Mobile In-App Integration

03/05/2025 11:44 am EST

Overview

We recommend that you deploy ID5 in mobile in-app environments via a server to server integration. We do support alternative integration pathways depending on your requirements. If required, please reach out to your ID5 customer services representative.

To ensure accurate cross-domain and cross-device reconciliation, clients should provide signals, such as hashed emails and MAIDs in the request. We also expect you to store the 'signature' provided in our response on the user's device and provision it to us in future requests. This is integral to an optimal set up since it helps us re-identify consenting users even if their signals change as well as respect opt out requests.

Below are general instructions on how to retrieve an ID5 ID server-side for mobile app inventory and make it available in bid requests to your demand partners. The auction should be delayed in order to retrieve the user's privacy preferences and the ID5 ID prior to sending out bid requests; the amount you delay may vary and so we recommend making it configurable for optimization purposes.

Process Flow

All the server-to-server requests should be made based on user even in the app and synchronously with them.

1. Check local storage cache for an available ID5 ID
    - *IF* there is no cached ID
      OR if the ID needs to be refreshed (we recommend a cache of 8 hours)
      OR if the user's privacy preferences have changed:
        - Initialize a new HTTP POST request to the ID5 endpoint. If you previously had a stored response, then subsequent requests must include the "signature" as part of the request to ID5;
        - Store the response from ID5 locally (either in-app in local storage or in a database on the server);
    - *ELSE* if there is a valid, up-to-date value in cache:
        - Pull latest ID5 ID response from Cache
2. With the ID you now have from step 1 above (from request or cache), prepare the data for the bid request.
    - Fields that you must put in the bid request:
        - `universal_uid`
        - `link_type`
3. Include this data in each bid request to your demand partners as an eids array. For more information on how this is typically done, you can review Sending the ID5 ID to DSPs.

Caching the response

The response we return for the request will need to be cached as some of the response data needs to be used in future requests for the users. Use the `ts` parameter sent in the request in order to set a TTL for the cache refresh and a TTL for the cache deletion.

- The TTL for the cache refresh should be set to 8 hours. After the 8 hours, on the back of a user event in the app, a new request to ID5 should be made and the cached data refreshed using the data from the API response.
- The TTL for the cache deletion should be set to 30 days. The TTL for the cache deletion should be refreshed with every response from the API. If there will not be a user event in the app, in the 30 days time window, the data should be deleted.

Building Server-Side Request

Server-Side Fetch endpoints for in-app

> **North America**
>
> https://na.id5-sync.com/ga/v1

> **Global**
>
> https://api.id5-sync.com/ga/v1

Request Type

HTTP POST with JSON body.

Request Headers

`Content-Type: application/json`

Partner Number

The `PARTNER` in the request body will be an ID5-provided Partner Number. This value will be static for you once we set you up in our system. You may use the endpoint during testing with the Partner Number 173. If you haven't already been assigned a Partner Number, please contact us to request one.

Server-Side Request Parameters

Request Body

Name	Required	Type	Description	Format
ts	x	string	Timestamp in form of string which extends the ISO-8601 extended offset date-time format to add the time-zone	`yyyymmddThhmmss<ffffff>+|-hhmm`
partner	x	integer	Partner Number provided by ID5	int32
bundle	x	string	A platform-specific application identifier intended to be unique to the app. On Android, this should be a bundle or package name. On iOS, it is typically a numeric ID.	
ver	x		Application version	
ip	x	string	IPv4 address closest to device	ipv4 dot-decimal
ua	x	string	The User Agent of the device's default browser	
signature	after initial call	string	The ID5 signature from a previous call, cached on the device or your server-side	
gdpr		integer	1 if gdpr applies to this request, 0 otherwise	
gdpr_consent		string	(where applicable) the TCF compliant consent string or see 'allowed_vendors'	
allowed_vendors		string array	ID5 Partner identifiers (starting with 'ID5-') or IAB Vendor IDs https://iabeurope.eu/vendor-list-tcf/ of vendors allowed to use the ID5ID	
us_privacy		string	US Privacy Consent https://docs.prebid.org/dev-docs/modules/consentManagementUsp.html	
gpp_sid		string	The GPP section ID(s) in force for the current transaction. In most cases, this field should have a single section ID. In rare occasions where such a single section ID can not be determined, the field may contain up to 2 values, separated by a comma. More information in GPP documentation	
gpp_string		string	A valid IAB Global Privacy Platform consent string.	
name		string	App name (may be aliased at the publisher's request)	
domain		string	Domain of the app	
maid		string	The device identifier (IDFA in Apple systems, GAID in Android systems)	uuid
maid_type		string	`idfa` or `gaid`	
hem		string	sha256 hash of the cleansed e-mail address. Learn how to cleanse the data here https://wiki.id5.io/en/identitycloud/retrieve-id5-ids/passing-partner-data-to-id5	sha256
phone		string	sha256 hash of the cleansed phone number	sha256
idfv		string	Apple ID for Vendors	uuid
puid		string	Partner specific user ID	
ipv6		string	The IPV6 of the device	ipv6
country		string	Country the user is located in	ISO-3166-1-alpha-2
region		string	Region code using ISO-3166-2; 2-letter state code if USA	ISO-3166-2; 2-letter state code if USA
city		string	City using United Nations Code for Trade & Transport Locations format	United Nations Code for Trade & Transport Locations format: https://unece.org/trade/uncefact/unlocode-country-subdivisions-iso-3166-2
att	x (for iOS requests)	boolean	If the user selected "Ask App not to Track", set the value to `1`, otherwise omit the field or set the value to `0`. Also omit the field for all non-IOS requests.	boolean
accept_language		string	A string representing languages accepted by end-user device, should be compatible with browser Accept-Language header.	Accept-Language header format

Name	Required	Type	Description	Format
segments		objects array	The segment ids a user may belong to and the destination platform that the segments should be pushed to. Only certain destination platforms are supported and there are backend configurations that need to be made in both ID5's and the destination platform's systems before this feature can be used. Please reach out to your ID5 representative or contact@id5.io for more information and to get started.	Array of segment objects (see below Segment object)

Segment Object

Name	Required	Type	Description	Example
destination	x	string	The destination platform. Should be the IAB Vendor ID	`999`
ids	x	string array	List of segment ids to add the user to	`[ '12345', '67890' ]`

Response Body

Name	Required	Type	Description	Format	Example
created_at	x	string	Timestamp in form of string which extends the ISO-8601 extended offset date-time format to add the time-zone	`yyyymmddThhmmss<ffffff>+|-hhmm`	`2013-02-01T12:52:34+09:00`
original_uid	x	string	A 1st party user ID that will be stable for this user on the domain. This is for reference only for the publisher and should not be shared with other partners. The value will be encrypted and will change periodically even for the same user on the same domain (while the underlying value is stable). If ID5 did not have consent, then the value will be "0		
universal_uid	x	string	The UID that is to be used for sharing with other parties. The value will be encrypted and will change periodically even for the same user on the same domain. If ID5 did not have consent, then the value will be "0"		
privacy	x	object	An object containing privacy information (see below)		
signature	x	string	ID5 Signature - a string that must be stored by the caller (cached on the device or your server-side) and sent back to ID5 on all future requests. See below for details about the Signature (see below for more details)		
ext	x	object	See below extension object		

Privacy Object

Name	Required	Type	Description	Format	Example
jurisdiction	x	string	The legal jurisdiction applicable to the request (e.g. "gdpr", "ccpa", etc), based on the location the request was made from	enum	gdpr
id5_consent	x	boolean	Indicates if ID5 had proper consent on the request to process the user's personal data. See below for more information about how ID5 handles requests with and without consent.		

ext Object

Name	Type	Description	Example
linktype	integer	See details here	1

Invalid Request Response

Name	Type	Description	Example
code	string	A code which univocally identifies the error	- partner_id_invalid - sha256_length_invalid - request_format_invalid - user_object_invalid - internal_id5_error
message	string	Human readable message about the error	- unknown partner - failed to parse json POST - missing ua - missing ts - ts older than allowed - invalid ts format - Fetch of ID5 ID disabled. Please contact ID5 to enable it. - Request from a country which is disallowed. Please contact ID5 to enable it.
type	string	A code which identifies the class of error	- validation_error - invalid_request_error - authentication_error

Example Request


```
{
 "ts": "2013-02-01T12:52:34+09:00",
 "partner": 123,
 "appid": "string",
 "bundle": "string",
 "ver": "string",
 "ip": "198.51.100.42",
 "ua": "Mozilla/5.0 (Linux; Android 11; moto e20 Build/RONS31.267-88-3; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chro
 "signature": "string",
 "gdpr": 0,
 "gdpr_consent": "string",
 "allowed_vendors": [
  "ID5-78",
  "134"
 ],
 "us_privacy": "1YNY",
 "gpp_sid": "6,7",
 "gpp_string": "DBABzw~1YNY~BVQqAAAAAgA",
 "name": "string",
 "domain": "string",
 "maid": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
 "maid_type": "idfa",
 "hem": "f97ea88ed181d60b0ba62a30579f1e10ad71eaf21b548e173de75718065c533f",
 "phone": "string",
 "idfv": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
 "puid": "string",
 "ipv6": "2001:0db8:5b96:0000:0000:426f:8a17:642a",
 "country": "string",
 "region": "string",
 "city": "string",
 "att": false,
 "accept_language": "de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7"
}
```


Example Valid Response


```
{
 "created_at": "2013-02-01T12:52:34+09:00",
 "original_uid": "string",
 "universal_uid": "string",
 "privacy": {
  "jurisdiction": "gdpr",
  "id5_consent": true
 },
 "signature": "string",
 "ext": {
  "linkType": 0
 }
}
```


Example Invalid Response


```
{
 "code": "partner_id_invalid",
 "message": "unknown partner",
 "type": "invalid_request_error"
}
```


ID5 Signature

The ID5 Signature will be returned on every response from ID5 and contains all "user state" information necessary to support cross-domain reconciliation. As an example, this could include the following pieces of data:

- Original UID value (an encrypted first party ID for this user on this domain/publisher)
- Cookie Birthdate
- Last Seen Timestamp (from this domain/publisher)

- Current ID5 ID value (encrypted)
- Link Type

> The Signature is used only by ID5 (it will be encrypted with a private key) and must be passed in every subsequent request to ID5.

Mobile Opt Ins/Opt Outs

User opt in and opt outs can be communicated via our Mobile Opt In/Opt Out endpoint