direkt von Digitrust zur Verfügung gestellten Skripten an.

Essenziell ist neben der Integration auf der Publisher-Seite die Unterstützung der Digitrust ID durch die vom Publisher zur Monetarisierung genutzten Advertising-Technology-Plattformen (SSP, DSP).

Advertising ID Consortium

Anders als andere Anbieter in diesem Dokument bietet das Consortium keine eigene Technologie an. Es werden vielmehr reichweitenstarke Technologien von teilnehmenden Technologieanbietern empfohlen.

Die vom Consortium empfohlenen Technologien sind die in diesem Dokument betrachteten Lösungen von LiveRamp, Digitrust und die Unified ID Solution von The Trade Desk. Durch diese Aufstellung verarbeitet und speichert das Consortium selbst keine Daten.

Mitglieder des Consortiums verpflichten sich, diese Technologien zu unterstützen. Vertraglich bietet das Consortium eine Lizenzierung von LiveRamp für Mitglieder an. Digitrust und The Trade Desk müssen direkt lizenziert werden.

Die Mitglieder des Consortiums kommen gleichermaßen aus dem Bereich der Demand und Supply Side. Auch Publisher konnten als Mitglieder gewonnen werden. Namentlich genannt werden The Rubicon Project, Index Exchange, DataXU, LiveRamp und The Trade Desk. Die Mitgliedschaft kostet jährlich 5.000,00 \$.

LiveRamp

Ihre Multi-Device-fähige Lösung ist unabhängig von Cookies. Damit ist sie nicht von den Einschränkungen in Firefox und Safari betroffen. Wo 3rd-Party-Cookies noch für Identity-Zwecke nutzbar sind (Chrome), nutzen sie sie, um maximale Reichweite zu liefern. Wo nicht auf Cookies zurückgegriffen werden kann, kommt LiveRamps ATS zum Einsatz. ATS steht für Authenticated Traffic Solution. Durch die Integration von ATS auf der Publisher-Seite erhält LiveRamp einen verschlüsselten Identifier (z. B. gehashte E-Mail-Adresse), der zur Überprüfung des bestehenden ID-Graphen genutzt wird. Findet LR einen zugehörigen Identifier im LiveRamp-Graph, wird dieser zusätzlich verschlüsselt und per Envelop an den Publisher und danach an die angeschlossene SSP gesendet. Der erhaltene gehashte Identifier wird danach sofort gelöscht.

Ihr Ansatz ist geräteübergreifend. Hierunter subsumieren sie alle Geräte, bei denen sie mit hoher Wahrscheinlichkeit davon ausgehen, dass sie derselben Person zuzuordnen sind. Laut LiveRamp bietet die Identity-Lösung eine neutrale, stabile ID für Konsumenten – unabhängig von Geräten und unter Einhaltung sämtlicher EU-Datenschutzregularien.

LiveRamp arbeitet ausschließlich deterministisch. In die Erkennung fließen nur absolute Daten ein. Erkennung über IP-Adressen und Ähnliches werden nicht durchgeführt.

LiveRamp hat die Consent Management Plattform Faktor.io (jetzt LiveRamp Privacy Manager) gekauft und bietet diese Lösung gebündelt mit der Identity-Lösung an. Hierdurch wird es für Publisher einfacher, die rechtlichen und technischen Aufgaben zu lösen. Solange der Publisher eine CMP im Einsatz hat, welche den IAB TCF Consent String ausgeben kann, ist der Einsatz von LiveRamps eigener CMP nicht notwendig. Für LiveRamp ist dies neben der notwendigen rechtlichen Lösung eine Hilfestellung zur Reichweitensteigerung. Darüber hinaus stellt LiveRamp Publishern die Nutzung einer Registration-Wall zur Verfügung.

LiveRamp ist einer der Technologie-Partner, die im Rahmen des Advertising ID Consortiums eine empfohlene Lösung anbieten.

Für Publisher ist es sehr einfach, ATS per JavaScript zu aktivieren, es kann aber ebenso ein Server-Side-Modul genutzt werden, um einen dauerhaften Identifier zu schaffen. (So kann zum Beispiel ATS über das Prebid ID Modul, über den Index Exchange Wrapper und auf Anfrage auch über weitere angeschlossene SSPs aktiviert werden.)

Mapp

Im Rahmen von Mapp Intelligence wird eine sogenannte Cross Device Bridge angeboten. Hierbei handelt es sich um ein Angebot zur anonymisierten, geräteübergreifenden Nutzer-Erkennung, die kein Login erfordert. Hierbei werden deterministische und probabilistische Methoden kombiniert. Die Technologie basiert einerseits auf gehashten E-Mail-Adressen und andererseits auf gerätespezifischen Merkmalen.

Die Cross Device Bridge ist im Zusammenspiel mit anderen Mapp-Produkten nutzbar. Advertiser können hierdurch z. B. personalisierte Kampagnen in der Customer Journey kontinuierlich

lich umsetzen und optimieren. Die Technologie basiert auf einem kooperativen Pool aus Cross-Device-Daten verschiedener Firmen aus Europa und den USA.

Auf der Publisher-Seite existiert keine Schnittstelle, die es ermöglichen würde, eine Webtrekk-basierte ID einem Adserver oder einer SSP zu übergeben.

Aufgrund dessen wird Webtrekk im Folgenden nicht genauer analysiert.

netID

Aus Perspektive der Werbevermarktung bietet netID eine Lösung für das Publisher- und Geräte-übergreifende Adressieren von Zielgruppen.

netID Accounts können vom User über einen der netID-Account-Anbieter (z. B. Web.de, Gmx.de) angelegt werden. Es werden auch Neuregistrierungen mittels beliebiger E-Mail-Adressen unterstützt. Hierbei ist die Nutzung besonders einfach, da bereits existierende Accounts bei Account-Anbietern direkt für netID genutzt werden können.

Bei netID Partnern kann der Nutzer bei der Erstverwendung in der Regel zwischen dem individuellen Login des Partners und dem Login mit netID wählen. Sofern er netID verwendet kann er das Angebot des Partners im Folgenden mit seinem netID Account nutzen und daher mit den gleichen Login Daten.

Wesentliche Hürden wie das mehrmalige Wählen und Merken von Passwörtern oder das Ausfüllen von langen Formularen für den Login auf einer Website sind hiermit genommen. Die rechtliche Grundlage ist bei diesem SSO auch immer geklärt und über alle Partner hinweg einheitlich gehalten. Ein Privacy Center gibt dem User die zentrale Kontrolle über seinen Login, seine Daten und deren Verwendung auf den Partnerangeboten.

Der User kann einer Weitergabe von Daten an einen Partner – immer auf Basis der Datenschutzbestimmungen des Partners – zustimmen. Für einen Publisher, der die netID unterstützt, bedeutet dies, dass er die E-Mail-Adresse z. B. für Newsletter-Aussendungen auf diesem Weg vom User abfragen kann.

Aus Perspektive der Vermarktung könnte der Publisher die pseudonymisierte E-Mail-Adresse als ID für das Targeting oder Frequency Capping nutzen. Diese Verwendung wird allerdings seitens netID über den SSO-Dienst datenschutzrechtlich nicht ermöglicht. Die Verwendung bzgl. dieser Anwendungsfälle wird über einen an eine Einwilligung gebundenen stabilen netID Identifier unterstützt, wobei die Einwilligung mittels der entsprechenden Einwilligungsmanagementprodukte der netID eingeholt werden kann. Die netID ist generell an keiner Stelle ein direkter Partner in der Vermarktungskette. Sie bietet dem Publisher technische Schnittstellen an, um mit netID-Nutzern zu interagieren. Die Nutzung dieser Schnittstellen bzw. der Daten liegt in der Hoheit des Publishers. Auch die damit verbundenen datenschutzrechtlichen Notwendigkeiten wie z. B. das Einholen der Zustimmung der Nutzer für werbliche Datenverarbeitung liegen aufseiten des Publishers. Die netID standardisiert diese jedoch für ihre Nutzer/Partner.

Aktuell integriert netID ihre Einwilligungsmanagementprodukte in TCF-2.0-basierte Consent-Management-Plattformen (CMPs), die auch eine werbliche Nutzung von Daten ermöglichen. Die Integration dieser Plattform mit dem zentralen Privacy Center des Nutzers bietet ein hohes Maß an Kontrolle über die Datennutzung. Der Einwilligung/Transparenz-Status, z. B. für den Zweck der werblichen Ansprache, wird für jeden Publisher individuell verwaltet. Der Nutzer erhält aber an einer Stelle den Überblick. Mit der CMP-Integration geht auch ein sogenannter Soft-Login einher, der zur Identifikation des Users und zur Verwaltung seines generellen Einwilligung/Transparenz-Status keine Registrierung (inkl. Stammdatentransfer) beim Publisher erfordert. Parallel dazu ist natürlich auch immer die Identifikation des Nutzers und

auch das Verwalten des Einwilligung/Transparenz-Status basierend auf einem SSO-Login (Hard-Login) beim Partner möglich. Diese Erweiterung wird mit dem IAB Transparency and Consent Framework (TCF) Version 2.0 in Q2 ausgerollt.

Flashtalking – Ftrack

Flashtalking bietet Ad-serving-Lösungen für die Advertiser-Seite an. In der Regel liefert Flashtalking die Werbemittel über die eigene Infrastruktur als Redirect aus. Hierdurch haben sie sehr viele Kontaktpunkte mit dem Gerät des Nutzers – diese können dann als deterministische Ankerpunkte für die Anreicherung des probabilistischen Algorithmus genutzt werden. Flashtalking bietet keine Media-Einkaufstechnologien an, sondern fokussiert sich auf eine unabhängige Messung der Auslieferung der Kampagnen und Deals.

Mit der Ftrack ID hat Flashtalking die Basis für die Attributionsanalyse und das Kampagnen-reporting geschaffen. Flashtalking bietet auf Basis dieser Daten einen Vergleich zu den Reportings, die von DSP- oder SSP-Seite erstellt werden.

Auf Basis der vom Browser übermittelten deterministischen und von Ftrack auf probabilistischem Weg verarbeiteten Signalen ist die Ftrack-Technologie in der Lage, Browser und Geräte mit einer sehr hohen Wahrscheinlichkeit wiederzuerkennen. Durch die verwendeten Methoden stellt Ftrack einen Ersatz von Cookies dar und ist damit nicht von den Einschränkungen bei der Cookie-Verarbeitung betroffen. Einen eigenen Cross-Device-Graphen umfasst Ftrack in Europa noch nicht. Für eine deviceübergreifende Analyse (als Basis für ihre Attributionslösung) arbeitet Flashtalking mit anderen Anbietern (z. B. Roq.ad oder TapAd) zusammen – die Device-Matchingrates werden durch den Einsatz der Ftrack-Technologie deutlich gesteigert. Durch die bisherige Fokussierung auf die reine Auslieferung und Messung für Advertiser ist die Ftrack

ID nicht für andere programmatische Akteure im Gebotsverfahren verfügbar. Flashtalking schließt jedoch nicht aus, dass sie die Ftrack ID für den programmatischen Markt öffnen.

Zeotap

Zeotaps bietet eine End-to-End Technologieplattform in Kombination mit einer globalen Onboarding- und Datenlösung. Die hierfür genutzten Daten erhält Zeotap aus Datenpartnerschaften und Integrationen mit Telekommunikationsanbietern, E-Commerce-Playern und App-SDK-Anbietern. Auf Basis von Pixel-, SDK- oder Server-to-Server-Integrationen mit diesen Datenpartnern werden die vorhandenen Identifier und Attribute extrahiert.

Diese Daten fließen in Zeotaps People/Identity-Graphen. Daten werden nur bei vorliegendem Consent genutzt. Zur Qualitätssicherung werden die verwendeten Daten z. B. gegen Nielsen DAR geprüft. Der Graph ermöglicht es u. a. durch proprietäre patentierte Zeotap-Technologie, Online- und Offline-Identifier deterministisch zu matchen.

Zeotap nutzt ausschließlich deterministische Daten. Dies können Identity-Daten, soziodemografische Daten, App-Nutzungsdaten oder auch Kaufabsichtsdaten von E-Commerce-Partnern sein.

Zeotap arbeitet hierfür mit personenbezogenen Daten wie Mobile Ad IDs, Cookie IDs, E-Mail-Adressen oder Telefonnummern. Diese Daten werden durch Hashing pseudonymisiert.

Im Graph wird eine zentrale, verbindende Zeotap ID verwendet, die die Identifier aus verschiedenen Datenquellen clustert. Ab Q1 2020 wird diese Zeotap ID unter dem Namen ID+ Unternehmen im programmatischen Ökosystem angeboten.

Sicherheit

Summary

Alle betrachteten Anbieter setzen auf eine Infrastruktur in der EU. Hinsichtlich der Verwendung personenbezogener Daten sind alle Anbieter stark sensibilisiert. Ein Großteil der Anbieter holt den Consent nach dem IAB Transparency and Consent Framework ein. Für die genutzte ID wird bei allen Anbietern mindestens ein Hash-Wert genutzt. Zum Teil werden IDs mittels Public/Private-Key-Verfahren einfach oder sogar mehrfach verschlüsselt.

Im Folgenden einige wesentliche Merkmale im Bereich der Sicherheit im Überblick.

	Infrastruktur in DE	Infrastruktur in EU	Beruft sich auf berechtigtes Interesse in EU	Werden personenbezogene Daten verarbeitet	ID gehasht	ID verschlüsselt	ID mehrfach verschlüsselt
ID5	Ja	Ja	Nein	Ab Ende 2019	Ja	Ja	Nein
Roq.ad	Ja	Ja	Nein	Ja	-	Ja	Nein
Digitrust	Ja - CDN	Ja	Nein	Nein	-	Ja	Nein
Liveramp	Nein	Ja	Nein	Ja	-	-	Ja
NetID	Ja	Ja	Nicht für Identifikation des Nutzers	Ja	-	Nein	Nein
Flashtalking - FTrack	Nein	Ja	Ja – iab TCF in Vorbereitung	Ja	Ja	Ja	Nein
Zeotap	Nein	Ja	Nein, nur expliziter consent	Ja	Ja	Nein	Ja

Die Anbieter im Detail

ID5

ID5 setzt bei der Generierung der Universal ID auf eine 256-bit-Verschlüsselung. Die ID wird serverseitig generiert, verschlüsselt, gespeichert und dann an den Client zur Speicherung gesendet. Für die Speicherung und Nutzung der ID holt ID5 die Einwilligung des Nutzers ein. Wenn sie mit weiteren Signalen arbeiten, erhalten sie die darin enthaltenen Daten grundsätzlich gehasht. Ihre Server betreiben sie als Firma aus dem Vereinigten Königreich in Frankreich und Deutschland.

Roq.ad

Die von Roq.ad genutzte Graph UserID wird auf Serverseite gespeichert. Roq.ad nutzt als Lerngrundlage z. B. gehashte E-Mail-Adressen und Nutzernamen. Für die der Lösung zugrunde liegende Datenverarbeitung holen sie den Consent über das IAB Transparency and Consent Framework 2.0 ein.

Die von Roq.ad genutzte Infrastruktur befindet sich in der EU.

Digitrust

Die Digitrust ID wird über die WebCrypto API im Browser erzeugt. Es handelt sich hierbei um 64-bit-Zufallsdaten. Die ID wird lediglich im Client in einem Cookie abgelegt. Digitrust erhebt keine personenbezogenen Daten. Digitrust holt über das IAB Transparency and Consent Framework die Einwilligung für die Speicherung der ID ein. Nur bei Einwilligung wird die ID in das Cookie geschrieben und weiterverwendet. Die unter Funktionsweise beschriebene Verschlüsselung der ID im Cookie bietet einen erhöhten Schutz gegen den Missbrauch der ID durch unberechtigte Dritte.

Digitrust sammelt und speichert keinerlei Daten. Die Auslieferung der nötigen Skripte erfolgt über ein CDN mit Edge Locations in Deutschland, sofern der Zugriff des Users aus Deutschland erfolgt.

LiveRamp

Zur Generierung einer ID nutzt LiveRamp bei der Integration in den Publisher ein JavaScript im Browser. Dem JavaScript wird z. B. eine E-Mail-Adresse (gehasht) übergeben. Diese wird von LiveRamp in eine IDL übersetzt, verschlüsselt und serverseitig durch eine API (LiveRamps Sidecar-Dienst) in den Envelop übersetzt. Dieser Envelop ist für jeden Request unique und erlaubt nur dem Publisher durch das Speichern in einem 1st-Party-Cookie (alternativ auch HTML5 Local Storage) Zugriff darauf. Für das Programmatic Advertising wird der verschlüsselte IDL Envelop an die SSP weitergegeben. Diese gibt ihn zunächst an den LiveRamp Service Sidecar weiter. Sidecar entschlüsselt ihn und gibt spezifisch verschlüsselte IDLs für jede der anzusprechenden DSPs zurück. Wenn LiveRamp diesen DSPs Advertiser- oder 3rd-Party-Daten (per Server-to-Server oder API) liefert, erhalten sie wieder „ihre“ verschlüsselten IDLs. Somit können DSPs Gebote auf die Bidrequests abgeben. Die ID kann nicht wieder depseudonymisiert werden.

Jegliche personenbezogenen Daten werden laut LiveRamp während des Matching-Prozesses im Graph durch anonyme Daten ersetzt. Keine personenbezogenen Daten werden von LiveRamp geloggt. Personenbezogene Daten erhält LiveRamp von Publisher- und Advertiser-Seite.

In den Graphen hat LiveRamp einen Universal Opt-out integriert. LiveRamp nutzt als Infrastruktur Google-Cloud-Komponenten in Brüssel.

netID

netID nutzt zum Betrieb ihrer Lösung ausschließlich Infrastruktur in der EU.

Mit netID verwaltet der Nutzer seine personenbezogenen Daten und deren Weitergabe immer bei seinem Account-Anbieter. Partner können diese mittels des SSO vom User abfragen, dieser kann dem Transfer dauerhaft zustimmen und später auch wieder widerrufen. Die Identifikation eines Nutzers für werbliche Zwecke / Personalisierung, basierend auf seiner netID, findet nur mit seiner Einwilligung statt.

Für den SSO-Prozess und andere Schnittstellen werden zum Teil die E-Mail-Adresse sowie Session-Informationen über den User in First-Party-Cookies abgelegt. Der Partner/Publisher, der netID nutzt, ist im Rahmen der geltenden Datenschutzrichtlinie dafür verantwortlich, wie und für welche Zwecke er die Userdaten nutzt.

Flashtalking – Ftrack

Ftrack ist für die Nutzung des IAB Transparency and Consent Frameworks vorbereitet. Für die aktuelle Nutzung zum Betrieb des Adservers beruft sich Flashtalking auf das berechtigte Interesse. Im Rahmen von Ftrack werden keine personenbezogenen Daten verarbeitet. Die Daten, die verarbeitet werden, werden gehasht verwendet.

Zeotap

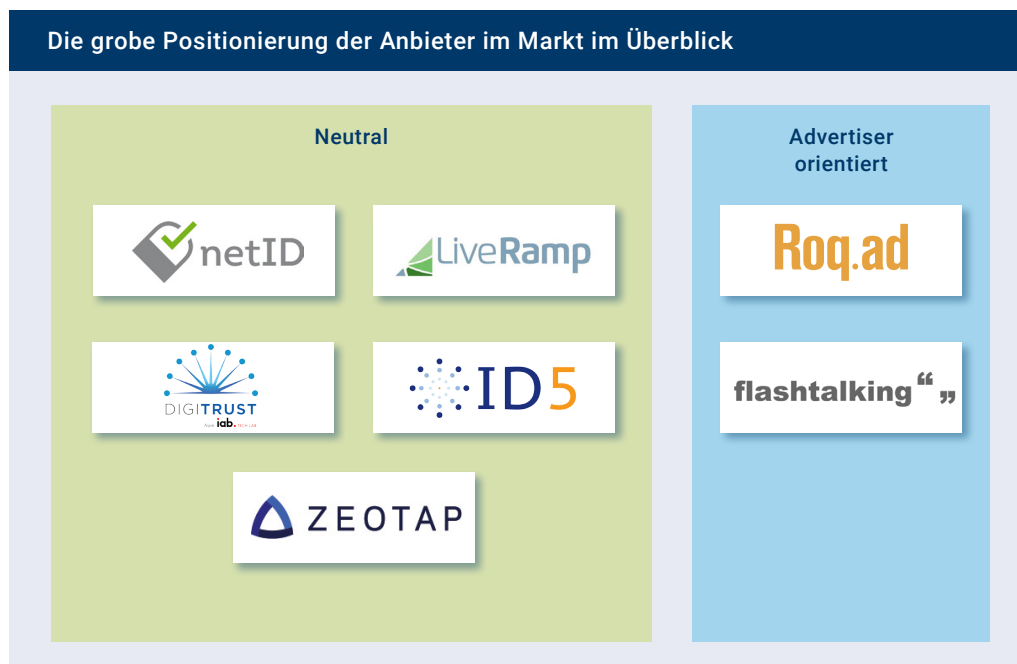
Die Zeotap ID wird basierend auf 1st Party Login Daten wie beispielsweise der Email Adresse serverseitig erzeugt und in Echtzeit mit den Partnern ausgetauscht. Durch den Zeotap Identity Graphen können weitere IDs sowie 3rd Party Daten mit der ID verknüpft werden.

Die beim Betrieb der Lösung erhobenen persönlichen Daten werden pseudonymisiert. Personenbezogene Daten werden nur bei Vorliegen einer expliziten Einwilligung des Users erhoben. Zeotap verfügt über mehrere Zertifizierungen für Datenschutz und Sicherheit ihrer Lösung.

Neutralität

Summary

Die betrachteten Anbieter positionieren sich teils neutral und teils auf der Advertiser/Käufer-Seite. Die Anbieter sprechen sich meist für eine kollaborative Entwicklung des Advertising Identity Ecosystems aus. Sie gehen meist von einem Szenario aus, in dem mehrere Identity-Anbieter im Markt koexistieren.



Vergleich Der Anbieter

ID5 – Universal ID

ID5 wurde vor mehr als 2 Jahren als Start-up gegründet und ist der Aussage des Co-Founders Scott Menzer nach durch die Investoren nicht strategisch im Advertising-Ökosystem gebunden. Ferner ist ihre strategische Ausrichtung eine vollkommen neutrale. Sie sprechen sich für eine Zusammenarbeit der verschiedenen Anbieter in ihrem Bereich aus. So sehen sie die Möglichkeit einer möglichst großen Abdeckung und Verbreitung von mindestens einer nutzbaren Identität. Der Kern der ID5-Technology ist Closed Source und proprietär. Die Teile, die zur technischen Integration der Marktteilnehmer benötigt werden, sind Open Source und werden von ID5 gepflegt. Die im Rahmen der Dienstleistung anfallenden Daten werden nicht für andere Zwecke als die der Dienstleistung genutzt.

Roq.ad

Die Lösung von Roq.ad ist aktuell eher auf der Käuferseite angesiedelt. Advertiser haben durch Roq.ad's Graphen die Möglichkeit, über das Matching von verschiedenen Identifikatoren von unterschiedlichen Geräten auf Personen eine genauere Zielgruppenansprache zu erreichen. Die Lösung ist eine Closed-Source-Implementierung, die klassische Machine-Learning-Methoden zur Berechnung des Graphen nutzt. Die erhobenen Daten werden für das laufende Training des Graphen und damit für alle Nutzer des Graphen genutzt.

Digitrust

Der Betrieb und vor allem die Weiterentwicklung von Digitrust wird durch das IAB techlab und die Mitglieder der Commit Group gesteuert. Mitglied kann hierbei unabhängig von seiner strategischen Positionierung jeder Marktteilnehmer werden, der Digitrust nutzt. Einzelne Firmen können strategische Entscheidungen nicht allein beeinflussen. Die Integrationsseite der Lösung ist offener Quellcode. Die Serverseite ist Closed Source. Die Dokumentation beschreibt die angewandten Methoden jedoch sehr transparent. Eine Weiterverwendung von Daten kann nicht erfolgen, da keine erhoben werden.

LiveRamp

LiveRamp ist ein neutraler Anbieter im Markt. LiveRamp ist gleichermaßen auf der Advertiser- und Publisher-Seite daran interessiert, Partnerschaften einzugehen, um die Reichweite seiner ID zu erhöhen. Die Lösung ist Closed Source.

Sie kommen so allen Nutzern des Graphen zugute. Die Daten werden nicht zu anderen Zwecken verwendet. LiveRamp ist nicht im Mediageschäft involviert, sondern sieht seine Lösung als Basis für andere, die im Daten- oder Mediageschäft einen personenbezogenen Identifier benötigen.

netID

NetID wurde als Stiftung gegründet, um eine möglichst neutrale Login-Lösung zu schaffen. NetID selbst positioniert sich als Daten schützender Dienst für die User und zudem als Partner und Enabler der Website-Betreiber auf Publisher- und Advertiser-Seite. Sie sind nicht im Mediageschäft involviert.

Datenverarbeitung in der Vermarktung liegen immer in der Hoheit des Website-Betreibers. Angebotene technische Funktionen oder Integrationen werden immer dem Publisher zur Nutzung im Rahmen seiner Vorhaben angeboten. Eine direkte Involvierung in die Vermarktungskette strebt NetID nicht an.

Flashtalking – Ftrack

Ftrack ist aktuell klar auf der Advertiser-Seite angesiedelt. Die Lösung ist Closed Source. Flashtalking ist nicht wie DSPs am Einkauf der Reichweite beteiligt. Der Adserver liefert auf von Dritten eingekauften Flächen aus und misst die Ergebnisse. Hierdurch sieht sich Flashtalking in einer neutralen Position. Für einen nicht ausgeschlossenen, aber nicht konkret geplanten Rollout von Ftrack als ID für das Advertising ID Ecosystem sieht sich Flashtalking dadurch neutral aufgestellt.

Zeotap

Die Lösung von Zeotap wird im Rahmen der zielgerichteten Kampagnenauslieferung und beim Targeten von Deals verwendet. Hierdurch richtet sich das Angebot gleichermaßen an die Publisher/Supply- und die Advertiser/Käufer-Seite. Mit dem Rollout der Zeotap ID als unabhängiger Identifier für das programmatische Ecosystem ist die ID auch in Kombination mit anderen Datenanbietern nutzbar geworden. Die der Lösung zugrundeliegende Technologie ist Closed Source.

Die beim Betrieb der Lösung gewonnenen Daten werden ausschließlich zur Erbringung der Leistung für den Kunden verwendet.

Qualität

Einführung

Die Lösungen können grob in drei zugrundeliegende Vorgehensweisen unterteilt werden.

Deterministisch

Eine Lösung, die auf deterministischen Daten aufbaut, wird immer möglichst absolute Daten verwenden. Konkret sind dies bei den hier untersuchten Anbietern E-Mail-Adressen oder Nutzer/Login-Namen. Diese werden verhasht als ID genutzt. Hierfür werden sie im Browser abgelegt und in die Vermarktungskette mitgegeben, zum Beispiel an den Adserver oder über die SSP in den Bidrequest.

Deterministische Verfahren sind sehr genau bei der Wiedererkennung von Personen. Dies geschieht auch über Browser, Geräte und Apps hinweg. Wo immer der gleiche Hash wiedergefunden wird, kann mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass es sich um dieselbe Person handelt. Lediglich bei der Nutzung eines Logins von mehreren Personen wird die Genauigkeit verringert.

Ein Hauptnachteil eines deterministischen Verfahrens ist die Reichweite. Sie hängt direkt von der Häufigkeit des Logins ab. In Gesprächen mit Anbietern wurde eine Login-Rate von 5 % als aktuell hoch genannt.

Ein weiterer Nachteil sind potenzielle Präzisionsverluste durch Familiennutzung eines Logins, z. B. auf dem Apple TV. Anbieter wie Apple oder Google steuern hier betriebs-systemseitig gegen, indem das einfache Wechseln von Profilen ermöglicht wird.

Probabilistisch & deterministisch gemischt

Bei dieser Vorgehensweise kommt zum beschriebenen deterministischen Ansatz eine Komponente hinzu. Beim probabilistischen Ansatz werden indirekte Daten genutzt. In dem gemischten Ansatz wird immer dann, wenn keine E-Mail-Adressen oder Login-Daten vorhanden sind, auf indirekte, nicht vom User direkt stammende Daten zurückgegriffen. Im Rahmen dieser Untersuchung wurden als Beispiele unter anderem verkürzte IP-Adressen, Zeitstempel, Geo-Location-Datensätze und Internet-Service-Provider-Informationen genannt. Konkret kann dies wie folgt genutzt werden: Eine Identity-Lösung erfasst z. B. innerhalb eines akzeptablen Zeitfensters zwei Zugriffe auf unterschiedlichen Publishern mit derselben IP-Adresse. Dies wird im Graphen als ein Datenpunkt gesichert. Mit der Zeit kommen weitere Datenpunkte hinzu. Ab einer bestimmten Menge an Datenpunkten kann die Identity-Lösung die unterschiedlichen Zugriffe miteinander verknüpfen und als von einer Person oder einem Haushalt stammend klassifizieren.

Der probabilistische Ansatz hat eine höhere Fehlerwahrscheinlichkeit als der deterministische. Wie hoch diese Fehlerwahrscheinlichkeit ist, kann in den betrachteten Lösungen variiert werden. Ist der Nutzer des Systems bereit, eine höhere Fehlerwahrscheinlichkeit einzugehen, geht dies einher mit einer höheren adressierbaren Reichweite. Im gegenteiligen Fall sinkt die Reichweite. Ein Fehler äußert sich einerseits in der Erkennung von mehreren Personen, obgleich es tatsächlich nur eine ist.

Andererseits können zwei unterschiedliche Personen als nur eine klassifiziert werden. Im Fall der Kombination von deterministisch und probabilistisch in einem System können über die Probabilistik generell Reichweiten erschlossen werden, die nur deterministisch nicht adressierbar wären.

Durch Markierung

Der dritte vorgefundene Ansatz basiert auf einer Markierung im verwendeten Browser. Hierbei wird eine ID generiert. In diesem Fall besteht die ID aus einer in Bezug auf die Person beliebigen Information wie z. B. einer Zufallszahl. Diese z. B. in einem Cookie oder im Local Storage gespeicherte ID wird nun bei jedem Kontakt betrachtet. Handelt es sich um dieselbe ID, wird eine Wiedererkennung angenommen.

Dieses Verfahren erfährt durch die schon beschriebenen Entwicklungen der Browser (v. a. Safari und Firefox) immer stärkere Einschränkungen. Ohne eine Ergänzung durch deterministische oder probabilistische Verfahren sind schon jetzt Reichweiteneinbußen bei ausschließlicher Verwendung dieses Verfahrens zu beobachten.

Anbieter nach Vorgehensweise betrachtet



Vergleich der Anbieter

ID5 – Universal ID

Hinsichtlich der verwendeten Methodik muss bei ID5 zwischen dem Jetzt und der in ihrer Roadmap skizzierten Zukunft unterschieden werden. Aktuell setzen sie auf Markierungen in Cookies (s. Funktionsweise ID5), wissend, dass das heute schon mit großen Einschränkungen verbunden ist. Eigener Aussage nach arbeiten sie an einem auf Publisher- oder Partner-Daten (Login-Allianzen) basierenden deterministischen System. Dieses soll, wo solche Daten nicht verfügbar sind, um ein Machine-Learning-basiertes probabilistisches System ergänzt werden. Ziel ist eine hohe Gesamterkennung.

Bei einem dualen Ansatz wie diesem muss beachtet werden, dass bei z. B. Gebotsabgabe nicht klar sein wird, ob die ID5 Universal ID für diese Bid Request über ein deterministisches oder ein probabilistisches Verfahren ermittelt wurde. Dies hat einen direkten Einfluss auf die Genauigkeit des verwendeten Targetings. Ein Frequency Cap wird so z. B. ungenauer. Nach eigener Aussage ist das Ziel des Anbieters, die Probabilistik nur dann zu nutzen, wenn die Identifizierung nahezu 100 % sicher ist. Sie erwägen, die Präzision der Probabilistik zu auditieren. Dies könnte die Transparenz gegenüber Partnern steigern. Diese Entwicklungen sind aber zum jetzigen Zeitpunkt noch in einer sehr frühen Phase.

Roq.ad

Roq.ad bietet ein Public-Graph-Modell und ein kundenspezifisches Private-Graph-Modell an. Die Präzision in der Zuordnung mehrerer Geräte zu einer Person kann zugunsten einer höheren Recall-Rate gesenkt werden. Hierbei erhöht sich die Reichweite bei sinkender Treffergenauigkeit. Steigert man die anvisierte Präzision, verringert sich die Zielgruppen-Reichweite. Im Private Graph kann die Präzision (Precision Rate) kundenspezifisch eingestellt werden. Typische Präzisionsraten liegen je nach Zielvorgabe zwischen 85 % und 95 %. Im Public-Graph-Modell werden alle 48 Stunden stets 2 Graphen je Land berechnet: ein präzisions-optimierter Graph und ein reichweitenoptimierter Graph. Im präzisionsoptimierten Graph liegt die Precision Rate bei 91 % mit 30 % Recall. Der reichweitenoptimierte Graph liegt bei 85 % Präzision mit 65 % Recall.

Digitrust

Bei Digitrusts Lösung handelt es sich um eine Cookie-basierte Lösung. Wie unter Funktionsweise beschrieben, unterliegen Cookies schon jetzt in Safari und Firefox starken Einschränkungen. Mit der Digitrust ID kann daher aktuell nur in Chrome Traffic sicher bearbeitet werden. Im Gegensatz zum Cookiematching bietet Digitrust prinzipbedingt eine höhere Matchrate. Geräteübergreifend arbeitet Digitrust nicht.

LiveRamp

LiveRamp baut auf einen Graphen auf. Sie nutzen dabei ausschließlich deterministische Daten und Methoden. Für den Aufbau des Graphen in einem Markt sind sie daher auf personenbezogene Daten der Publisher-Seite angewiesen. Prinzipbedingt sind sie nicht durch die Einschränkungen der Cookies betroffen. Auf einer ausreichenden Datenbasis (Publisher-Integrationen) breitflächig eingesetzt, verspricht LiveRamp in allen Browsern Publisher-übergreifend und auch Geräte-übergreifend ein sicheres Matching anzubieten.

NetID

Die Login/Single-Sign-on-Lösung von NetID arbeitet zu 100 % deterministisch. Ist ein User hard oder soft eingeloggt, liegt eine Identität vor, die bei Einwilligung des Users genutzt werden kann. Loggt sich der User nicht ein, ist er für netID und den Website-Betreiber unbekannt. NetID beschränkt die eigene Lösung auf dieses Verfahren, stellt es aber dem Publisher frei, die zur Verfügung stehenden Nutzerdaten in Verbindung mit anderen Identity-Lösungen, die z. B. Graphen anbieten, zu nutzen, um die Reichweite zu erhöhen.

Flashtalking – Ftrack

Der Cookie-Ersatz Ftrack arbeitet mit probabilistischen Algorithmen auf Basis deterministischer Ankerpunkte. Persönliche Informationen werden hierbei nicht verwendet. Die Präzision der Lösung liegt laut Flashtalking bei 95 % bis 98 %.

Zeotap

Die Lösung von Zeotap arbeitet 100 % deterministisch. Nach Erfahrung von Zeotap ist der Qualitätsverlust bei Nutzung von probabilistischen Daten sehr hoch. Gegen Nielsen-Daten gemessen erreicht der deterministische Datensatz von Zeotap eine Erkennungsgenauigkeit von Personen von bis zu 94 %.

Relevanz

Die Anbieter im Detail

ID5 – Universal ID

ID5 zählt heute 1,5 Mio. Unique-Abrufe der Universal ID monatlich in Deutschland. Ohne in Deutschland bisher direkt aktiv zu sein, haben sie diese Skalierung vor allem über Einbindungen in Partnerplattformen, aber auch Publishern wie Duden.de, Gentside.de und Ohmymag.de erreicht. Sie starten aktuell eine aktive Vermarktung ihres Produkts in Deutschland. Diese zielt auf Tech-Plattformen und große Publisher ab.

ID5 wird von Advertising-Plattformen wie Appnexus und Bidswitch unterstützt. Auf der Supply-Seite wird ID5 unter anderem von Smart unterstützt. Neben weiteren unterstützen die folgenden Demand-Side-Plattformen ID5: Mediamath, Avocet, Adot und Adform.

Roq.ad

Roq.ads Cross-Device Identity Graph umfasst eine Marktabdeckung von 80 % der deutschen Onliner. Eine ähnliche Marktabdeckung wird auch in weiteren Ländern wie Österreich, Schweiz, USA und Polen erzielt

Roq.ad wird unterstützt von marktführenden Demand-Side-Plattformen (DSPs) und Adservern wie The Trade Desk, Xandr, ActiveAgent, Addition, Flashtalking und vielen weiteren.

Digitrust

Digitrust selbst erhebt keine Nutzungsdaten oder KPIs, die Unique User oder anderweitige Reichweiten-KPIs ermitteln lassen.

Auf dem CDN, welches die clientseitigen Skripte ausliefert, kann lediglich die Zahl von 6.000 monatlichen Website-Domains ermittelt werden, auf denen Digitrusts Skripte genutzt werden. Im deutschen Markt ist Digitrust noch nicht sehr häufig in Bidrequests zu sehen.

Unterstützt wird Digitrust von den Demand-seitigen Plattformen Adform, Mediamath, Sizmek und Supply-Side-Plattformen (SSPs) wie Index Exchange, Openx, sovrrn, pubmatic und rubicon project.

LiveRamp

LiveRamp steht beim Markteinstieg in Deutschland noch am Anfang. Im Oktober dieses Jahres hat die aktive Vermarktung des Produkts in Deutschland begonnen. Ihr Ziel ist eine Matchrate von 20 % im deutschen Markt für Ende Q1 2020. Der Markteintritt in Deutschland beginnt mit starken Akquise-Tätigkeiten auf der Publisher-Seite. Auch mit NetID wurden Gespräche geführt. In den USA konnte LiveRamp bereits eine hohe Reichweite aufbauen.

NetID

NetID meldet über alle angeschlossenen Partner/Account-Anbieter hinweg 38 Mio. aktive User pro Monat. Aktuell verzeichnen sie 60 Partner, welche sich zum Großteil aus Online-Publishern und TV-Portalen zusammensetzen.

Account-Anbieter und Nutzer des SSO sind die Gründungsmitglieder der Stiftung web.de, GMX, 7Pass & ProSieben, RTL sowie 1und1. Partner, die den SSO nutzen, sind unter anderem C&A, DPD, ProSieben.de, Kabel1.de.

Flashtalking – Ftrack

Kampagnenbezogen arbeitet Flashtalking Ftrack mit anderen Anbietern auf der Advertiser-Seite zusammen. Zu nennen wären Roq.ad und Tapad, wenn es um Cross-Device-Reporting als Basis für eine channelübergreifende Attribution geht.

Zeotap

Zeotaps Graph ist in 9 Märkten verfügbar, hierzu zählen Nordamerika, Mittel-/Südamerika, Europa (DE, UK, FR, IT, ES) und Indien.

Der Graph von Zeotap deckt ca. 70 % der deutschen Nutzer ab. Der Schwerpunkt liegt hierbei bei Nutzern mobiler Endgeräte. Ca. 70 % der gesammelten Datenpunkte sind mobile Daten. Die restlichen 30 % sind Desktop-Daten.

Eine weitere Steigerung der Relevanz für den deutschen Markt möchte Zeotap über neue Datenpartnerschaften und Publisher-Integrationen erreichen. Die Publisher-Integrationen sollen durch eine Zusammenarbeit mit einer deutschen CMP skaliert werden.

Zeotaps Daten können in der aktuellen Form in bis zu 100 Marketing/Advertising-Kanälen, z. B. DMPs (Adobe, Salesforce, Neustar), Social (Facebook/Instagram, Snapchat), DSPs (The Trade Desk, Adform, Active Agent, Google, MediaMath etc.) oder SSPs/Adservern (z. B. Google AdX/DFP, Smart, Appnexus, Oath) genutzt werden.

Appendix

Erhebungszeitraum

Die Studie wurde von November 2019 bis Januar 2020 erhoben und gibt den Stand der technischen Entwicklungen zu diesem Zeitpunkt wieder. Alle weiteren technischen Änderungen werden ab dem Zeitpunkt werden von der Arbeitsgruppe geprüft und referenzierend auf diese Studie zur Verfügung gestellt.

Kosten und Abrechnungsmodelle

Summary

Die wesentlichen Aspekte der Kosten pro Anbieter im Überblick.

	Publisher	SSP	DSP	Advertiser	Mitgliedschaft nötig
ID5	Nein	Nein	Ja	Nein	Nein
Roq.ad	Ja	Ja	Ja	Ja	Nein
Digitrust	Nein	Ja	Ja	Nein	Ja
LiveRamp	Nein	Nein	Nein	Ja	Nein
NetID	Vermarktungs- produkte: Ja Nur SSO: Nein	Nein	Nein	Nein	Nein
Flashtalking - FTrack	Nein	Nein	Nein	Ja	Nein
Zeotap	Nein	Nein	Nein	Ja	Nein

Die Anbieter im Detail

ID5 – Universal ID

Aktuell ist die ID5 Universal ID kostenlos für alle Parteien. Im nächsten Jahr führt ID5 ein Abrechnungsmodell ein, welches wie folgt funktioniert:

- Für Publisher bleibt sie kostenlos
- Für SSPs, die die ID nur vom Publisher in Richtung DSPs weitergeben, ist sie kostenlos
- Für Marktteilnehmer, die die ID entschlüsseln müssen (DSPs), wird es kostenpflichtig
- Für Marktteilnehmer, die eine Matchingtable für einen ID-Abgleich benötigen, wird es kostenpflichtig

Eine Preisliste und weitere Informationen zu den Vertragskonditionen liegen aktuell noch nicht vor. Sie soll sich aber an den Preisen der Cookie-Matching-Lösung von ID5 orientieren.

Roq.ad

Das Preismodell von Roq.ad basiert für alle Marktteilnehmer auf einem Software-as-a-Service-Modell:

- Publisher: Flat Fee ab 2.000 € pro Monat
- SSP: Kosten abhängig vom Traffic-Volumen
- DSP: Kosten abhängig vom Traffic-Volumen
- Advertiser: Flat Fee ab 2.000 € pro Monat

Digitrust

Für Publisher ist Digitrust kostenlos nutzbar, eine IAB Techlab oder IAB Mitgliedschaft ist nicht nötig.

Das Kostenmodell von Digitrust basiert auf einer Abrechnung bei den angeschlossenen Technologieplattformen auf der Verkäufer- und Käufer-Seite. Hier richtet sich die Höhe der monatlichen Kosten nach dem jährlichen gemanagten Media-Budget (annual managed media) oder Nettoumsatz (annual net revenues):

- jährlich gemanagtes Media Budget < 5 Mio. \$
oder jährlicher Nettoumsatz < 1 Mio. \$: kostenlos
- jährlich gemanagtes Media Budget < 50 Mio. \$
oder jährlicher Nettoumsatz < 10 Mio. \$: 2.500 \$ / Monat
- Andere Plattformen: 5.000 \$ / Monat

Um Digitrust nutzen zu können, muss die Plattform zudem Mitglied im IAB Techlab sein. Details hierzu siehe hier: <https://iabtechlab.com/about-the-iab-tech-lab/join-the-iab-tech-lab/>

LiveRamp

LiveRamp finanziert sich ausschließlich über die Advertiser. Das Modell sind gestaffelte monatliche Gebühren pro Eintrag. Für alle anderen Marktteilnehmer ist LiveRamp kostenlos nutzbar.

NetID

Die Nutzung des Single-Sign-on-Dienstes ist für Partner wie z. B. Online-Publisher kostenlos. Die Stiftung arbeitet nicht profitorientiert. Die laufenden Kosten des Betriebs werden durch kostenpflichtige Angebote gedeckt. Hierunter fallen unter anderem:

- Die aktuell in der Entwicklung befindlichen Produkte und technischen Funktionen, die die Vermarktung und Personalisierung unterstützen. Diese setzen sich aus jährlichen Gebühren und volumenabhängigen Betriebskosten für technische Dienstleister zusammen.
- Fachbeiratsmitgliedschaften (z. B. Publishing/Vermarktung)
- Betrieb und Bereitstellung von Kernkomponenten z. B. für Accountanbieter

Flashtalking – Ftrack

Für die Verwendung von Ftrack in seiner aktuellen Form als Basis des Reportings zahlt der Advertiser. Hierbei handelt es sich um einen Aufschlag auf den technischen TKP für den Adserver.

Zeotap

Bei Zeotap zahlen Advertiser eine Lizenzgebühr für die Nutzung der Plattform und der darin enthaltenen Services. Publisher, die eine Partnerschaft mit Zeotap eingehen, werden in der Regel basierend auf den Identity Linkages (hashed E-Mail zu ID+) vergütet, die sie in den Graphen hineingeben.

Bundesverband Digitale Wirtschaft (BVDW) e.V.

Der Bundesverband Digitale Wirtschaft (BVDW) e.V. ist die Interessenvertretung für Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Als Impulsgeber, Wegweiser und Beschleuniger digitaler Geschäftsmodelle vertritt der BVDW die Interessen der digitalen Wirtschaft gegenüber Politik und Gesellschaft und setzt sich für die Schaffung von Markttransparenz und innovationsfreundlichen Rahmenbedingungen ein. Sein Netzwerk von Experten liefert mit Zahlen, Daten und Fakten Orientierung zu einem zentralen Zukunftsfeld. Neben der DMEXCO und dem Deutschen Digital Award richtet der BVDW eine Vielzahl von Fachveranstaltungen aus. Mit Mitgliedern aus verschiedensten Branchen ist der BVDW die Stimme der digitalen Wirtschaft.

Fokusgruppe Programmatic Advertising

Programmatic Advertising (PA) ist mit zweistelligen Wachstumsraten in Deutschland weiter auf Erfolgskurs. Es ist ein zentraler Erfolgsfaktor im Mediabusiness der Zukunft und einer der wichtigsten Vorteile der digitalen Kanäle im Wettbewerb um die Mediabudgets. Den programmatischen Handel digital adressierbarer Medien in Deutschland weiterzuentwickeln und nachhaltig zu gestalten, ist das Ziel unserer Fokusgruppe Programmatic Advertising. Qualität und Professionalisierung stehen dabei im Fokus. Das Gremium aus Agenturen, Vermarktern, Technologydienstleistern und Plattformanbietern setzt dazu auf segmentübergreifende Zusammenarbeit. Hauptaufgaben sind die Vermittlung der wichtigsten Fachbegriffe, Wirkungsweisen und Methoden, die Entwicklung technischer Standards sowie die Bewertung von Qualitätskriterien und der Einsatz von Daten. Die Fokusgruppe kooperiert zudem mit verschiedenen nationalen und internationalen Partnerverbänden, wie dem IAB Europe, um länderübergreifend Entwicklungen abzustimmen und voranzutreiben.

www.bvdw.org

Online-Vermarkterkreis (OVK) im BVDW

Der Online-Vermarkterkreis (OVK) ist das zentrale Gremium der deutschen Online-Vermarkter. Hier haben sich unter dem Dach des Bundesverbandes Digitale Wirtschaft (BVDW) e.V. 16 der größten deutschen Online-Vermarkter zusammengeschlossen, um der Bedeutung der Online-Werbung kontinuierlich mehr Gewicht zu verleihen.

Oberste Ziele sind die Erhöhung von Markttransparenz und Planungssicherheit sowie Standardisierung und qualitätssichernde Maßnahmen für die gesamte digitale Branche.

Darüber hinaus realisiert der OVK wichtige Projekte wie Kongresse, Studien und Fördermaßnahmen und engagiert sich in nationalen und internationalen Gremien für die Weiterentwicklung der Branche.

www.ovk.de



Impressum

Market Research zum Advertising-Identity-Ökosystem

Erscheinungsort und -datum	Berlin, Mai 2020
Herausgeber	Bundesverband Digitale Wirtschaft (BVDW) e.V. Schumannstraße 2, 10117 Berlin, +49 30 2062186 - 0, info@bvdw.org , www.bvdw.org
Geschäftsführer	Marco Junk
Präsident	Matthias Wahl
Vizepräsidenten	Thomas Duhr, Anke Herbener, Achim Himmelreich, Alexander Kiock, Marco Zingler
Kontakt	Alexandra Treidler, Bereichsleiterin Digital Marketing, treidler@bvdw.org
Vereinsregisternummer	Vereinsregister Düsseldorf VR 8358
Rechtshinweise	Alle in dieser Veröffentlichung enthaltenen Angaben und Informationen wurden vom Bundesverband Digitale Wirtschaft (BVDW) e.V. sorgfältig recherchiert und geprüft. Diese Informationen sind ein Service des Verbandes. Für Richtigkeit, Vollständigkeit und Aktualität können weder der Bundesverband Digitale Wirtschaft (BVDW) e.V. noch die an der Erstellung und Veröffentlichung dieses Werkes beteiligten Unternehmen die Haftung übernehmen. Die Inhalte dieser Veröffentlichung und / oder Verweise auf Inhalte Dritter sind urheberrechtlich geschützt. Jegliche Vervielfältigung von Informationen oder Daten, insbesondere die Verwendung von Texten, Textteilen, Bildmaterial oder sonstigen Inhalten, bedarf der vorherigen Zustimmung durch den Bundesverband Digitale Wirtschaft (BVDW) e.V. bzw. die Rechteinhaber (Dritte).
Ausgabe	Erstausgabe
Titelmotiv	© iStock / ipopba

Die dieser Publikation zugrundeliegende Untersuchung wurde durchgeführt von:
NK & Co. GmbH, www.nkco.de, Borodinstraße 14, 13088 Berlin



Herausgeber

Bundesverband Digitale Wirtschaft (BVDW) e.V.
Schumannstraße 2, 10117 Berlin

+49 30 2062186 - 0, info@bvdw.org, www.bvdw.org