Market research on the advertising identity ecosystem

www.bvdw.org

Market research on the advertising identity ecosystem

Management summary

Regulatory[1] and technical[2] developments are doing away with the established technical foundation (3rd party cookies) for targeted control of digital advertising.

The industry must therefore agree on a new standard by which advertisers, media companies and their technology partners can adhere to existing business models and at the same time meet the consumers' needs for data sovereignty. The central question for all market participants remains the same: How can we maintain the proper addressability of digital advertising?

This BVDW e. V. Bundesverband Digitale Wirtschaft - German Association for the Digital Economy) white paper on the Advertising Identity Ecosystem is based on a study commissioned by the "OVK (Online-Vermarkterkreis) Unit Programmatic & Data" to examine the most widely used technologies and the providers of identity solutions.

Since several browser manufacturers (Firefox, Safari) no longer support 3rd-Party Cookies or Fingerprinting for cross-webpage user tracking or have announced such a restriction (Google Chrome), a special focus of the study was assessing the basic technologies of relevant providers available on the market.

The aim of the study was to generate a complete picture of the different technological approaches under headings such as functionality, security, sustainability, quality of addressability, scalability and neutrality of the providers and thus provide a basis for decision making for users of the technologies.

The current high market dynamics in this area lead us to expect that there will be further new ways of working and new providers in the market in the future. The period covered by the first version of the white paper is between November 2019 and February 2020. In the version under consideration (second version) and its period covered (between March 2020 and September 2021) it is possible and probable that the scope of services offered by some of the vendors considered will expand rapidly. Changes can also be expected with regard to the price overview in the attachment.

Further developments and more in-depth concepts around Advertising Identity, e. g. browser-based targeting possibilities ("Google Sandbox") or the initiative of the IAB - Project Rearc, will be dealt with in more detail in subsequent publications as soon as they are sufficiently specific and available in products. Nor are the technical details of the transmission of Advertising Identity within the programmatic process chain or the possibilities of linking consent management and persistent Advertising Identity (Consented Identity) the focus of the present evaluation.

1 GDPR, e-privacy, EuGH/BGH judgements, data protection authorities
2 Browser as a 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/

Background

For several years it has been on the verge of becoming reality and it is being finalised right now: The 3rd party cookie as an extensively used tool delivering digital forms of targeted and group-based advertising will die out. The browser manufacturers are providing support to the legal developments with technical barriers which are becoming more complex. The goal seems to be to ultimately prevent general “publisher” tracking of users via cookies and similar browser-based storage methods.

This development pays particular attention to the technologies used for marketing: the various ad servers used for delivery, the associated targeting systems and the programmatic systems.

Even with cookies, it was important to create pseudonymised recognition between publisher, browser and device. The 3rd Party Cookie tool was never fully developed, but was widely accepted and therefore became the only one which is commonly utilised. With its coming discontinuation, the opportunity is being opened for a far more wide ranging solution that can overcome more barriers. This brings with it many unknowns. It remains an open question how target group reach and CPMs will develop during and after the transition phase.

Since the first publication of this Market Research in May 2020, a clear development away from 3rd party cookies and fingerprinting can be observed among providers. Furthermore, IAB TCF 2.0 enjoys broad support.

Research

Within the scope of this document, relevant and fully developed identity solution providers were analysed and discussions were held with the providers.

The aim is to create an overview of the world in which these providers operate. What makes them stand out, where do they interact with each other and how can the solutions best be used for the purposes of BVDW members? Beyond that, it is also worthwhile delving a bit deeper. What technical solutions have been used for the products and what are the technical constraints of current developments?

The results have been divided into the main topics into which this document is organised:

- Who are the solution providers?
- How do the solutions work?
- What’s the security like?
- How is the quality to be assessed?
- What scaling has been achieved and how is it developing?
- How is the solution positioned in the market?
- What are the costs of use for market participants?

Results

Brief introduction of the providers

ID5 – Universal ID

ID5 is an identity solution provider founded in 2017. It started with the mission of optimising inefficient cookie syncing. In July 2019, ID5 launched "Universal ID" a privacy-first universal identifier that enables publishers and brands to address users in environments where third-party cookies and MAIDs are blocked.

Unified ID 2.0

The industry-wide, international open source project Unified ID 2.0 was initiated by one of the largest DSPs, The Trade Desk. This framework provides an ID to the ad ecosystem based on hashed and encrypted user email addresses. It is not only solving for the depreciation of the 3rd Party Cookie but is designed as a new identity solution for all digital channels, including mobile, audio and Connected TV. Unified ID 2.0 is already supported by publishers, like the Washington Post and Newsweek, advertisers like Publicis, Omnicom and IPG, data and measurement companies like Nielsen and Comscore, as well as adtech companies, including Criteo, Magnite, Xandr, Index Exchange and Pubmatic.

Roq.ad

Roq.ad was founded in 2015 with the mission to enable device independent addressing of people and target groups in digital marketing.

LiveRamp

Started in 2011, LiveRamp is a data connectivity platform powered by core identity capabilities and an unparalleled network, enabling companies to better connect, control, and activate data. Over the past four years, LiveRamp has been building a fully interoperable and neutral infrastructure, which delivers end-to-end addressability for the ecosystem powered by its Authenticated Traffic Solution (ATS). This solution addresses the deprecation of third-party cookies and other device identifiers, including IDFAs.The infrastructure leverages deterministic people based identity to enable activation and measurement. According to its own information, the company has the third largest reach after Facebook and Google.

netID

The provider of single sign-on and consent management solutions European netID Foundation was founded in March 2018. It was founded in the form of a foundation. The aim of the foundation is, on the one hand, to offer an independent alternative to the SSO (Single Sign On) offerings of Google and Facebook. On the other hand, it aims to enable transparent management of user consents, on the basis of which user data can continue to be used for advertising purposes in compliance with data protection laws.

Flashtalking – FTrack

Flashtalking's mission is to provide a media-independent ad serving and ad analytics platform for advertisers. With FTrack, Flashtalking has a cookie independent ID that Flashtalking uses to measure the delivery of advertising to advertisers. In 2021 Flashtalking launches its new Identity Framework that provides advertisers two methods to resolve identity when using Flashtalking's personalisation and measurement solutions.

ID+ powered by Zeotap

Zeotap was founded in 2014 in Berlin with the vision of building a privacy-first data platform for the digital marketing ecosystem. Until 2021, Zeotap has grown its global team to 200 data-enthusiasts and is backed by leading global investors.

ID+ is a European universal digital marketing solution that aims to resolve identities at scale in the nearing cookieless future dominated by privacy regulations. Supported by publishers, large global brands, and members from the advertising, marketing, and technology ecosystem, Zeotap's ID+ initiative enables this ecosystem to work together to proactively safeguard the future of identity and addressability. Powered by the Zeotap Customer Intelligence Platform and its native third-party identity resolution, ID+ is built on the back of the world's largest high quality identity graph and is available across Europe, the UK, and India. The deterministic graph, with a strong backbone of hashed emails, hashed phone numbers and MAIDs (Mobile Ad IDs), counts over 400M ID-verified/self-declared linkages coupled with unified and curated data profiles.

Operating principles, advantages and disadvantages

Introduction to the underlying technologies

The solutions considered in this document are all based on one of the currently available technical options or a combination of these. The following is a functional explanation:

Cookies

A cookie stores a combination of a key and a value. The value can be any information, encrypted or in plain text. It is often a pseudonymised ID for recognition. If a cookie is written, the domain under which it was written is always included in the cookie. With cookies, a distinction is made between how and in what context they are written/read:

How: **Server side,** context: **1st party**
During the construction of the page www.PublisherA.com various requests from the browser go to the server. The server answers them with the HTML page and e.g. images and CSS files. To each of these answers the server can give the browser an instruction to write a cookie. As long as the server does this at www.PublisherA.com, it is called a 1st-party cookie, which is written on the server side.

How: **Server side,** context: **3rd party**
In addition to the components that are loaded from this server when www.PublisherA.com is called up, third-party systems such as the SSP www.SSP.com are also integrated. For this purpose, the HTML page of www.PublisherA.com contains components that are accessible on the server at www.SSP.com. The browser then retrieves these components. If www.SSP.com answers one of these requests with the instruction to write a cookie, this is called a server-side cookie, which is written in a 3rd-party context. 3rd party, because the user has called www.PublisherA.com and www.SSP.com is a third party from the user's point of view.

How: **Client-side,** context: **1st party only**
In YesvaScript there is the possibility of writing cookies. www.PublisherA.com has integrated a YesvaScript script on its page, which comes from this server. Furthermore www.PublisherA.com has integrated a script from www.SSP.com. Both scripts are able to read and write cookies. All these cookies are 1st-party cookies. So the cookie written by the script from www.SSP.com cannot be read by SSP on www.PublisherB.com. All cookies remain with PublisherA.

In Firefox, access to 3rd party cookies is blocked for trackers listed on the disconnect.me list.

Safari blocks access to 3rd party cookies for trackers. Trackers are recognized by an AI based on certain patterns.

Chrome/Chromium will also restrict access to 3rd party cookies as part of the switch to the Privacy Sandbox.

eTag

eTag stands for "Entity Tag". It is a data field that can be stored in web resources such as HTML pages, scripts or images in the cache of the browser. Similar to a server-side cookie, the server controls the filling of the eTag in the cache via an instruction in the response. The eTag is used for cache validation. Based on the eTag that the server has previously set, it can identify the version of the resource already in the cache. It decides whether it has to send a newer HTML page or a newer image to the browser. If not, it can save bandwidth and send the message "not modified".

The (invisible) picture www.SSP.com/tracker/1x1.gif is integrated in www.PublisherA.com. This way the SSP can put a pseudonymous ID “ABCDEF” into the eTag and thus into the cache of a browser. This browser is used to call www.PublisherB.com, which also includes www.SSP.com/tracker/1x1.gif. The value of the eTag is sent from the cache “ABCDEF” in the browser’s request to the server. The server can use this data field to determine that it is the same browser. The procedure is similar in function to that of a 3rd party cookie. Since an image is used as the storage location of the eTag here, this procedure is also called Image Cache.
A demonstration can be found here: https://lucb1e.com/rp/cookielesscookies/

Authentication Cache

The HTTP protocol offers a so-called Basic Authentication. Here, the browser sends a user name/password combination to the server for authentification when requested by the server. For the first call of a resource protected in this way (for example, pixels on the server), the browser asks the user using a dialog. For all subsequent calls, the username-password combination from the cache is used. Using a combination of server-side implementation and YesvaScript, the dialog for the user can be suppressed and a unique ID can be used as the username-password combination. This can then be used like a cookie-based ID further along in the process. This method can also be used in a 3rd party context and thus across publishers.

This method is dependent on how long the access data is kept in the browser cache.

mobile iOS IDFA / Android GAID

Mobile devices based on iOS or Android offer so-called advertising identifiers. The advertising identifiers are provided by the operating system. The user of the device can deactivate or reset the identifier to render previously collected data unusable. Since iOS 14.5 Apps must use the “App Tracking Transparency“ Framework to request users permission for authorization of cross company tracking.

App developers can scan the identifiers in the app code and use them by following the applicable iOS and Android guidelines for tracking.

The identifiers are device-specific. This means that all ad networks in all apps running on the same device will get the same ID.

In mobile browsers the Advertising IDs are not usable.

Local Storage

Since HTML5 is supported by the relevant browsers, there is the possibility to store data in so-called Local Storage in the browser. If this is done in a 3rd party context, it can be used for cross-publisher tracking in the same way as cookies.

In Firefox, local storage access is generally blocked for trackers listed on the disconnect.me list.
With regard to tracking methods Safari has severely limited the lifetime of local storage data.
Chrome/Chromium will also restrict access to Local Storage as part of the transition to the Privacy Sandbox.

Fingerprinting

For fingerprinting, features are collected and combined in the user's system. The aim is to collect a manageable but high number of attributes. If the attributes on different systems are sufficiently varied, the result is a fingerprint of the system. Specifically, for fingerprinting with regard to tracking via YesvaScript, the following features are used:

- Browser and Version
- Installed plug-ins
- Screen resolution
- Operating system and version
- Installed Fonts

The accuracy with which the same browser can be reliably recognised depends on how many browsers which have the same combination of these attributes.
Mapped to a campaign can mean:

- The frequency cap of the campaign is set to "4 insertions per user per day".
- Two browsers, used by two completely different users, have the same attributes.
- With correct identification, the two users could create 8 ad impressions.
- However, both generate a maximum of 4 ad impressions in the campaign on one day, as they are recognized as one device.

Mozilla plans to restrict the attributes that can be used for fingerprinting in Firefox.
For Chrome/Chromium, changes have been announced in the Privacy Sandbox that will restrict fingerprinting without being specific.
Apple has not announced any concrete plans for Safari so far, but it can be assumed that further developments will follow.
In Safari the fingerprinting defense feature which prevents access to data for fingerprinting is turned on by default.

Login

A login is a highly secure recognition method. A login is considered deterministic.

A login initiates the user´s direct interaction with the system used for the login. Given the user's consent, the login can be used pseudonymously as an ID in order to recognize the user in connected third-party systems. Examples of login-based web services are browser-based e-mail services and social networks. These services use the login directly on their promotions and can also use it for marketing by their partners under the appropriate legal conditions.

Another form of login is the Single Sign-on (SSO). Here the login is forwarded by the provider to other participating websites. From the user perspective, only one login needs to be created. With this login, the user can then easily log in to all promotions that support the SSO. From the provider's perspective, such a solution is better organised because the obstacle of creating an account is replaced by a few confirming clicks when logging in via the SSO for the first time.

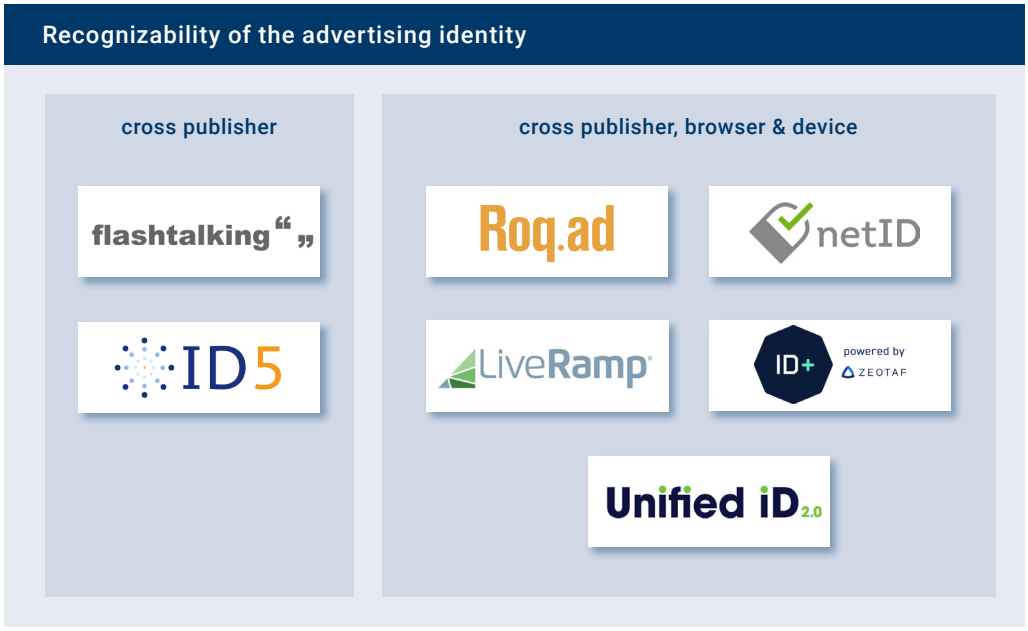
Examples of SSO providers are Facebook and Google as well as the German provider netID, which is discussed in this document.

SUMMARY

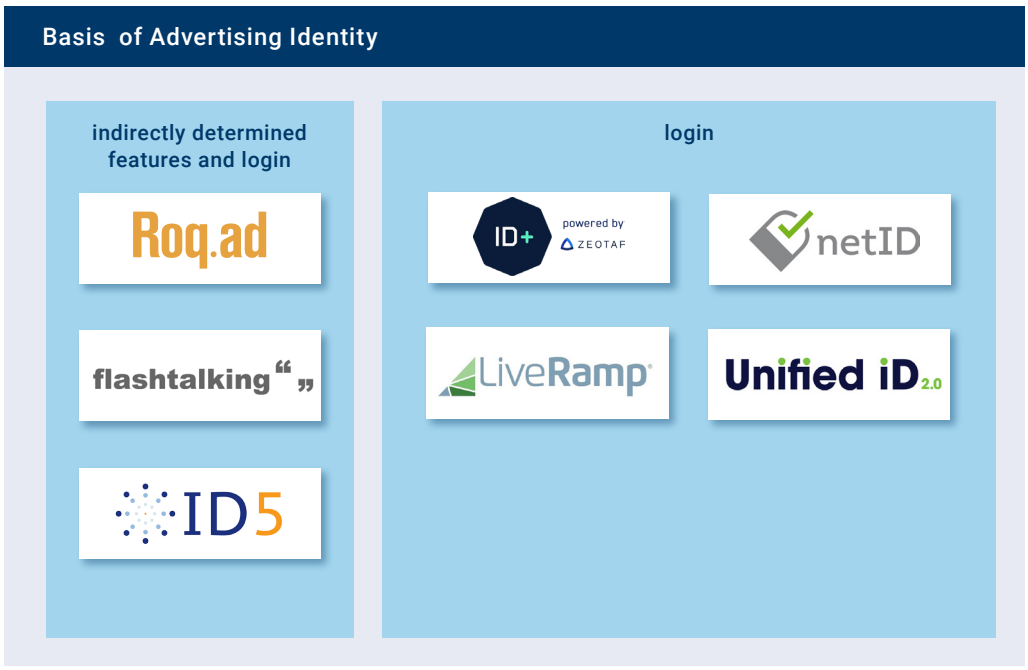
An important aspect when looking at the functioning of the system is the question of the breadth to which the solutions offer recognizability:

1. Cross Publisher Level
2. cross browser and device level across publishers

Here the field of the considered suppliers is broadly diversified.



The data on which the solutions are based can be divided into two groups.



Key features of the solutions at a glance.

	ID5	Roq.ad	Unified ID 2.0	LiveRamp	netID	Flashtalking – FTrack	ID+
Integrated in the Prebid User ID module*	Yes	No	Yes	Yes	Yes	No	Yes
Function dependent on 3rd party cookies	No	No	No	No	No	No	No
Develops solution for 3rd party cookie problems	Yes	Yes	Yes	Yes	Yes	-	Yes
Identification possible in Safari	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Identification possible in Firefox	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CMP for range increase (Soft Login) integrated	No	No	No	Yes	Yes	No	through Partner-ship
Enables frequency capping in the programmatic environment	Yes	Yes	Yes	Yes	Yes	No, not involved in media-buying	Yes
Enables cross device targeting in the programmatic environment	No	Yes	Yes	Yes	Yes	No	Yes
Uses fingerprinting	No	No	No	No	No	No	No

*In addition to Prebid, marketable header bidding solutions from other SSP providers support the integration of the various identity providers and the corresponding transfer of the advertising identity to affiliated technology partners

Details Of The Providers

ID5 – Universal ID

The ID5 Universal ID is a first-party identifier that ID5 provides to its publisher partners when it has users' consent. Publishers share the ID with their monetisation partners, enabling them to address users in all browsers, to frequency cap and to measure the results of their campaigns. To enforce users' privacy choices and to protect publishers' data, ID5 encrypts its ID and provides the description key only to authorised platforms.

To ensure that Universal ID values are consistent across the different websites distributing them to the advertising ecosystem, ID5 uses deterministic or probabilistic methods, depending on what signals are available.

Deterministic
When a publisher can provide signals such as hashed emails or login / SSO IDs, ID5 uses them to anchor consistent identifiers across the websites that have collected them.

Probabilistic
When hashed emails or login / SSO IDs are not available, ID5 processes signals shared via the HTTP Protocol using a proprietary algorithm to infer the uniqueness of a user across websites. This algorithm runs on a combination of information, including the IP address, user agent string, page URL and timestamp of the visit.

User consent is required for these identification methods to comply with data protection regulations.

Authenticated users only count for a small percentage of publishers' traffic. By combining both methods, ID5 can maximise the number of addressable users which benefits both buyers and sellers of data-driven digital advertising.

Publishers can integrate Universal ID via the Prebid User ID Module or the ID5 API.

Unified ID 2.0

The Unified ID 2.0 (UID2) Solution was originally introduced to the market by The Trade Desk mid 2020. The goal is to provide a common technology and concept of a reliable identifier for the programmatic ecosystem, which is able to replace third-party cookies and also provides a reliable identity framework for other digital channels, like audio, Connected TV and mobile. Powered by a secured technology that encrypts and hashes a consumer's email address for their protection, the solution is open source, interoperable and non-commercial.

All partners who support the UID2 use it for transferring and matching this one ID for one user. Matching multiple IDs to one user like in a user graph is not part of the UID2 framework. However The Trade Desk is offering the Adbrain Graph to extend UID2 to MAID/Cookie independently from the UID2 framework for advertisers on their platform. The UID2 is interoperable with other identifiers, such as RampID by LiveRamp and Zeotap ID+. Additionally Advertisers and Publishers can leverage their existing SSO service by simply creating UID2 from consented user email address.

A participating publisher can request the framework to generate a UID2 token to be used with a connected SSP. The publisher will first gather consent from the user and then initiate the generation. When calling the SSP the publisher will provide the UID2 token. This token can then be used by DSPs to match data based on the UID2 in an auction with an appropriate bid.

In detail this process is supported by different roles in the framework. Administrators provide keys to DSPs to decrypt UID2 tokens for bidding. They also send user opt-outs to DSPs to enable them respecting user privacy. Operators generate UID2s for data providers and publishers based on hashed, salted and encrypted emails (consent required). To distribute user opt-outs UID2 tokens need to refreshed by the publishers using refresh tokens. The Transparency and Control Portal provides a central cross-publisher UID2 opt-out to end users. It distributes the opt-out request to the Administrator and Operators. Auditors audit all partners against the code of conduct and provide the results to administrators and operators. All partners using UID2 need to follow the code of conduct governed by an independent body. While The Trade Desk has built the initial code base, operational responsibility is being migrated to an independent organization and the relevant code is currently being open sourced by the IAB Tech Lab.

Prebid will serve as one of the operators for UID2 in the United States.

The unified ID 2.0 was submitted to the Partnership for Responsible Addressable Media (PRAM) for review in January 2021. As a key member of PRAM, the IAB Tech Lab has also provided extensive feedback on the UID2 framework and will be managing feedback on UID2's open source code moving forward.

Roq.ad

The underlying technology is based on a proprietary cross-device, cross-publisher graph developed by Roq.ad. The Roq.ad solution ingests whatever identifiers it sees from its data partners, analyses the profiles of those IDs and where/when they were seen online in order to map them together to represent a person, without need for any login data from clients. Historically, the tool has leveraged cookies, Mobile device IDs (MAIDs), and Connected TV IDs as it's core identifiers; with the reduction in MAIDs from Apple's addition of AppTrackingTransparency in iOS 14.5 and Google's announced depreciation of 3rd party cookies, the number and type of IDs Roq.ad maps is likely to increase significantly, and could include: Publisher IDs, First-Party cookies, email token IDs across multiple vendors, ioT device IDs, etc.

Somewhat different than other providers in the market, Roqad does not push a "Roqad ID" as a transactable currency for the industry (though it could be used that way). Instead they endeavour to give all of their clients all of the IDs they see mapped to their customers' first party data.

Deterministic data are used as a training dataset to help teach the Roq.ad algorithm the appropriate matches. For example, encrypted user names or e-mail addresses tied to IDs can be used to identify successful pairs built by the algorithm and weigh characteristics used to determine that match more highly in future matching. For the probabilistic procedure, more loosely defined attributes such as encrypted and shortened IP addresses, time stamps, geolocation data sets, internet service providers and many other attributes are used. On this basis, assumptions are made as to the probability of several device identifiers being the same person. Online, mobile and also offline data can be used. The probabilistic approach is also generally regarded as very stable in discussions with other market participants if the probability threshold is set high enough.

Roq.ad uses tags that enable web and mobile apps to be identified. Roq.ad's primary customer base is ad buying platforms and data providers. It is also used by AdNetworks, AdServers, SSPs, major publishers, brands, and eCommerce companies. As noted above, Roqad does not intend to be an "industry currency," and as such does not require outreach to or buy-in from non-customer publishers. Roq.ad expects those publishers to choose whichever stable ID they have access to, and deliver it to the industry. From there, Roq.ad will map it with all other known, stable IDs for that person.

Use cases such as cross-device (i) remarketing, (ii) audience amplification and (iii) storytelling in Programmatic Advertising are fully supported via Roq.ad's partner integrations in market leading demand side platforms and ad servers such as The Trade Desk, AppNexus, ActiveAgent, Adition, Flashtalking and many more.

As a graph-based system, the Roq.ad ID is less affected by cookie restrictions, and without third party cookies, are likely to see higher scale than deterministic providers.

LiveRamp

Their omnichannel solution is not dependent on third-party cookies or device-based identifiers; therefore it is not affected by cookie deprecation in Firefox and Safari, and soon, Chrome. LiveRamp connects authenticated publisher inventory to marketer demand through its Authenticated Traffic Solution (ATS), which is deployed by publishers. When an individual signs in, ATS hashes a piece of personal information such as their email or phone number, finds a corresponding RampID (LiveRamp's pseudonymous, people-based identifier), then additionally encrypts and returns it to the publisher in an „envelope." Hashed data is deleted immediately after system lookup. The SSP receives and decrypts the envelope then uniquely encodes RampIDs for each DSP.

LiveRamp incorporates all devices they conclude with a high degree of probability are assigned to the same person. According to LiveRamp, their identity solution provides a neutral, stable ID for consumers — independent of device and in compliance with all EU data protection regulations.

LiveRamp works exclusively deterministically. Only absolute data is included in the recognition process. Recognition via IP addresses and the like are not performed.

LiveRamp offers Privacy Manager, a consent management platform with ATS, making it easier for publishers to meet consent requirements set by GDPR. The use of LiveRamp's own CMP is not necessary so long as the publisher has a CMP in use, which can output the TCF Consent String. LiveRamp also offers publishers the use of a registration wall, an analytics dashboard, and a host of other tools to aid in navigating the post-cookie world.

For publishers, it is very easy to activate ATS via JavaScript, but a server-side module can also be used. (For example, ATS can be activated via the Prebid ID module, via the Index Exchange wrapper and, on request, via other connected SSPs).

netID

In addition to its single sign-on netID offers a consent and ID management solution, which from the perspective of advertising marketing can be used for addressing target groups across publishers and devices.

netID accounts can be created by the user via one of the netID account providers (e.g. Web.de, Gmx.de and in future also Deutsche Telekom). New registrations using any e-mail address are also supported via netid.de. The use of netID is very easy, because already existing accounts with account providers can be used directly for netID. With netID Partners users usually choose between the proprietary login of the partner and the Single Sign-on of netID. If netID is utilised the user can hereafter tap into the partner's products with his netID account and naturally, with the same login data. Significant obstacles such as repeated selection and the remembering of passwords or the filling out of long forms for the login on a website are hereby overcome. The legal basis for this SSO is always clarified and kept uniform across all partners. A Privacy Center gives the user centralised control over his login, his data and their use.

The user can agree to a transfer of data to a partner - always on the basis of the partner's data protection regulations. For a publisher/website operator that supports netID this means that they can request the e-mail address of the user in this way, e.g. for newsletter mailings.

From a marketing perspective, the Publisher could use the pseudonymized e-mail address as an ID for targeting or frequency capping. However, this type of data usage is not legally allowed based on the SSO service. The usage regarding these use cases is supported by a stable netID identifier which is bound to a permission, whereby the permission can be obtained by means of the corresponding consent management products of netID. netID is generally not a direct partner in the marketing chain at any point. It offers technical interfaces to publishers/website operators to interact with netID Users. The use of these interfaces, or more precisely, the data, is the responsibility of the publisher. Also the related data protection requirements, such as obtaining the users' consent for commercial data processing, lies with the publisher. However, netID standardises these for its users/partners.

Among other things, netID's consent management products support TCF 2.0-based consent management platforms (CMPs), which also allow for the use of data for advertising purposes. The integration of this platform with the user's central Privacy Center offers a high degree of control over data usage. The consent / transparency status, e.g. for the purpose of advertising, is managed individually for each publisher. However, the user is provided with an overview. The CMP integration is also accompanied by a so-called soft login which for identifying the user and managing his general consent / transparency status does not require registration (incl. master data transfer) with the publisher Parallel to this, the identification of the user and also the administration of the consent / transparency status based on an SSO login (hard login) with the partner is always possible.

Flashtalking – FTrack / Identity Framework

Flashtalking offers ad serving solutions to the advertiser. Usually Flashtalking delivers the ads as redirect through its own infrastructure. This provides many points of contact with the user's device - these can then be used as deterministic anchor points for enriching the probabilistic algorithm.

Flashtalking does not offer media buying technologies, but focuses on independent measurement of the delivery of campaigns and deals (cookieless reach and frequency as well as the right allocation of conversions) – its cookieless technology is furthermore used for cookieless Re-Messaging, Sequencing and other mechanisms that help delivering the right message in a given situation according to the communication-strategy.

With FTrack ID, Flashtalking has created the basis for attribution analysis and campaign reporting. Based on this data, Flashtalking offers a comparison to the reports generated by the DSP or SSP side.

Based on the deterministic signals transmitted by the browser and processed by FTrack in a probabilistic way, FTrack technology is able to recognize browsers and devices with a very high degree of probability. Due to the methods used, FTrack represents a replacement for cookies and is therefore not affected by the limitations of cookie processing. For a cross-device analysis (as a basis for their attribution solution) Flashtalking works together with other providers (e.g. Roq.ad). The device matching rates are significantly increased by using FTrack technology.

FTrack is not fingerprinting. While the FTrack technology leverages several data signals, it does not collect personally-identifiable or sensitive data from a user's device. Flashtalking does not use any opaque or hidden techniques. With the increasing focus on privacy in the evolving ad tech ecosystem, Flashtalking continues to ensure that they natively include consumer notice and choice in all ads served by Flashtalking. They provide consumers with the

option to opt out of interest-based creative personalisation and all tracking (both cookie-based and cookieless) with ease.

Flashtalking never builds user profiles, sells user behaviour data, monetises user data "in the bid stream" or shares or combines user data across clients.

In 2021 Flashtalking launches its new Identity Framework:

Flashtalking's new Identity Framework provides advertisers two methods to resolve identity when using Flashtalking's personalization and measurement solutions:

1. Identity Resolution Service:
This option inputs various identity signals (such as device IDs and third-party IDs) and reconciles them to a single device FTrack ID. Flashtalking's FTrack ID is then carried through the framework to all downstream personalization and measurement services.
2. Partner Identity Service:
The second option onboards a single partner ID of the advertiser's choice (e.g. advertiser user ID, purchased ID or industry standard ID), and then carry it through the framework to all downstream personalisation and measurement services.

ID+ powered by Zeotap

Zeotap is a Customer Intelligence Platform (CIP) that helps companies better understand their customers and predict behaviours, to invest in more meaningful experiences. Zeotap enables brands to build on a nucleus of first-party data to win new customers and grow their loyal base. The independent but integrated modules include customer data unification, identity resolution, enrichment, analytics/modeling, and activation to 100+ partners in the marketing ecosystem.

Recognized by Gartner as a „Cool Vendor" (2020), by AdExchanger as the "Best Data-Enabling Technology" (2019), and by G2 as a leader in Spring 2021 the platform meets the highest enterprise data privacy and security standards, including GDPR, ISO 27001, and CSA STAR. Zeotap serves the world's top brands, agencies, and publishers across Europe and India.

ID+ is an embedded component into the Zeotap Customer Intelligence Platform and allows its clients for "walled garden-like" activation across participating publishers in the open web. The ID+ solution is independent of third party cookies, and therefore provides a unique opportunity for publishers to create addressable media inventory in browsers such as Safari or Firefox today as well as Chrome in the near future.

The ID+ ties back into the deterministic Zeotap identity graph, ultimately linking multiple identities to the same person. ID+ matches to the ID graph are based on hashed identifiers used for user authentication on the publisher properties (most commonly, hashed email and hashed phone number).

Safety

Summary

All the providers considered rely on infrastructure in the EU. With regard to the use of personal data, all providers are highly sensitive to that matter. The majority of providers obtain the Consent according to the IAB Transparency and Consent Framework. All providers use at least one hashed value for the ID used. In some cases, IDs are encrypted once or even multiple times using public/private key procedures.

The following is an overview of some of the essential features in the area of security.

	Infra-structure in Germany	Infra-structure in EU	Invokes legitimate interest in EU	Personal data are processed	ID hashed	ID encrypted	ID encrypted several times
ID5	Yes	Yes	No	Yes	Yes	Yes	Yes
Unfied ID 2.0	-	Planned	No	Yes	Yes	Yes	Optional*
Roq.ad	Yes	Yes	No	Yes	-	Yes	No
LiveRamp	-	Yes	No	Yes	Yes	Yes	Yes
netID	Yes	Yes	Not for identification of the user	Yes	-	No	No
Flashtalking - FTrack	No	Yes	No, just explicit consent via TCF2.0	No	Yes	Yes	No
ID+	No	Yes	No, only with explicit consent	Yes	Yes	Yes	Yes

* Can be enabled with Double Encryption for Publishers

Details of the providers

ID5

The ID5 ID is a pseudonymous identifier that is encrypted using a hierarchical encryption algorithm. The algorithm makes it only decryptable by platforms that have both up-to-date decryption keys (provided by ID5) and have user consent to process data for the request. This allows ID5 to enforce consumer privacy preferences rather than just relying on platforms to manage usage of the ID based on their own reading of consent preferences. Users can opt-out of ID5 completely or exercise their consumer rights via the ID5 Privacy Preferences Center. When a consumer opts out of ID5, their ID is reset and unlinked, preventing it from ever being used by ID5 or any other platform that holds data tied to the ID. Moreover, the TCF consent signals are respected in order to comply with the privacy decisions of the users.
ID5 has data centres located in France and Germany.

Unified ID 2.0

UID2 addresses the broader aspects of safety in multiple ways. First of all UID2 is an open source project. Thus a broad review of the used concepts and technology will be possible. On the ID level UID2 is using SHA256 combined with a secret salt to make it close to impossible to reengineer the PII involved. The salt is changed every 12 months. The resulting ID is called the raw UID2. From a user's perspective UID2 provides a central and (publisher-) global way to opt-out. The users will be able to manage the opt-out through the Transparency and Control Portal. Thereby a central distribution of the opt-out signal to all participating parties is possible.

To further secure the ID from leaking the UID2 is not spread through the ecosystem. On the supply side a publisher handles UID2 tokens which are encrypted raw UID2s. By using nonces in this process no two UID2 tokens for one user look the same. On the buy side involved parties will get the keys to decrypt the tokens and be able to match the raw UID2 against data.All involved parties are bound to a code of conduct which has to be followed. Independent auditing bodies will make sure they are followed. For example in terms of correctly handling user consent before sending PII into the ecosystem.

Roq.ad

The Graph UserID used by Roq.ad is stored on the server side. Roq.ad uses e.g. hashed e-mail addresses and usernames as a training dataset for the probabilistic data algorithm. For the data processing on which the solution is based, Roq.ad uses the IAB Transparency and Consent Framework (TCF) to obtain user consent. The infrastructure used by Roq.ad to support European operations is located in the EU, while North American operations are supported by US-based infrastructure.

LiveRamp

To generate a RampID, LiveRamp uses a JavaScript in the browser during a publisher's ATS integration. A piece of consented, first-party data, such as an email address is hashed and passed to the JavaScript. This is translated by LiveRamp into their pseudonymous, people-based identifier, RampID, encrypted and translated on the server-side by an API into an „envelope." This envelope is unique for each request and allows only the publisher access to it by storing it in a first-party cookie (alternatively HTML5 local storage). For programmatic advertising, SSPs are able to read the encrypted envelope via the „sidecar" appliance, SSPs decrypt the envelope and returns specifically encrypted RampIDs for each of the DSPs to be addressed. If LiveRamp provides these DSPs with advertiser or third-party data (via server-to-server or API), they receive „their" encrypted RampIDs again. This allows DSPs to place bids on the bid requests. LiveRamp does not allow for re-identification of the user. According to LiveRamp, no personal data is logged by LiveRamp. As described above, hashed data is immediately deleted once it is matched to a pseudonymized identifier. Additionally, any personal data LiveRamp connects with is provided by publishers and advertisers with appropriate consent gained from users. LiveRamp has integrated a universal opt-out with their identity solution. LiveRamp uses Google Cloud components in Brussels as infrastructure.

netID

netID exclusively uses infrastructure in the EU to operate its solutions. With netID, the user is always able to decide which data which netID partner for which processing purpose receives from him. In addition the user has the option of always checking centrally with his account provider which data releases he has given so far. Partners can request these data from the user via the SSO, the user can agree to the transfer permanently and revoke it later. The identification of a user for advertising purposes / personalization, based on his netID, only takes place with his consent. For the SSO process and other interfaces, netID opens a login session for every netID user, which is stored in a first party cookie. In this way, it is possible for partners to access the released data. The Partner/Publisher who uses netID is responsible within the scope of the applicable data protection guidelines for how and for what purposes he uses the User data.

Flashtalking – FTrack

FTrack is active vendor on the IAB Transparency and Consent Framework. FTrack is only used in the event of user consent. No personal data is processed within the framework of FTrack. The data that is processed is used hashed.

ID+ powered by Zeotap

The Zeotap ID+ is based on successful user authentication on the publisher website. An authentication event can be a user sign in, a registration for a newsletter or a soft-login through a CMP or based on the use of a login-wall technology.

The ID+ solution uses an easy to integrate Javascript to hash the first-party identifier (email or phone number) before securely transferring it to the Zeotap ID+ server. The hashed email or phone number is then looked up in the high quality Zeotap identity graph. Based on a successful match a pseudonymous, tokenised ID+ (an ID which is specific to the user and publisher) is generated and returned to the publisher. Hashed user identifiers received are deleted right after the matching process (in case of ID+ Basic). The publisher- and user-specific ID+ is stored in a first-party cookie allowing only the publisher to access it.

Personal user data (even though pseudonymized) can only be used for ID+ matching after the user has provided explicit consent for the respective purposes and data transfers. Zeotap is able to consume consent signals from all leading Consent Management Platforms based on TCF 2.0 or similar GDPR compliant language.

For European publishers, all data remains within the EU at all times as data matching is executed on Zeotap ID+ servers located in Europe. ID+ agreements are executed with Zeotap - a German legal entity within Europe. In terms of enabling “walled garden-like” transactions in the programmatic ecosystem, the ID+ solution isn’t only integrated with publishers but also SSPs. ID+ enabled SSPs have a specific Zeotap ID+ translation system embedded in their technology stack. This solution decrypts the publisher-specific ID+ token and then re-encrypts it for the participating DSPs in near-real time. This translation mechanism ensures DSPs can execute programmatic bids based on ID+ segments which have been previously shared by Zeotap CIP clients. At the same time, user privacy is protected by multiple layers of security to prevent uncontrolled tracking and build up of behavioural user profiles.

Zeotap holds several certifications for privacy and security:

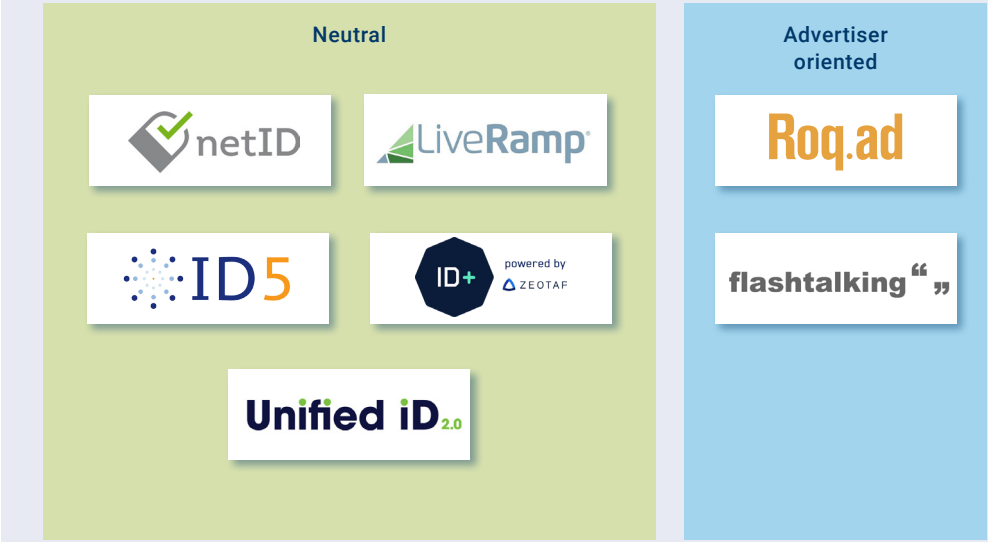
- ISO/IEC 27001 (information security management)
- CSA STAR (Cloud Security) e-Privacy GDPR-ready seal
- CIPT (Certified Information Privacy Technologist)
- CISSP (one of the most sought-after and elite certifications in the information security industry)
- CCISO (Certified Chief Information Security Officer)

Neutrality

Summary

The providers considered position themselves partly neutrally and partly on the advertiser/ buyer side. The providers usually advocate a collaborative development of the Advertising Identity Ecosystem. They usually assume a scenario in which several identity providers co-exist in the market.

Overview of rough positioning of providers in terms of neutrality



Comparison of the providers

ID5 – Universal ID

ID5 was founded in 2017 with the goal to provide identity solutions to the digital advertising ecosystem. ID5 aims to remain a neutral party in the ecosystem by avoiding any conflict of interest with their clients and partners. As such, they do not buy or sell media or data, build user profiles, or use the data generated via their service for any purpose other than providing an identity product. ID5 advocates cooperation between themselves and the other identity providers in their field. The core of the ID5 technology is closed source and proprietary, but the client-side code required for publishers and brands to integrate is open-sourced and maintained by ID5. ID5 is an active participant in Prebid.js to foster the development of the User ID module and ensure a healthy and compliant marketplace.

Unified ID 2.0

The UID2 is an open industry initiative, not a proprietary Trade Desk offering. As a underlaying tech fabric, the UID2 can be adopted by all sides of the advertising ecosystem. Participants will agree to a code of conduct as well as audits. Foundational to this code of conduct is that members may never transact on the ID outside of the encrypted transmission system. Ongoing access to encryption keys will require compliance with the code of conduct. A governing body will regularly audit participating ad tech companies. That's why UID2 is considered a neutral solution by design.

Roq.ad

Roqad's solution serves ad buying platforms, data brokerages, sell side providers, major publishers, brands, and ecommerce companies. Roq.ad's graphs give advertisers the opportunity to reach a more precise target group by matching different identifiers from different devices to people and households. The solution is a closed-source implementation that uses machine learning to calculate the graph

LiveRamp

LiveRamp is a neutral, interoperable player in the market. LiveRamp is equally interested in both advertiser and publisher sides, entering into partnership to increase the reach and accessibility of its infrastructure. LiveRamp is not involved in the media business, but sees its solution as a basis for those who need to resolve data from disparate sources in order to reach audiences and measure outcomes in the digital advertising space.

netID

NetID was established as a foundation to create the most neutral market solutions possible for the topics of login and consent management or cookie-independent user targeting. NetID itself positions itself as a data protection service for users and also as a partner and enabler for website operators (First Parties) on the publisher and advertiser side. They are not involved in the media business.

Data processing beyond Login and consent management in marketing is always in the sovereignty of the website operator. Any technical functions or integrations offered are always offered to the publisher for use in the context of his projects. NetID does not aim at a direct involvement in the marketing chain.

Flashtalking – FTrack

FTrack is currently clearly positioned on the advertiser side. The solution is closed source. Flashtalking is not involved in buying the reach like DSPs. The ad server delivers on space purchased from third parties and measures the results. This puts Flashtalking in a neutral position. Flashtalking is therefore in a neutral position with regard to a rollout of FTrack as an ID for the Advertising ID Ecosystem, which has not been ruled out but is not specifically planned.

ID+ powered by Zeotap

Zeotap's universal ID solution ID+ has been founded as an interoperable open initiative for the digital marketing ecosystem. The primary objective of ID+ has been to enable Zeotap CIP clients to deterministically reach their users across the open web in a cookieless future. At the same time, ID+ is set up to connect the publishers and advertisers in the best possible way.

Quality

Introduction

The solutions can be roughly divided into two underlying approaches.

Deterministic

A solution based on deterministic data will always use absolute data as far as possible. Specifically, for the providers analyzed here, this means e-mail addresses or users/login names. These are used as ID on a hash basis. For this purpose, they are stored in the browser and passed on to the marketing chain, for example to the ad server or via the SSP in the bidrequest.

Deterministic methods are very accurate in the recognition of persons. This also happens across browsers, devices and apps. Wherever the same hash is found again, it can be assumed with high probability that it is the same person. Only when several people use the same login, the accuracy is reduced.

A major disadvantage of a deterministic method is the range. It depends directly on the frequency of the login. In discussions with providers, a login rate of 5% was mentioned as currently high.

Another drawback is a potential loss of accuracy through family use of a login, such as on Apple TV. Providers such as Apple or Google take countermeasures on the operating system side by enabling easy switching of profiles.

Probabilistic & deterministic mixed

This approach adds a component to the deterministic approach described above. The probabilistic approach uses indirect data. In the mixed approach, indirect data that does not originate directly from the user is always used if no e-mail addresses or login data is available. In the context of this research, examples of data used include shortened IP addresses, time stamps, geo-location data sets and Internet service provider information. In concrete terms, this can be used as follows: For example, an identity solution records two accesses to different publishers with the same IP address within an acceptable time window. This is saved in the graph as one data point. With time, additional data points are added. From a certain amount of data points on, the identity solution can link the different accesses and classify them as originating from one person or household.

The probabilistic approach has a higher likelihood of error than the deterministic approach. How high this error probability is can be varied in the solutions considered. If the user of the system is willing to accept a higher likelihood of error, this is accompanied by a higher addressable range. In the opposite case, the range decreases. On the one hand, an error manifests itself in the recognition of several persons, although it is actually only one. On the other hand, two different persons can be classified as only one. In the case of a combination of deterministic and probabilistic approaches in one system, ranges can generally be opened up via the probabilistic approach that would not be addressable only deterministically.

Comparison of the providers

ID5 – Universal ID

ID5 ensures that Universal ID values are consistent across the different websites distributing them to the advertising ecosystem. ID5 links user IDs across domains using deterministic or probabilistic methods, depending on what signals are available.

"Hard signals" used to power deterministic linkage are generally rare. By combining both methods, ID5 can maximise the number of identifiable users which benefits both buyers and sellers of data-driven digital advertising. When "hard signals" are passed in the Universal ID request, they take priority for cross-domain linkage purposes. ID5 performs a real-time look-up for the value provided and returns the ID5 ID that was already associated with that value. If the value doesn't exist in the ID5 database, a new ID5 Universal ID is created and provided in the response. ID5 requires sha256 hashing & base64 encoding to ensure that personally identifiable information isn't transmitted in the Universal ID call.

When "hard signals" are not available, ID5 processes "soft signals" using a proprietary algorithm to determine the chances that a user has already been attributed a Universal ID value. This algorithm runs on a combination of information, including the IP address, user agent string, page URL and timestamp of the visit, and operates within a 95% confidence interval.

ID5 indicates which method was used to link the ID in a field called "linkType" that is made available in the ID object returned by ID5. This can help platforms make optimization or targeting decisions based on the accuracy requirements they may have.

Unified ID 2.0

UID2 is based on a purely deterministic concept. All forms of the UID2 used in the ecosystem are based on deterministic personal identifiable information. The UID2 framework aims to solve the problem of transporting an advertising ID securely and reliable through the whole advertising ecosystems, while giving consumers maximum transparency and control. To make it future-proof it is designed to be completely independent of third party cookies. This also means that the UID2 will work in all environments like desktop, mobile, apps, Connected TV and browsers. Coverage will rely on the industry adoption of the UID2. Any identity solution will only have as much reach as it has logged in users. As more publishers join the initiative, the coverage is instantly and continuously growing, because existing email addresses,

which the publisher may already have together with user consent, can immediately generate UIDs. To help grow this base amongst publishers, which do not collect email addresses from users so far, The Trade Desk and Criteo are collaborating on a single sign on solution called OpenPass. This will be one way to offer the enduser a convenient way to log in to a publishers page. However, using the UID2 does not depend on using a specific SSO solution, because the initiative aims at being interoperable with most leading SSO solutions. Partners can use a proprietary login a SSO of their choice or OpenPass to collect the PII needed for generating UID2. UID2's open and interoperable approach with other leading ID solutions has also been a key factor in generating scale during the initial US beta period.

Roq.ad

Roq.ad offers a fully GDPR compliant, 2-way consented TCF (Transparency Consent Framework) Public Graphmodel and a customized Private Graphmodel. The precision in assigning multiple devices to one person can be reduced in favour of a higher recall rate. In this case, the range is increased while the accuracy of hits decreases. If the targeted precision is increased, the target group range is reduced. In the Private Graph, the precision rate can be adjusted according to customer requirements. Typical precision rates are between 85 % and 95 % depending on the target. In the Public Graphmodel, 2 graphs per country are always calculated every 48 hours: a precision-optimized graph and a reach-optimized graph. In the precision-optimized graph, the precision rate is 91 % with a 30 % recall. The range-optimized graph is 85% precision with 65% recall.

LiveRamp

LiveRamp's solution leverages its deterministic offline identity to create an infrastructure to connect publishers and markets. They are therefore dependent on first-party data from the publisher's side. In principle, they are not affected by the limitations of cookies. Widely used on a sufficient database basis (publisher integrations), LiveRamp promises to offer a secure matching in all browsers across all publishers and devices.

netID

netID's login/single sign-on solution is 100% deterministic. If a user is logged in, an identity is present which can be used with the user's consent. If the user does not log in, he is unknown to netID and the website operator. NetID restricts its own solution to this procedure, but leaves it up to the publisher to use the available user data in connection with other identity solutions, which offer e.g. graphs, in order to increase the reach.

Flashtalking – FTrack

The cookie replacement FTrack works with probabilistic algorithms based on deterministic anchor points. Personal information is not used here. According to Flashtalking, the precision of the solution is >90 %.

ID+ powered by Zeotap

The underlying identity graph powering Zeotap's ID+ solution is 100% deterministic. From a publisher perspective, the ID+ solution is fueled by first-party identities from authenticated users to create addressable media inventory. On the other side, advertisers match their first-party client base to the ID+ graph to execute successful audience based targeting campaigns. This privacy-centric mechanism replicates known functionality from walled gardens and makes it accessible at scale to the open web.

Relevance

Details of the providers

ID5 – Universal ID

ID5 today sees 200 million unique users of Universal ID per month in Germany. ID5 is active with numerous German publishers, such as Gutefrage, MSO Digital, Meinestadt, Finya and Quarter Media, as well as partner platforms, like Aniview, Setupad, and NetworkN.

On the supply side, ID5 is supported by over 40 SSPs, including Pubmatic, YieldLab, Smart, Magnite, OpenX, Improve Digital, Adform, Bidswitch, and inMobi. On the buy-side, ID5 is integrated with Adform, Platform161, Avocet, MediaMath (Q3 2021), and Adition (Q3 2021). ID5 also works with data platforms such as Eyeota, Tapad, Sharethis, Mediarithmics, Piano, and YouGov.

Unified ID 2.0

UID2 started with a beta phase mid March 2021 in the US and APAC. In May 2021, 170 Million people were already associated with a UID2. The global rollout of UID2 is expected in H2 2021. Identity and Data Partners like Tapad, Neustar, Kochava, Epsilon, LiveRamp, Nielsen, comscore and Oracle will adopt the solution. DSPs like Criteo & Xandr, SSPs like Magnite, Pubmatic Index Exchange, SpotX, OpenX are supporting the UID2. The independent industry organisation Prebid will serve as one of the Operators for UID2 in the USA. The Trade Desk is in final talks with an independent industry body about taking over the role as administrator for UID2.

Roq.ad

Roq.ad's cross-device identity graphs are focused on Europe and North America, including an 80% market share of German online users and 60% of North American users. Roq.ad is supported by market-leading demand side platforms (DSPs), data providers, and ad servers such as The Trade Desk, AppNexus, ActiveAgent, Adition, Knorex, Flashtalking, ShareThis, eyeota, and many more.

LiveRamp

LiveRamp entered the German market at the end of 2019 and has since extended its connectivity capabilities into the walled gardens through unique partnerships enabling activation and measurement of data on RampID, as opposed to advertisers' first-party data. LiveRamp has an offline identity graph with coverage of 40+ million adults and is continuing to extend that reach across the open internet via their Authenticated Traffic Solution (ATS).

Since entering the German market, LiveRamp has integrated with key local adtech platforms such as Virtual Minds, and publishers (e.g., Burda Media) in addition to the global and European publisher and adtech platform ecosystem. LiveRamp's identity infrastructure supports The Trade Desk's Unified ID 2.0—and will continue to support other ID solutions—making it simpler for publishers and advertisers to connect data for media activation.

netID

netID reports a potential of 38 million active users per month across all connected partners/ account providers. Currently, they have more than 100 partners, most of which are online publishers, ecommerce providers and TV portals.

Account providers and users of the SSO are the founding members of the foundation web.de, GMX, 7Pass, 1und1 and, shortly, Deutsche Telekom. Partners using the SSO include C&A, DPD, Prosieben.de, Kabel1.de or the Süddeutsche Zeitung.

Flashtalking – FTrack

On a campaign basis Flashtalking FTrack works with other providers on the advertiser side. Roq.ad, Tapad or other device graph providers, which provide cross-device reporting as a basis for cross-channel attribution.

ID+ powered by Zeotap

Zeotap's Customer Intelligence Platform and the ID+ solution are available across Europe (Germany, Austria, Switzerland, UK, Italy, Spain and France) and India with over 60 leading European publishers as well as global SSPs and DSPs already on board.

Appendix

Survey period

The first version of study was conducted from November 2019 to January 2020. In the version under consideration (second version) and its period covered (between March 2020 and September 2021) reflects the state of the art at that time. All further technical changes from that date will be reviewed by the working group and made available with reference to this study.

Costs and price models

Summary

An overview of the main aspects of costs per provider

	Publisher	SSP	DSP	Advertiser	Membership required
ID5	No	No	Yes	No	No
Unified ID 2.0	No	No	No	No	No*
Roq.ad	Yes	Yes	Yes	Yes	No
LiveRamp	No	No	No	Yes	No
netID	Marketing products: Yes only SSO: No	No	No	No	No
Flashtalking - FTrack	No	No	No	Yes	No
ID+	No	No	No	Yes	No

* Participating companies are required to sign and adhere to a Code of Conduct.

Details of the provider

ID5 – Universal ID

The ID5 Universal ID is free of charge for publishers, brands, and SSPs who pass the encrypted ID in bid requests. Platforms that need to use and decrypt the ID, such as DSPs or data platforms, pay a monthly license fee.

Unified ID 2.0

The UID2 is an open source non commercial solution. No central license or usage fee applies to incorporating it.

Roq.ad

Roq.ad's pricing model is based on a software-as-a-service model for all market participants starting with a flat fee (depending on traffic volume) at 4000 € per month.

LiveRamp

LiveRamp is financed exclusively by the advertisers. The model is based on staggered monthly fees per entry. For all other market participants LiveRamp can be used free of charge.

netID

Use of the single sign-on service is free of charge for partners such as online publishers. The foundation does not work on a profit-oriented basis. The running costs of the operation are covered by paid services. These include, among others:

- The products and technical functions that support marketing and personalization. These consist of annual fees and volume-based operating costs for technical service providers.
- Expert advisory board memberships (e.g. publishing/marketing)
- Operation and deployment of core components e.g. for account providers

Flashtalking – FTrack

The advertiser pays for the use of FTrack in its current form as the basis for reporting. This is a surcharge on the technical CPM for the ad server.

ID+ powered by Zeotap

At Zeotap, advertisers pay a license fee for the use of the platform and the services it contains. Publishers pay no fee and earn additional revenue by pushing data through the graph. Publishers who partner with Zeotap are typically paid based on the identity linkages (hashed email to ID+) that they bring to the graph.

Bundesverband Digitale Wirtschaft (BVDW) e.V.

The German Association for the Digital Economy (BVDW) is the central body for the representation of interests of companies that operate digital business models and whose value creation is based on the implementation of digital technologies. As the driving force, guide and accelerator of digital business models, the BVDW represents the interests of the digital economy towards politics and society and campaigns for the creation of market transparency and framework conditions that encourage innovation. With figures, data and facts, its network of experts provides orientation for a central area of the future. Besides DMEXCO and the German Digital Award, the BVDW organizes a multitude of professional events. With members from many different industries, the BVDW is the voice of the digital economy.

Programmatic Advertising Focus Group

Programmatic Advertising (PA) continues to be on course for success in Germany with double-digit growth rates. It is a central success factor in the media business of the future and one of the most important advantages of digital channels when competing for media budgets. The goal of our focus group Programmatic Advertising is to further develop and sustainably shape the programmatic trade of digitally addressable media in Germany. Here, the focus is on quality and professionalization. To this end, the committee of agencies, marketers, technology service providers and platform providers focuses on cross-segment cooperation. The main tasks are the communication of the most important technical terms, effectiveness and methods, the development of technical standards as well as the evaluation of quality criteria and the use of data. The focus group also cooperates with various national and international partner associations, such as IAB Europe, in order to coordinate and promote transnational developments.

www.bvdw.org

Online-Vermarkterkreis (OVK) in the BVDW

The Online-Vermarkterkreis (OVK) is the central committee of German online publishers and advertising sales houses. Under the umbrella of the Bundesverband Digitale Wirtschaft (BVDW) e.V., 16 of Germany‘s leading suppliers of digital ad space have joined forces to continuously increase the importance of online advertising.

The primary objectives are to heighten market transparency and planning reliability as well as standardisation and quality assurance measures for the entire digital advertising industry. In addition, the OVK implements important projects such as congresses, studies and promotional activities and is involved in national and international committees for the further development of industry.

www.ovk.de

PROGRAMMATIC ADVERTISING
FOKUSGRUPPE IM BVDW

ONLINE-VERMARKTERKREIS IM BVDW

Imprint

Market research on the advertising identity ecosystem

Place and date of publication	Berlin, October 2021
Publisher	Bundesverband Digitale Wirtschaft (BVDW) e.V. [German Association for the Digital Economy] Schumannstraße 2, 10117 Berlin, +49 30 2062186 - 0, info@bvdw.org, www.bvdw.org
Managing Director	Marco Junk
President	Dirk Freytag
Vice Presidents	Thomas Duhr, Anke Herbener, Corinna Hohenleitner, Dr. Moritz Holzgraefe, Alexander Kiock, Julian Simons
Contact	info@bvdw.org
Association register number	Register of associations Düsseldorf VR 8358
Legal notice	All information in this publication was diligently researched and verified by the Bundesverband Digitale Wirtschaft (BVDW) e.V. This information is a service of the association. Neither the BVDW nor the companies participating in the compilation and publication of this work assume any liability for correctness, completeness and currentness. The content of this publication and/or references to content of third parties are protected by copyright. Any copying of information or data, especially the use of texts, parts of texts, picture material or other content, requires the prior written approval of the Bundesverband Digitale Wirtschaft (BVDW) e.V. or owners of rights (third parties).
Edition	Second edition
Titelmotiv	© iStock / ipopba

The research on which this publication is based was conducted by:
NK & Co. GmbH, www.nkco.de, Borodinstraße 14, 13088 Berlin