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 white paper on the Advertising Identity Ecosystem is based on a study commissioned by the "OVK Unit Programmatic & Data" at the end of 2019 to examine the most widely used technologies and the providers of identity solutions.

Since several browser manufacturers (Firefox, Safari) no longer support 3rd-party cookie/fingerprinting for cross-webpage user tracking or have announced such a restriction (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. Since the period covered by the white paper is between November 2019 and February 2020, 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.

Research

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

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 a start-up founded more than two years ago. It started with the mission of optimising inefficient cookie syncing. Since then, ID5 has been trying to solve the problem of Advertising Identity. To that end, the company is working on the product "Universal ID".

The Trade Desk – Unified ID Solution

As one of the largest DSPs, The Trade Desk offers several solutions in the area of Advertising Identity. Among others is the Unified ID Solution. This is a cookie-based identity solution based on the company's own advertising infrastructure. The Trade Desk has decided not to participate in this research.

Roq.ad

Founded in 2015, Roq.ad began with the mission of enabling device independent targeting of people and target groups in digital marketing.

Digitrust

Digitrust was founded as a non-profit organisation with the mission of optimising cookie syncing. Later the company was taken over by IAB Techlab, inclusive of its solutions and infrastructure. The strategic direction as well as the concrete roadmap were placed in the hands of the members of the Digitrust Commit Group within the IAB Techlab. Members of this group are always Digitrust users.

Advertising ID Consortium

The Advertising ID Consortium was founded in 2017 with the goal of helping participants in the programmatic advertising business to minimize the number of cookie syncs while working within the scope of the Advertising Identity. The members of the Consortium come from both the demand and supply side. Since 2018, marketers and publishers can also become members.

LiveRamp

Started in 2011 with the mission of minimising loss of range due to inefficient cookie syncing, LiveRamp implemented a deterministic, people and graph based solution. According to its own information, the company has built the third largest graph after Facebook and Google.

Mapp

Founded 15 years ago as a start-up, Webtrekk has been part of MAPP, a marketing cloud provider, since mid-2019. MAPP is positioned in the field of website analytics and, with its broad customer base, has become indispensable in this area.

netID

European netID Foundation, the single sign-on provider, was founded in March 2018. It was established in the form of a foundation. The aim of this foundation is to offer an independent alternative to the SSO range of Google and Facebook.

Adbrain

Adbrain's mission is to enable addressing and measurability of individuals and households in digital marketing. In 2017 Adbrain was acquired by The Trade Desk. The Trade Desk, along with Adbrain, has decided not to participate in this research.

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.

Zeotap

Founded in late 2014 and originally started with data partners from the telecommunications industry, Zeotap can now also draw on data from e-commerce and app SDK providers. This customer intelligence platform provides an agnostic ID for the Martech Ecosystem and for publishers. This solution is an extension of the Zeotap identity solution currently being used for CRM onboarding.

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.
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.

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.

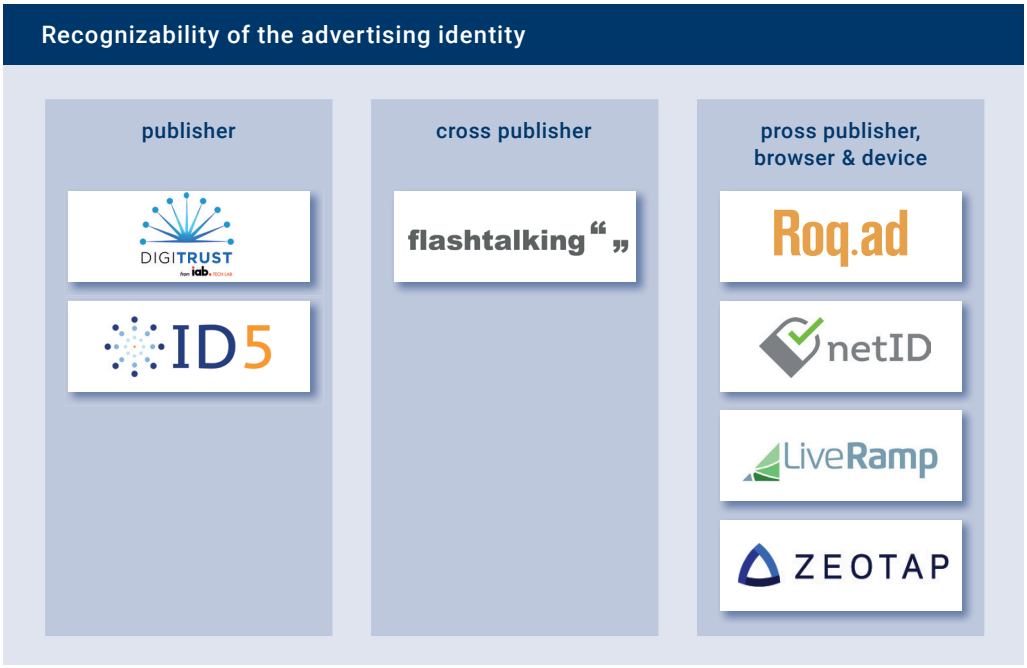
Examples of SSO providers are Facebook and Google as well as the German provider netID, which is discussed in this document.

SUMMARY

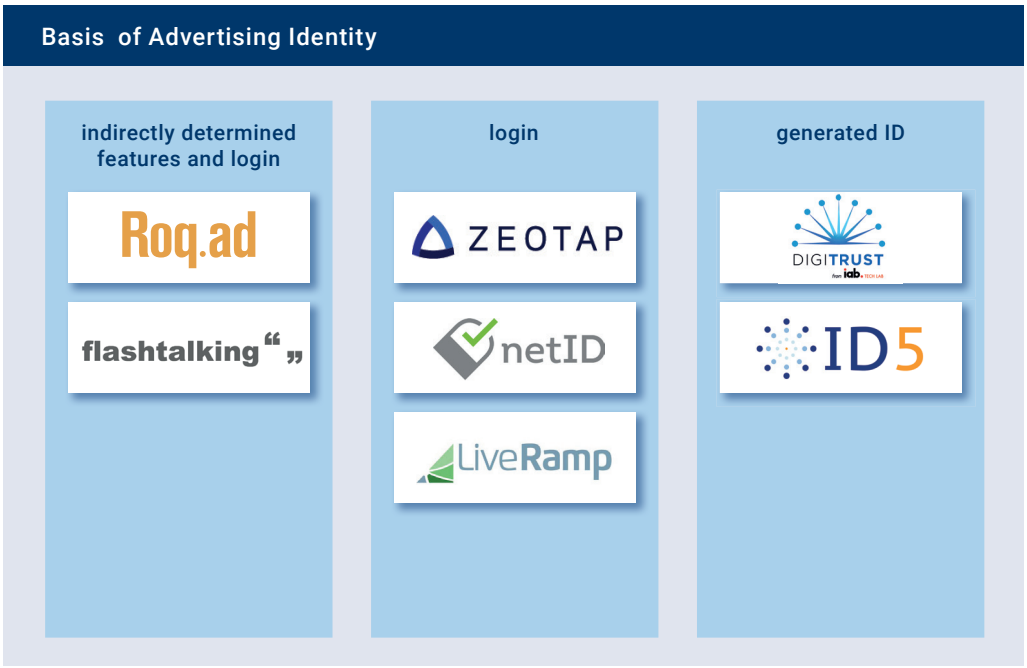
An important aspect when looking at the functioning of the system is the question of the breadth to which the solutions offer recognizability:

1. publisher / website / domain level
2. cross publisher level
3. 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 three groups.



Key features of the solutions at a glance.

	ID5	Roq.ad	Digitrust	LiveRamp	netID	Flashtalking – FTrack	Zeotap
Integrated in the Prebid User ID module*	Yes	No	Yes	Yes	Yes	No	Yes
Function dependent on 3rd party cookies	Yes	No	Yes	No	No	No	No
Develops solution for 3rd party cookie problems	Yes	-	No	-	-	-	Yes
Identification possible in Safari	No	Yes	No	Yes	Yes	Yes	Yes
Identification possible in Firefox	No	Yes	No	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	Indirect	Yes	Yes
Enables cross device targeting in the programmatic environment	No	Yes	No	Yes	Indirect	No	Yes
Uses fingerprinting	No	No	No	No	No	Yes	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

ID5 relies on client-side and 3rd-party cookies for its Universal ID product. They generate an ID and write it on the client side as a 1st-party cookie under the publisher domain and as a 3rd party cookie under the ID5 domain.

The 3rd party cookies are blocked in Safari and Firefox and will potentially be restricted in Chrome. For ID5 this already means that in Safari and Firefox they can only be recognized within one publisher. In Chrome across publishers as well.

They react to this restriction with an extension of their product, which is currently being developed and, according to the manufacturer, will be available in a first version in the first half of 2020. Publishers can use the ID generated for them to send additional signals, such as a hashed e-mail address or a Publisher ID. If ID5 finds this signal in their data records they can assume on that basis that it is the same browser.

In addition, they develop a probabilistic model which, on the basis of less unique information, is supposed to enable the most accurate recognition possible. In order to solve the cookie problem comprehensively, they are also in talks with login alliances, whose ID they could also use as a signal. They plan to test a first version of this product extension at the end of 2019.

Cross-device use of the Universal ID is dependent on the partners from whom ID5 receives signals for recognition.

Publisher Integration can be done via the Prebid User ID module. There are also scripts for Prebid-independent integration.

Roq.ad

The underlying technology is based on a proprietary cross-device graph developed by Roq.ad. Based on cookies, mobile advertising IDs and other attributes in each device request, this graph combines different devices under one Roq.ad User ID. Deterministic and probabilistic data are used for this purpose.

Deterministic data, for example, encrypted user names or e-mail addresses, is used. 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. In discussions with other market participants the probabilistic approach is also generally regarded as very stable if the probability threshold is set high enough.

Roq.ad has tags that enable web and mobile apps to be identified. Roq.ad is primarily used on the advertiser's website. Publisher integration and the transmission of the Roq.ad ID in the bidstream from the publisher via the SSP to the DSP are seen less frequently.

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 integration in market leading demand side platforms and ad servers such as The Trade Desk, AppNexus, ActiveAgent, Adition, Flashtalking and many others.

As a graph-based system, the Roq.ad ID is less affected by cookie restrictions. However, this only applies as long as there is sufficient data in the graph to merge the devices.

Digitrust

Digitrust has developed a solution that, with the limitations of browsers (cookies), enables cross-publisher identification of users in a device. This enables Digitrust to support classic Programmatic Advertising use cases. However, cross-device identification is not possible because a corresponding graph is not provided.

The Digitrust ID can be used to further limit the very complex cookie syncing. The Cookie Sync, which is still widely used, is carried out via a large number of requests from the browser to the technology providers in the marketing chain. This high number of requests significantly increases the loading times of websites. In addition, the procedure is inefficient, which reduces reach or targeting of groups.

Digitrust's method promises faster loading times and less loss of reach in contrast to cookie syncing.

Digitrust uses a 64-bit ID that is generated client-side and stored in the cookie of most publisher integrations. In rare cases the ID is generated on the server side. The content of the ID is generated randomly. The special feature of the ID is that it is stored in the cookie in encrypted form. There are dedicated public keys for each publisher with which the IDs are encrypted. This means that the 1st-party cookie of two publishers in the same browser contains different encrypted content with the same ID. Since both publishers use different public keys for encryption, they cannot be merged without the private key. The publisher passes the encrypted DigiTrust ID to the SSP or to its own ad serving technology. Only here on the server side is the ID decrypted with the private key and included in the bidrequest as a 4th-party identifier, for example.

Digitrust's solution is based 100% on 3rd party cookies. In Firefox Digitrust is blocked (disconnect.me list). In Safari, Digitrust is most likely also often blocked. Digitrust is focusing its further development on those devices and browsers on which 3rd party cookies are still available. An e.g. graph-based solution for the cookie problem is not planned.

Digitrust can be used via the UserID module in prebid. In addition, Digitrust offers direct proprietary integration by means of scripts provided directly by Digitrust.

In addition to integration on the publisher side, support of the Digitrust ID by the Advertising Technology Platforms (SSP, DSP) used by the publisher for monetization is essential.

Advertising ID Consortium

Unlike other providers in this document, the Consortium does not offer its own technology. Rather, high-reach technologies from participating technology vendors are recommended.

The technologies recommended by the Consortium which are considered in this document are LiveRamp, Digitrust, and The Trade Desk Unified ID Solution . Through this set up, the Consortium itself does not process or store data.

Members of the Consortium agree to support these technologies. Contractually, the Consortium offers a licensing of LiveRamp to members. Digitrust and The Trade Desk must be licensed directly.

The members of the Consortium come from both the demand and supply side. Publishers could also be gained as members. The Rubicon Project, Index Exchange, DataXU, LiveRamp and The Trade Desk are mentioned by name.
The membership costs $5,000.00 per year.

LiveRamp

Their multi-device capable solution is not dependent on cookies. Therefore it is not affected by the restrictions in Firefox and Safari. Where 3rd party cookies can still be used for identity purposes (Chrome), they use them to deliver maximum reach. Where cookies cannot be used, LiveRamps ATS is used. ATS stands for Authenticated Traffic Solution. By integrating ATS on the publisher side, LiveRamp receives an encrypted identifier (e.g. hashed email address) which is used to verify the existing ID graph. If LR finds a corresponding identifier in the LiveRamp graph, it is additionally encrypted and sent via Envelop to the publisher and then to the connected SSP. The received hashed identifier is then immediately deleted.

Their approach is cross-device. They then incorporate all devices that they conclude with a high degree of probability are assigned to the same person. According to LiveRamp, the 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 suchlike is not performed.

LiveRamp has purchased the Consent Management Platform Faktor.io (now LiveRamp Privacy Manager) and offers this solution bundled with the Identity solution. This makes it easier for publishers to solve legal and technical tasks. As long as the publisher has a CMP in use, which can output the TCF Consent String, the use of LiveRamp's own CMP is not necessary. For LiveRamp this is, in addition to the necessary legal solution, an aid to increasing the reach. Furthermore, LiveRamp offers publishers the use of a registration wall.

LiveRamp is one of the technology partners offering a recommended solution within the Advertising ID Consortium.

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

Mapp

Within the context of Mapp Intelligence a so-called Cross Device Bridge is provided. This is utilised for anonymous, cross-device user identification that does not require a login. It combines deterministic and probabilistic methods. The technology is based on the one hand on hashed e-mail addresses and on the other hand on device-specific features.

The Cross Device Bridge can be used in combination with other Mapp products. This enables advertisers to continuously implement and optimize personalized campaigns in the customer journey, for example. The technology is based on a cooperative pool of cross device data from various companies in Europe and the USA.

On the publisher side, there is no interface that would make it possible to transfer a Webtrekk-based ID to an ad server or SSP.

For this reason, Webtrekk will not be analysed in more detail below.

netID

From the perspective of advertising marketing netID offers a solution 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). New registrations using any e-mail address are also supported. 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 who supports netID this means that he 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 by 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. The netID is generally not a direct partner in the marketing chain at any point. It offers technical interfaces to the Publisher 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.

Currently, netID integrates its consent management products into 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, eg. 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. This extension is rolled out with the IAB Transparency and Consent Framework (TCF) Version 2.0, which is happening in Q2 2020.

Flashtalking – Ftrack

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.

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. Ftrack does not yet include its own cross-device graph in Europe. For a cross-device analysis (as a basis for their attribution solution) Flashtalking works together with other providers (e.g. Roq.ad or TapAd). The device matching rates are significantly increased by using Ftrack technology.

Due to the previous focus on pure delivery and measurement for advertisers, the Ftrack ID is unavailable to other programmatic parties in the bidding process. However, Flashtalking does not rule out whether they will open the Ftrack ID to the programmatic market or not.

Zeotap

Zeotaps offers an end-to-end technology platform combined with global onboarding and data solution. Zeotap obtains data used for this purpose from data partnerships and the integration with telecommunications providers, e-commerce players and app SDK providers. Based on pixel, SDK or server-to-server integrations with these data partners, the existing identifiers and attributes are extracted.

This data flows into Zeotap's people/identity graphs. Data is only used if a consistency is present. For quality assurance, the data used is checked e.g. against Nielsen DAR. The graph enables deterministic matching of online and offline identifiers, among other things, through proprietary patented Zeotap technology.

Zeotap uses only deterministic data. This can be identity data, socio-demographic data, app usage data or purchase intent data from eCommerce partners.

Zeotap works with personal data such as mobile ad IDs, cookie IDs or email addresses. This data is pseudonymized by hashing.

A central, connecting Zeotap ID is used in the graph, clustering the identifiers from different data sources. From Q1 2020 this Zeotap ID will be offered under the name ID+ to companies in the programmatic ecosystem.

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	From the end 2019	Yes	Yes	No
Roq.ad	Yes	Yes	No	Yes	-	Yes	No
Digitrust	Yes - CDN	Yes	No	No	-	Yes	No
LiveRamp	No	Yes	No	Yes	-	-	Yes
netID	Yes	Yes	Not for identification of the user	Yes	-	No	No
Flashtalking - FTrack	No	Yes	Yes – iab TCF in preparation	Yes	Yes	Yes	No
Zeotap	No	Yes	No, nur expliziter consent	Yes	Yes	No	Yes

Details of the providers

ID5

ID5 uses 256-bit encryption when generating the Universal ID. The ID is generated on the server side, encrypted, stored and then sent to the client for storage. ID5 obtains the user's consent to store and use the ID. If they work with additional signals, they basically get the data contained in it hashed. They operate their servers as a company from the United Kingdom in France and Germany.

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 user names as a learning basis. For the data processing on which the solution is based, they use the IAB Transparency and Consent Framework to obtain the consensus.
The infrastructure used by Roq.ad is located in the EU.

Digitrust

The Digitrust ID is generated via the WebCrypto API in the browser. This is 64-bit random data. The ID is only stored in a cookie in the client. Digitrust does not collect personal information. Digitrust uses the IAB Transparency and Consent Framework to obtain consent to store the ID. Only with consent will the ID be written to the cookie and used. The encryption of the ID in the cookie described under Functionality offers increased protection against misuse of the ID by unauthorized third parties.

Digitrust does not collect or store any data. The delivery of the necessary scripts takes place via a CDN with Edge Locations in Germany, provided the user's access is from Germany.

LiveRamp

To generate an ID, LiveRamp uses a YesvaScript in the browser during integration into the publisher. An e-mail address (hashed) is passed to the YesvaScript. This is translated by LiveRamp into an IDL, encrypted and translated on the server side by an API (LiveRamp's sidecar service) into the envelope. This envelope is unique for each request and allows only the publisher access to it by storing it in a 1st-party cookie (alternatively HTML5 local storage). For Programmatic Advertising, the encrypted IDL envelope is passed to the SSP. The SSP first passes it on to the LiveRamp Service Sidecar. Sidecar decrypts it and returns specifically encrypted IDLs for each of the DSPs to be addressed. If LiveRamp provides these DSPs with advertiser or 3rd party data (via server-to-server or API), they receive "their" encrypted IDLs again. This allows DSPs to place bids on the bid requests. The ID cannot be depseudonymized again.

According to LiveRamp, any personal data are replaced by anonymous data in the graph during the matching process. No personal data are logged by LiveRamp. LiveRamp receives personal data from publishers and advertisers.

LiveRamp has integrated a universal opt-out in the graph. LiveRamp uses Google cloud components in Brussels as infrastructure.

netID

netID exclusively uses infrastructure in the EU to operate its solution.

With netID, the user always manages his personal data and its transfer with his account provider. 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, the e-mail address as well as session information about the user are partly stored in first-party cookies. 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 prepared for the use of the IAB Transparency and Consent Framework. For the current use for the operation of the ad server Flashtalking refers to the legitimate interest. No personal data is processed within the framework of Ftrack. The data that is processed is used hashed.

Zeotap

The Zeotap ID is generated on the server side based on 1st party login data such as email address and exchanged with partners in real time. Using the Zeotap Identity Graph, additional IDs and 3rd party data can be linked to the ID.

The personal data collected during the operation of the solution is pseudonymized. Personal data will only be collected if the user has given his explicit consent.

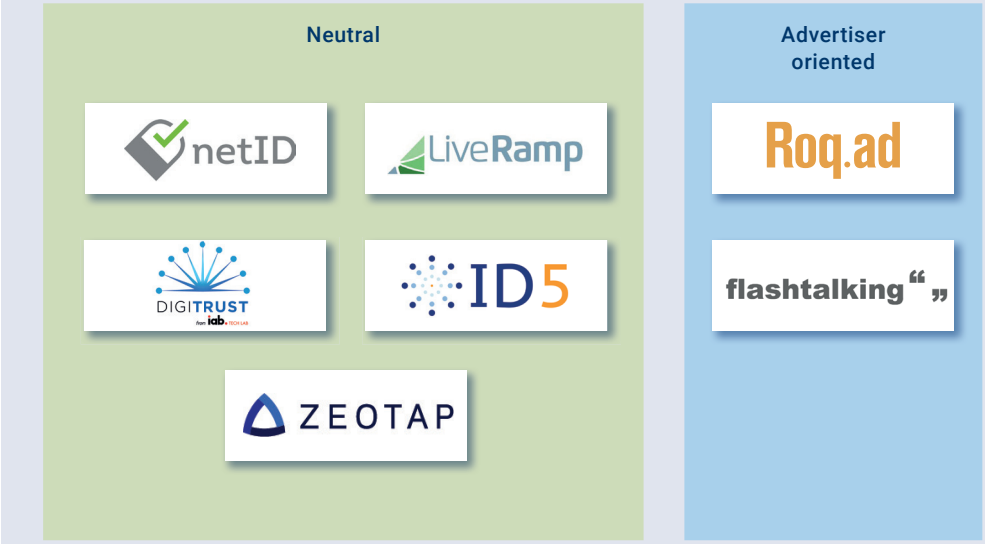
Zeotap has several certifications for privacy and security of its solution.

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 more than 2 years ago as a start-up and, according to co-founder Scott Menzer, is not strategically tied into the advertising ecosystem by investors. Furthermore, their strategic orientation is a completely neutral one. They advocate cooperation between the various providers in their field. Thus they see the possibility of the greatest possible coverage and distribution of at least one usable identity. The core of the ID5 technology is closed source and proprietary. The parts needed for the technical integration of market participants are open source and are maintained by ID5. The data generated in the course of service provision is not used for any other purpose than service provision.

Roq.ad

The solution from Roq.ad is currently more on the buyer side. Roq.ad's graphs give advertisers the opportunity to reach a more precise target group by matching different identifiers from different devices to people. The solution is a closed-source implementation that uses classical machine learning methods to calculate the graph. The collected data is used for the ongoing training of the graph and thus for all users of the graph.

Digitrust

The operation and especially the further development of Digitrust is controlled by the IAB techlab and the members of the Commit Group. Any market participant using Digitrust can become a member, regardless of their strategic positioning. Individual companies cannot influence strategic decisions alone. The integration side of the solution is an open source code. The server side is a closed source. However, the documentation describes the methods used very transparently. No further use of data can be made as none is collected.

LiveRamp

LiveRamp is a neutral player in the market. LiveRamp is equally interested on the advertiser and publisher side in entering into partnerships to increase the reach of its ID. The solution is closed source.

The data collected within the solution is used for the ongoing training of the graph. This way it benefits all users of the graph. The data is not used for any other purpose. LiveRamp is not involved in the media business, but sees its solution as a basis for others who need a personal identifier in the data or media business.

netID

netID was established as a foundation to create a login solution that is as neutral as possible. netID itself positions itself as a data protection service for users and also as a partner and enabler for website operators 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.

Zeotap

Zeotap's solution is used for targeted campaign delivery and deal targeting. As a result, the offer is equally directed at the publisher/supply and advertiser/buyer side. With the rollout of the Zeotap ID as an independent identifier for the programmatic ecosystem, the ID can also be used in combination with other data providers. The technology underlying the solution is closed source.

The data obtained from the operation of the solution is used exclusively to provide the service to the customer.

Quality

Introduction

The solutions can be roughly divided into three 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.

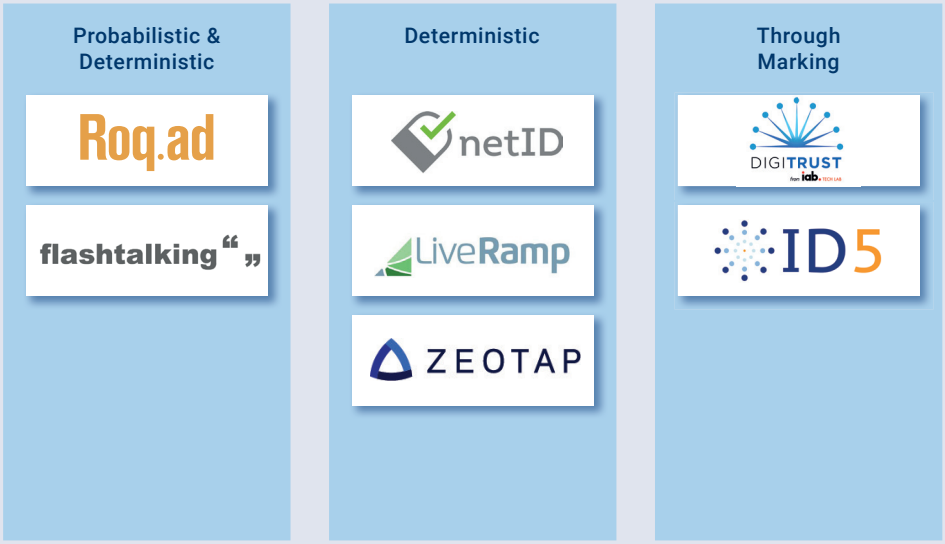
The probabilistic approach has a higher likelihood of error than the deterministic approach. How high this error probability is can be varied in the solutions considered. If the user of the system is willing to accept a higher likelihood of error, this is accompanied by a higher addressable range. In 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.

Through marking

The third approach found is based on a marker in the browser used. This generates an ID. In this case, the ID consists of any information relating to the person, such as a random number. This ID, e.g. stored in a cookie or in the local storage, is now considered at each contact. If it is the same ID, recognition is assumed.

This procedure is becoming increasingly limited due to the developments in browsers (especially Safari and Firefox) described above. Without the addition of deterministic or probabilistic methods, range losses can already be observed when using this method exclusively.

Overview of providers by approach



Comparison of the providers

ID5 – Universal ID

With ID5, a distinction must be made between the present and the future outlined in their roadmap with regard to the methodology used. Currently, they rely on markers in cookies (see functioning of ID5), knowing that this is already associated with major limitations today. According to their own statement, they are working on a deterministic system based on publisher or partner data (login alliances). Where such data is not available, this is to be supplemented by a machine learning based probabilistic system. The goal is a high overall detection rate.

With a dual approach such as this one, it must be noted that when bidding, for example, it will not be clear whether the ID5 Universal ID for this bid request was determined using a deterministic or probabilistic method. This has a direct influence on the accuracy of the targeting used. For example, a frequency cap will be less accurate. According to its own statement, the provider's goal is to use probabilistics only if the identification is almost 100% certain. They consider auditing the precision of the probabilistic. This could increase transparency towards partners. However, these developments are still in a very early phase at this point in time.

Roq.ad

Roq.ad offers a public graph model and a customized private graph model. 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 (Precision Rate) can be adjusted according to customer requirements. Typical precision rates are between 85 % and 95 % depending on the target. In the public graph model, 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 30 % recall. The range-optimized graph is 85% precision with 65% recall.

Digitrust

Digitrust's solution is a cookie-based. As described under How it works, cookies are already severely restricted in Safari and Firefox. With Digitrust ID, therefore, only Chrome Traffic is currently able to handle cookies securely. In contrast to cookie matching, Digitrust offers a higher match rate. Digitrust does not work across devices.

LiveRamp

LiveRamp is based on a graph. They use only deterministic data and methods. For the construction of the graph in a market they are therefore dependent on personal 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 hard or soft, 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 95% to 98%.

Zeotap

The Zeotap solution is 100% deterministic. In Zeotap's experience, the quality loss when using probabilistic data is very high.

Measured against Nielsen data, Zeotap's deterministic data set achieves up to 94% accuracy in detecting people.

Relevance

Details of the providers

ID5 – Universal ID

ID5 today counts 1.5 million unique calls of Universal ID per month in Germany. Without having been directly active in Germany so far, they have achieved this scaling mainly through integration in partner platforms, but also publishers such as Duden.de, Gentside.de and Ohmymag.de. They are currently starting an active marketing of their product in Germany. This is aimed at tech platforms and large publishers.

ID5 is supported by advertising platforms like Appnexus and Bidswitch. On the supply side, ID5 is supported by Smart, among others. Among others, the following demand side platforms support ID5: Mediamath, Avocet, Adot and Adform.

Roq.ad

Roq.ad's cross-device identity graph covers a market share of 80% of German online users. Similar market coverage is also achieved in other countries such as Austria, Switzerland and Poland.

Roq.ad is supported by market-leading demand side platforms (DSPs) and ad servers such as The Trade Desk, AppNexus, ActiveAgent, Adition, Flashtalking and many more.

Digitrust

Digitrust itself does not collect any usage data or KPIs that allow unique users or other reach KPIs to be determined.

On the CDN that delivers the client-side scripts, Digitrust can only determine the number of 6,000 monthly website domains that use Digitrust scripts. In the German market Digitrust is not yet very often seen in bidrequests.

Digitrust is supported by the demand side platforms Adform, Mediamath, Sizmek and supply side platforms (SSPs) such as Index Exchange, Openx, sovrn, pubmatic and rubicon project.

LiveRamp

LiveRamp is still at the beginning of its market entry in Germany. Active marketing of the product in Germany began in October of this year. Its goal is a match rate of 20 % in the German market for the end of Q1 2020. The market entry in Germany is beginning with strong acquisition activities on the publisher side. Talks have also been held with netID. In the United States, LiveRamp has already established a high reach.

netID

netID reports 38 million active users per month across all connected partners/account providers. Currently, they have 60 partners, most of which are online publishers and TV portals.

Account providers and users of the SSO are the founding members of the foundation web.de, GMX, 7Pass & ProSieben, RTL and 1und1. Partners using the SSO include C&A, DPD, Prosieben.de, Kabel1.de and others.

Flashtalking – Ftrack

On a campaign basis Flashtalking Ftrack works with other providers on the advertiser side. Roq.ad and Tapad are two of them, which provide cross-device reporting as a basis for cross-channel attribution.

Zeotap

Zeotaps Graph is available in 9 markets, including North America, Middel and South America, Europe (DE, UK, FR, IT, ES) and India.

Zeotap's graph covers about 70% of the German users. The focus is on users of mobile devices. About 70 % of the collected data points are mobile data. The remaining 30 % are desktop data.

Zeotap would like to further increase its relevance for the German market through new data partnerships and through publisher integrations. Publisher integrations are to be scaled up through cooperation with a German CMP.

Zeotap's data in its current form can be used in up to 100 marketing/advertising channels, e.g. DMPs (Adobe, Salesforce, Neustar), Social (Facebook/Instagram, Snapchat), DSPs (The Trade Desk, Adform, Active Agent, Google, MediaMath etc.) or SSPs/Adservers (e.g. Google AdX/DFP, Smart, Appnexus, Oath).

Appendix

Survey period

The study was conducted from November 2019 to Yesnuary 2020 and 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
Roq.ad	Yes	Yes	Yes	Yes	No
Digitrust	No	Yes	Yes	No	Yes
LiveRamp	No	No	No	Yes	No
netID	Marketing products: Yes only SSO: No	No	No	No	No
Flashtalking - FTrack	No	No	No	Yes	No
Zeotap	No	No	No	Yes	No

Details of the provider

ID5 – Universal ID

Currently the ID5 Universal ID is free of charge for all parties. Next year, ID5 will introduce a billing model that works as follows:

- It remains free for publishers
- For SSPs who only pass on the ID from the Publisher to the DSPs, it is free
- For market participants who have to decrypt the ID (DSPs), there is a fee to be paid
- For market participants who require a matching table for ID matching, there is a fee to be paid

A price list and further information on the contract conditions are not yet available. However, it should be based on the prices of the cookie matching solution from ID5.

Roq.ad

Roq.ad's pricing model is based on a software-as-a-service model for all market participants:

- Publishers: Flat Fee from 2.000 € per month
- SSP: Costs depending on traffic volume
- DSP: Costs depending on traffic volume
- Advertiser: Flat Fee from 2.000 € per month

Digitrust

Publishers can use Digitrust free of charge, IAB Techlab or IAB membership is not required.

Digitrust's cost model is based on billing for the connected technology platforms on the seller and buyer side. The monthly costs are based on the annual managed media budget or annual net revenues:

- annual managed media budget < $5 million or annual net sales < $1 million: free of charge
- annual managed media budget < $50 million or annual net sales < $10 million: $2,500 / month
- Other platforms: $5,000 / month

In order to use Digitrust as a platform, it must also be a member of the IAB Techlab. For details see here: https://iabtechlab.com/about-the-iab-tech-lab/join-the-iab-tech-lab/

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 currently under development 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.

Zeotap

At Zeotap, advertisers pay a license fee for the use of the platform and the services it contains. 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

Imprint

Market research on the advertising identity ecosystem

Place and date of publication	Berlin, May 2020
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	Matthias Wahl
Vice Presidents	Thomas Duhr, Anke Herbener, Achim Himmelreich, Alexander Kiock, Marco Zingler
Contact	Alexandra Treidler, Head of Digital Marketing, treidler@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	First 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

Herausgeber
Bundesverband Digitale Wirtschaft (BVDW) e.V.
Schumannstraße 2, 10117 Berlin
+49 30 2062186 - 0, info@bvdw.org, www.bvdw.org