IMPROVE DIGITAL
Real time advertising technology

API
DOCUMENTATION

IMPROVE DIGITAL – OPENRTB API SPECIFICATION DOCUMENT

Version Open RTB 2.2 – Last modified: May 2018

May 2018	GDPR specifications: user and regulations objects were adjusted and also the User matching section.
March 2018	Added **at** parameter to bid and deal object
October 2017	Clickmacro is mandatory.
September 2017	Updated the max time. Our new APAC datacenter has a max time of 250 milliseconds.
June 2017	Added keywords parameter to the site and app objects.
April 2017	Added type parameter to the geo object.
March 2017	Added minbitrate parameter to the *video* object. Added maxbitrate parameter to the *video* object. Added playbackmethod parameter to the *video* object.
June 2016	Amended *static notification URL* description. Added macro *${AUCTION_ID}* for static notification URL. Amended type for *carrier* in the device object.
May 2016	Added *w, h* parameters in the *video* object.
January 2016	General revision (amended multiple sections and descriptions). Modified *bid request examples*. Modified *bid response examples*. Updated *Supported Objects/Parameters* table. Updated *Bid Request Hierarchy*.
June 2015	Added *bundle* parameter in the *app* object. Added *wseat* parameter in the *deals* object.
May 2015	Amended description for *ext.page* in the deals object.
April 2015	Amended *maxduration/minduration* in the video object.
February 2015 – V3	Added *ifa* parameter in the *device* object.

February 2015 – V2	Added *click macro* examples.
February 2015 – V1	Added *storeurl* in the *app* object.
January 2015	Added oRTB 2.2 parameters: *bidfloor*, *protocols* and *api*. Added *dsp_callback* parameter in match calls.

INDEX

1.1 BIDDING OVERVIEW

1.2 BIDDING API
1.3 TRANSPORT
1.4 MAX TIME
1.5 DATA FORMAT
1.6 SUPPORTED OBJECTS/PARAMETERS

2.1 BID REQUEST HIERARCHY
2.2 OBJECT LIST
2.3 BID OBJECT
2.4 IMPRESSION OBJECT
2.5 BANNER OBJECT
2.6 VIDEO OBJECT
2.7 REGULATION OBJECT
2.8 PMP OBJECT
2.9 DEALS OBJECT
2.10 SITE OBJECT
2.11 APP OBJECT
2.12 PUBLISHER OBJECT
2.13 DEVICE OBJECT
2.14 GEO OBJECT
2.15 USER OBJECT
2.16 EXAMPLE BID REQUEST - BANNER
2.17 EXAMPLE BID REQUEST – VIDEO
2.18 EXAMPLE BID REQUEST - APP

3.1 BID RESPONSE HIERARCHY
3.2 BID RESPONSE OBJECT
3.3 SEAT BID OBJECT
3.4 BID OBJECT
3.5 EXAMPLE BID RESPONSE - BANNER
3.6 EXAMPLE BID RESPONSE - VIDEO
3.7 EXAMPLE BID RESPONSE - APP

4.1 NOTIFICATION
4.2 PUBLISHER_WIN_PRICE_ENCRYPTED ENCRYPTION ALGORITHM

5.1 USER MATCHING
5.2 USER MATCHING API PARAMETERS

5.3 REDIRECT API IMPLEMENTATION
5.4 EXAMPLE OF USER MATCH TAG WITH REQUEST

Table 1.1
Table 1.2
Table 1.3
Table 1.4
Table 1.5
Table 1.6
Table 1.7
Table 1.8
Table 1.9
Table 1.10

Annex A

1.1 BIDDING OVERVIEW

With RTB bidding, the price is determined by a server side API call between the RTB bidder and Improve Digital. The ad tag provided by the RTB bidder is only called when the buyer is selected as the winning bidder for that impression. **All bids and wins are in USD.**

1.2 BIDDING API

The bidding API should be implemented by the RTB bidder and receives bid requests from Improve Digital. The RTB bidder can provide Improve Digital with several endpoint URL's depending on their server's location (Europe x2 endpoints, US x1 endpoint).

1.3 TRANSPORT

The base protocol between Improve Digital and the RTB bidder is HTTP. Specifically, HTTP POST is required for bid requests. All calls should return HTTP code 200 except for an empty bid response, which should return HTTP 204.

1.4 MAX TIME

Improve Digital should receive the bid response within 120 milliseconds from the moment the bid request leaves Improve Digital. This applies to all our data centers except for our APAC data center which has a max time of 250 milliseconds.

1.5 DATA FORMAT

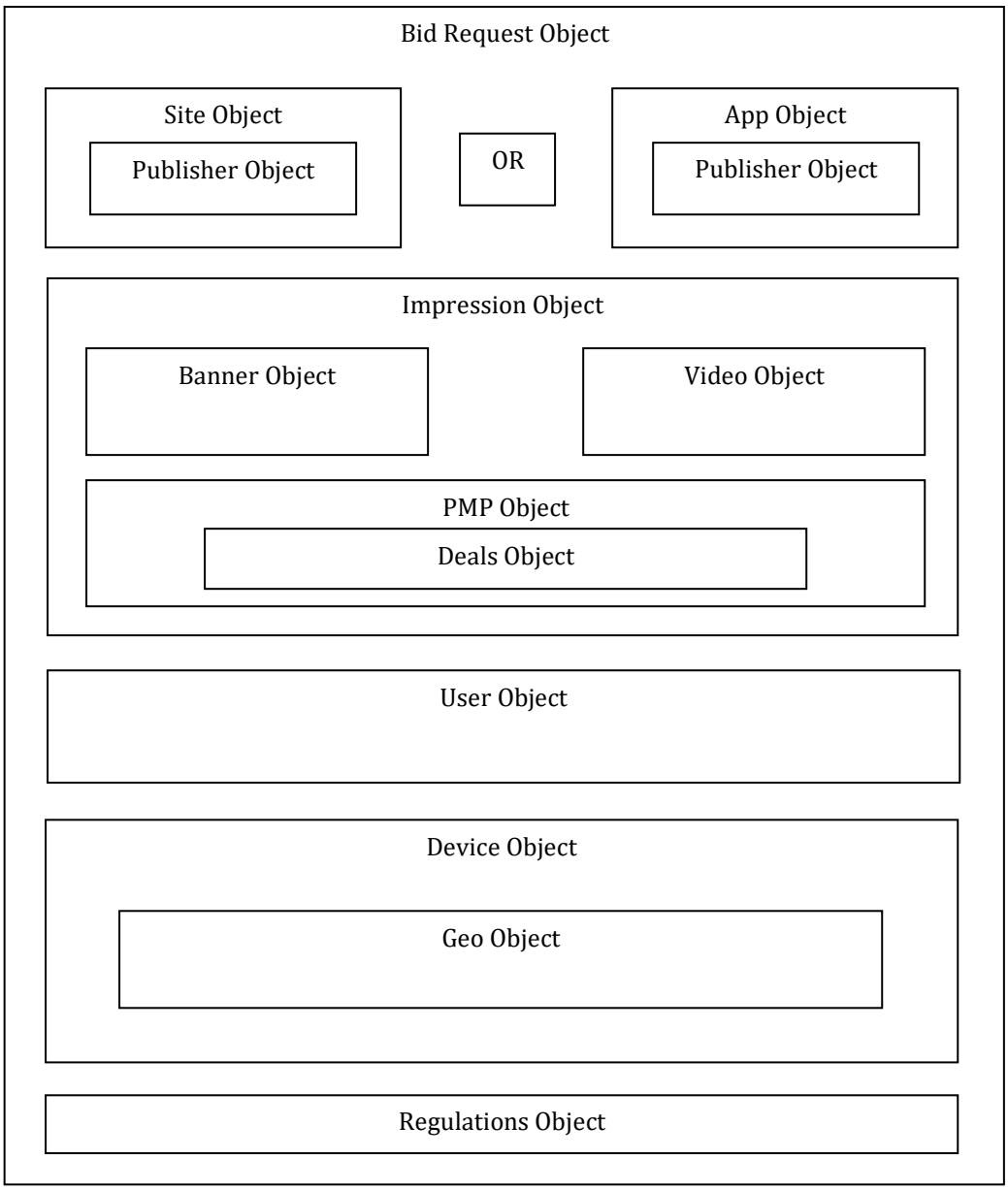
JSON (JavaScript Object Notation) is the supported format of bid request and bid response data payloads.

1.6 SUPPORTED OBJECTS/PARAMETERS

Supported Object Name	Recommended Parameters NOT Supported	Optional Parameters Supported
Bid Request Object		bcat
Impression Object	displaymanager	tagid
	displaymanagerver	ext (see Impression Object)

Banner Object		pos
		expdir
		ext (see Banner Object)
Video Object	w	battr
	h	pos
		ext (see Video Object)
		api
Regulations Object		coppa
		ext (see Regs Object)
PMP Object		private
		deals
Deals Object		seatid
		bidfloor
Site Object		name
		domain
		cat
		sectioncat
		pagecat
		page
		ext (see Site Object)
App Object		name
		domain
		cat
		sectioncat
		pagecat
		ext (see App Object)
Publisher Object		
Device Object		didsha1
		didmd5
		carrier
		make
		model
		os
		osv
Geo Object		lat
		lon
		country
		type
User Object		ext (see User Object)

2.1 BID REQUEST HIERARCHY



2.2 OBJECT LIST

The top-level bid request object contains a globally unique request ID.

Field	Type	Default	Description

bid	Object		See Bid Object
imp	Object		See Imp Object
banner	Object		See Banner Object
pmp	Object		See PMP Object
deals	Object		See Deals Object
video	Object		See Video Object
site	Object		See Site Object
app	Object		See App Object
device	Object		See Device Object
geo	Object		See Geo Object
user	Object		See User Object

2.3 BID OBJECT

Field	Type	Default	Description
id	String		Unique identifier of the bid request.
at	Object		Auction type, where 1 = First Price, 2 = Second Price Plus.
imp	Array of objects		Array of impression objects.
site	Object		See Site Object
app	Object		See App Object

device	Object		See Device Object
user	Object		See User Object
bcat	Array of strings		Blocked advertiser categories - see Table 1.5

2.4 IMPRESSION OBJECT

The "imp" object describes the impression being auctioned. Multiple impression objects are supported, and each size that is associated to a single impression will generate a separate impression object with a unique imp id. The bidder must respond with the impid in the bid response.

Field	Type	Default	Description
id	String		Identifier of the impression.
banner	Object		See Banner object
video	Object		See Video Object
pmp	Object		See PMP Object
tagid	String		Identifier of the placement.
secure	Integer	0	Flag to indicate whether the impression requires secure URL creative assets and markup. A value of "1" means that the impression requires secure assets. A value of "0" means that secure assets are not mandatory.

2.5 BANNER OBJECT

The "banner" object describes the expected nature of the banner that will be shown when the bidder wins the auction.

Field	Type	Default	Description
w	Integer		Width of the impression in pixels.
H	Integer		Height of the impression in pixels.
pos	Integer		Ad position - see Table 1.1
battr	Array of integers		Blocked creative attributes - see Table 1.2. If blank, assume all types are allowed.
expdir	Array of integers		Properties of the expandable ad - see Table 1.3 for expandable directions.

2.6 VIDEO OBJECT

Improve Digital supports VAST 3.0 and previous versions. All videos are Linear.

Field	Type	Default	Description
mimes	Array of strings		MIME types supported.
maxduration	Integer		Maximum video ad duration in seconds.
minduration	Integer		Minimum video ad duration in seconds.
protocol	Integer	3	Video bid response protocols (**kept for backward compatibility but will be eventually deprecated. Please use "protocols" instead to specify protocols)** - see Table 1.7
protocols	Array of integers	2,3,5,6	Video bid response protocols - see Table 1.7
w	Integer		Width of the player in pixels.
h	Integer		Height of the player in pixels.
startdelay	Integer		Indicates the start delay in seconds for preroll, midroll or postroll - see Table 1.4
linearity	Integer	1	Indicates whether the ad impression is linear or can be any type. A value of "1"

			denotes Linear / Instream. A value of "2" denotes Non-Linear/Overlay (Improve Digital currently supports Linear Impressions only).
battr	Array of integers		Blocked creative attributes - see Table 1.2. If blank, assume all types are allowed.
api	Array of Integers		List of supported API frameworks for this impression - see Table 1.8. If an API is not explicitly listed, it is assumed not to be supported.
minbitrate	integer		Minimum bit rate in Kbps. Exchange may set this dynamically, or universally across their set of publishers. Validation limit minimal bitrate > 0 and < 15,000, Min bitrate has to be one lower than maximum bitrate
maxbitrate	integer		Maximum bit rate in Kbps. Exchange may set this dynamically, or universally across their set of publishers. Validation limit maximal bitrate > 0 and < 20,000
playbackmethod	Array of integers		List of allowed playback methods. If blank, assume that all are allowed. See Table 1.9 Video Playback Methods for a list of possible values.
ext.aspect_ratio	String		Aspect ratio of the player.

2.7 REGULATIONS OBJECT

Field	Type	Scope	Description
coppa	Integer		It refers to the United States Children's Online Privacy

			Protection Act ("COPPA"). A value of "1" means that the site is primarily viewed by children (while "0" means that it is not expected to be primarily viewed by children).
ext.gdpr	Integer	Optional	Signals whether or not the request is subject to GDPR regulations. Which is an optional integer that indicates: 0 = No 1 = Yes Under OpenRTB conventions for optional attributes, omission indicates Unknown.

2.8 PMP OBJECT

Field	Type	Default	Description
deals	Array of objects		List of deals.
private_auction	Integer		A value of "1" indicates that only bids for the enumerated deals will be accepted. A value of "0" (or unspecified) indicates that open market bids are welcome as well.

2.9 DEALS OBJECT

Field	Type	Default	Description
id	String		Unique identifier of the deal.
at	Integer		Optional override of the overall auction type of the bid request, where 1= First Price, 2 = Second Price Plus, 3 = the value passed in bidfloor is the agreed upon deal price.

bidfloor	Integer		Minimum CPM price of the deal expressed in USD (only passed for deals).
ext.seatid	Array of strings		ID of the bidder seat who is allowed to make the bid (kept for backward compatibility when introducing the "wseat" field).
ext.page	String		url of the page to be associated to the buyer related to the deal, replacing at all levels (targeting, reporting, etc.) the value passed through site.page or app.storeurl.
wseat	Array of strings		ID of the bidder seat who is allowed to make the bid. Although it is an array, currently we do not allow multiple seats to bid on the same deal.

2.10 SITE OBJECT

The "site" object describes the site where the ad will be shown.

Field	Type	Default	Description
id	String		Site ID in Improve Digital – used for debugging purposes.
name	String		Site name. It is not always exposed by the publisher in the bid requests.
domain	String		Top-level domain of the site. It is not always exposed by the publisher in the bid requests.
cat	Array of strings		IAB content categories for the overall site - see Table 1.5
sectioncat	Array of strings		IAB content categories for the section - see Table 1.5

pagecat	Array of strings		IAB content categories for the page - see Table 1.5
page	String		URL of the page. It is always exposed in the bid requests.
publisher	Object		See Publisher Object
keywords	String		List of keywords describing this site in a comma separated string.

2.11 APP OBJECT

The "app" object describes the app where the ad will be shown.

Field	Type	Default	Description
id	String		App ID in Improve Digital – used for debugging purposes.
name	String		App name in Improve Digital.
domain	String		Top-level domain of the application.
cat	Array of strings		IAB content categories for the overall site - see Table 1.5
sectioncat	Array of strings		IAB content categories for the section - see Table 1.5
pagecat	Array of strings		IAB content categories for the page - see Table 1.5
ext.creative_display_types	Array of strings		Possible values: "display", "interstitial", "resize" and "expand".
ext.resize_height	Integer		Height dimension ad can resize to (only sent with creative_display_types resize).
ext.resize_width	Integer		Width dimension ad can resize to (only sent with creative_display_types resize).
publisher	Object		See Publisher Object
storeurl	String		app store URL for an installed app.

bundle	String		Application bundle or package name (e.g., com.foo.mygame). This is intended to be a unique ID across multiple exchanges.
keywords	String		List of keywords describing this app in a comma separated string.

2.12 PUBLISHER OBJECT

Field	Type	Default	Description
id	String		Unique identifier of the Publisher.

2.13 DEVICE OBJECT

The "device" object provides information related to the user device.

Field	Type	Default	Description
dnt	Integer		Do not track – value "0" means that do not track is set to false in the browser, while value "1" means that do not track is set to true.
ua	String		Browser user agent.
ip	String		IPv4 address closest to the device.
didsha1	String		SHA1 hashed device ID.
didmd5	String		MD5 hashed device ID.
dpidsha1	String		SHA1 hashed platform-specific ID (e.g., Android ID or UDID for iOS).
dpidmd5	String		MD5 hashed platform-specific ID (e.g., Android ID or UDID for iOS). It should be interpreted as case insensitive.
language	String		Browser language.
make	String		Device Make.
model	String		Device Model.
devicetype	Integer		Device Type - see Table 1.6
os	String		Device operating system.
osv	String		Device operating system version.
carrier	String		http://en.wikipedia.org/wiki/Mobile_network_code

geo	Object		See Geo Object
ifa	String		Native identifier for advertisers: an opaque ID assigned by the device or browser for use as an advertising identifier (e.g. Apple's IFA, Android's Advertising ID, etc).

2.14 GEO OBJECT

The "geo" object is situated within the device object and only relates to device derived Geo information.

Field	Type	Default	Description
country	String		Country based on IP look up. ISO 3166-1 alpha 2 http://en.wikipedia.org/wiki/ISO_3166-1_alpha-2
lon	Float		Longitude from -180 to 180. West is negative.
lat	Float		Latitude from -90 to 90. South is negative.
type	Integer		Indicate the source of the geo data (GPS, IP address, user provided). See Table 1.10 Location Type for a list of potential values. Type should be provided when lat/lon is provided.

2.15 USER OBJECT

The "user" object provides information known or derived about the human user of the device.

Field	Type	Default	Description
id	String		Publisher user id.
buyeruid	String		External user id.
ext.consent	String		Contains the consent string (daisy bit).The user consent string is optional, but highly recommended if the request is subject to GDPR regulations (i.e., *Regs.ext.gdpr* = 1). The default sense of consent under GDPR is "opt-out" and as such, an omitted consent string in a request subject to GDPR would

			need to be interpreted as equivalent to the user fully opting out of all defined purposes for data use by all parties.
ext.improve_consent	Integer		The extension attribute "*improve_consent*", integer, which is an Improve specific extension containing Improve Consent values found in Table 1.11

2.16 EXAMPLE BID REQUEST – BANNER (example with open auction, direct deals and with GDPR consent)

```
{
"site":{
        "domain":"http://improvedigital.com",
        "pagecat":["IAB17-39","IAB17-40"],
        "publisher":{"id":"671"},
        "id":"121485",
        "name":"Test Site Display",
        "page":"http://www.improvedigital.com/bannerexample"
        },
"imp":[
      {
       "secure":0,
       "tagid":"835725",
       "banner":{
                "h":250,
                "pos":1,
                "w": 970
                },
       "id":"1",
       "pmp":{
             "deals":[
                   {"wseat":["1234"],
                    "bidfloor":0.010730,
                    "ext":{
                          "page":"http://www.improvedigital.com/news",
                          "seatid":"1234"
                          },
                    "id":"204508"
                    },
                   {"wseat":["789"],
                    "bidfloor":0.0214590,
                    "ext":{
                          "page":"http://www.improvedigital.com/",
                          "seatid":"789"
                          },
```

```
                "id":"204513"
                }
               ],
        "private_auction":0
        }
 },
{"secure":0,
 "tagid":"835725",
 "banner":{
          "h":90,
          "pos":1,
          "w":728
          },
 "id":"2",
 "pmp":{
        "deals":[
               {"wseat":["1234"],
                "bidfloor":0.010730,
                "ext":{
                      "page":"http://www.improvedigital.com/news",
                      "seatid":"1234"
                      },
                "id":"204508"
                },
               {"wseat":["789"],
                "bidfloor":0.0214590,
                "ext":{
                      "page":"http://www.improvedigital.com/",
                      "seatid":"789"
                      },
                "id":"204513"
                }
               ],
        "private_auction":0
        }
       },
{"secure":0,
 "tagid":"835725",
 "banner":{
          "h":60,
          "pos":1,
          "w": 468
          },
 "id":"3",
 "pmp":{
        "deals":[
               {"wseat":["1234"],
                  "at" : 2,
     "bidfloor":0.010730,
                "ext":{
                      "page":"http://www.improvedigital.com/news",
                      "seatid":"1234"
```

```
                        },
                    "id":"204508"
                    },
                   {"wseat":["789"],
                     "at" : 2,
                    "bidfloor":0.0214590,
                    "ext":{
                          "page":"http://www.improvedigital.com/",
                          "seatid":"789"
                          },
                    "id":"204513"
                    }
                   ],
             "private_auction":0}
            }
           ],
"user":{
          "buyeruid":"12345",
          "id":"55abced4-1416-4cd6-9f64-ef2c28e2c9f5"
          "ext":{
                      "consent": "CONSENT_STRING",
                           "improve_consent":1
             }
          },
"device":{
         "geo":{
              "country":"NL"
              },
         "ua":"Mozilla/5.0 (Windows NT 6.3; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0",
         "osv":"Windows_Other",
         "ip":"46.226.57.66",
         "devicetype":2,
         "os":"Windows",
         "dnt":0,
         "language":"en"
         },
"regs":{
       "coppa":0
       "ext":{
                      "gdpr": 1
            }

       },
"id":"1a46691f-7c94-490d-9cbf-47af9c8470fd",
 "at" : 2
}
```


2.17 EXAMPLE BID REQUEST VIDEO (example with open auction and direct deals and no GDPR consent)


```
{
"site":{
```

```
        "domain":"http://www.improvedigital.com",
        "pagecat":["IAB10-4"],
        "publisher":{
                    "id":"671"
                    },
        "id":"120157",
        "name":"Test Site Display - Video",
        "page":"http://www.improvedigital.com/videoexample"
        },
"imp":
      [
       {"secure":0,
        "tagid":"838343",
        "id":"1",
        "pmp":{
              "deals":[
                     {"wseat":["1234"],
                      "bidfloor":0.0106410,
                      "ext":{
                            "page":"http://www.improvedigital.com",
                            "seatid":"1234"
                            },
                      "id":"206018"
                      },
                     {"wseat":["789"],
                      "bidfloor":0.0106410,
                      "ext":{
                            "page":"http://www.improvedigital.com",
                            "seatid":"789"
                            },
                      "id":"206022"
                     }
                     ],
               "private_auction":0
              },
"video":{
        "startdelay":0,
        "protocols":[2,3,5,6],
        "linearity":1,
        "protocol":3,
        "pos":1,
        "ext":{
              "aspect_ratio":"4x3"
              },
        "mimes":["video/mpeg","video/mp4","video/quicktime","video/x-ms-wmv","video/x-flv"],
        "minduration":5,
        "maxduration":30
        }
       }
      ],
"user":{
       "buyeruid":"543210",
```

```
        "id":"55abced4-1416-4cd6-9f64-ef2c28e2c9f5"
        "ext":{
                        "consent": "CONSENT_STRING",
                            "improve_consent": 0
                }
        },
"device":{
          "geo":{
                "country":"NL"
                },
          "ua":"Mozilla/5.0 (Windows NT 6.3; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0",
          "osv":"Windows_Other",
          "ip":"46.226.57.66",
          "devicetype":2,
          "os":"Windows",
          "dnt":0,
          "language":"en"
          },
"regs":{
        "coppa":0
             "ext":{
                        "gdpr": 1
                }
        },
"id":"f9ffdf5b-0733-4136-9146-fe7f9b88b14c",
   “at” : 2
}
```

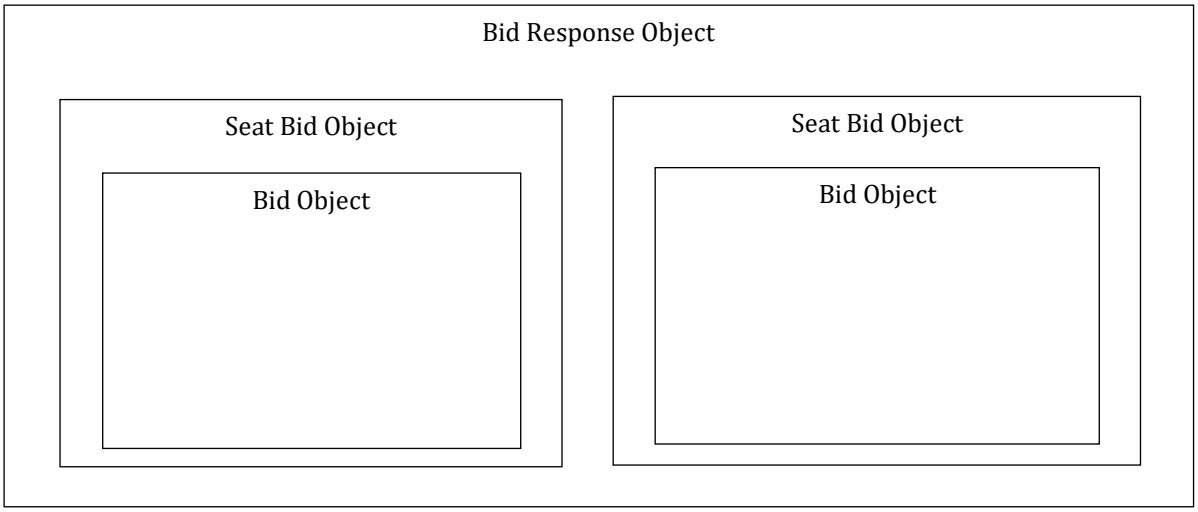

2.18 EXAMPLE BID REQUEST APP (example with open auction)


```
{
"app":{
        "domain":"http://improvedigital.com/",
        "id":"121487",
        "storeurl":"http://www.improvedigital.com/storeexample",
        "sectioncat":["IAB1-6"],
        "pagecat":["IAB3-10","IAB3-5"],
        "publisher":{"id":"671"},
        "ext":{
              "resize_width":350,
              "resize_height":350,
              "creative_display_types":['resize"]
              },
        "bundle":"TestBUNDLE",
        "cat":["IAB1"],
        "name":"inApp Test Site"
       },
"imp":
       [
        {"secure":0,
```

```
        "tagid":"835590",
        "banner":{
                "h":320,
                "pos":1,
                "w":320
                },
        "id":"1"
        },
       {"secure":0,
        "tagid":"835590",
        "banner":{
                "h":50,
                "pos":1,
               "w":300
                },
        "id":"2"
         },
        {"secure":0,
         "tagid":"835590",
         "banner":{
                  "h":50,
                  "pos":1,
                  "w":320
                  },
        "id":"3"
        }
       ],
"user":{
       "id":"55abced4-1416-4cd6-9f64-ef2c28e2c9f5"
       },
"device":
        {"geo":
              {"lat":52.373193,
               "lon":4.892597,
               "country":"NL"
               },
         "carrier":"TestCARRIER",
         "ifa":"31b08ce2-73d3-4c49-beef-fd3d467627a6",
         "model":"Apple_iPhone",
         "make":"Apple",
         "dpidmd5":"d8f60ef34d012f738b6ddf57cda9e3b6",
"ua":"Mozilla/5.0 (iPhone; CPU iPhone OS 7_1_1 like Mac OS X) AppleWebKit/537.51.2 (KHTML, like Gecko)
Version/7.0 Mobile/11D257 Safari/9537.53",
         "osv":"iOS_7",
         "ip":"46.226.57.66",
         "devicetype":4,
         "os":"iOS",
         "dpidsha1":"99b7ffc9d3dc8103c9916a4974c9807cbf60cdb8",
         "dnt":0,
         "language":"en"
         },
"regs":{
```

```
        "coppa":0
        },
"id":"8c5430d9-2747-476e-90d3-a04c690beced",
   "at" : 2
}
```

3.1 BID RESPONSE HIERARCHY



3.2 BID RESPONSE OBJECT

Field	Scope	Type	Default	Description
id	Required	String		ID of the bid request.
seatbid	Required	Array of objects		At least one seat bid object is required in a bid seat.

3.3 SEAT BID OBJECT

Field	Scope	Type	Default	Description
bid	Required	Array of objects		Array of bid objects.

seat	Optional	String		ID of the bidder seat who is making the bid (mandatory when bidding on deals).

3.4 BID OBJECT

Field	Scope	Type	Default	Description
id	Required	String		Identifier chosen by the RTB bidder.
impid	Required	String		ID of the impression object the bid applies to.
price	Required	Float		Bid price in $ CPM.
nurl	Required for VAST bids	String		Win Notice Url - to be used for VAST response ONLY. Must contain win price macro (see notification). Must return VAST XML response.
adm	Required for Display and App bids	String		Actual ad markup - to be used for banner and app responses ONLY. Must contain win price macro (see notification)
adomain	Required	Array of strings		List of top-level domains for advertiser to be used in blacklisting.
ext.advertiser	Required	String		Name of the advertiser placing bid.

dealid	Optional	String		Indicates that the bid belongs to the deal object. Mandatory to be returned in the bid object for PMP deals.

3.5 EXAMPLE BID RESPONSE BANNER (example with one bid for one Deal ID)


```
{
  "id" : "1a46691f-7c94-490d-9cbf-47af9c8470fd",
  "seatbid" : [
    {
      "bid" : [
        {
          "adm" : "<a href="[click_url]http://anyURL"><img style=\"border: 0;\" width=\"90\"
height=\"728\" src=\"http://anyImagePath\" alt=\"\"/></a><img width=\"1\" height=\"1\" border=\"0\"
alt=\"\" src=\"http://anyImagePath&p=[publisher_win_price]\"/>",
          "adomain" : [ "anySampleDomain.com" ],
          "dealid" : "204508",
          "ext" : {
            "advertiser" : "AdvertiserABC"
          },
          "id" : "1",
          "impid" : "2",
          "price" : 5
        }
      ],
      "seat" : "1234"
    }
  ]
}
```

3.6 EXAMPLE BID RESPONSE VIDEO (example with one bid for the open auction)


```
{
  "id" : "f9ffdf5b-0733-4136-9146-fe7f9b88b14c",
  "seatbid" : [
    {
      "bid" : [
        {
          "adomain" : [ "anySampleDomain1.com", "anySampleDomain2.com" ],
          "ext" : {
            "advertiser" : "AdvertiserXYZ"
          },
          "id" : "1",
          "impid" : "1",
          "nurl" : "http://vast_url.com/vast_path",
          "price" : 5
        }
      ],
      "seat" : "10"
    }
  ]
}
```


3.7 EXAMPLE BID RESPONSE APP (example with one bid for the open auction)


```
{
  "id" : "8c5430d9-2747-476e-90d3-a04c690beced",
  "seatbid" : [
    {
      "bid" : [
        {
          "adm" : "<a href="[click_url]http://anyURL"><img style=\"border: 0;\" width=\"50\"
height=\"300\" src=\"http://anyImagePath\" alt=\"\"/></a><img width=\"1\" height=\"1\" border=\"0\"
alt=\"\" src=\"http://anyImagePath&p=[publisher_win_price]\"/>",
          "adomain" : [ "anySampleDomain.com" ],
          "ext" : {
            "advertiser" : "SampleAdvertiser"
          },
          "id" : "1",
          "impid" : "2",
          "price" : 4
        }
      ],
      "seat" : "buyer4199"
    }
  ]
}
```

4.1 NOTIFICATION

Improve Digital will notify the RTB bidder with feedback on the results of each won impression. If the RTB bidder wins the auction and the creative is served, the notification will be provided as a macro on the winning ad tag.

We support the below macros:

Macro	Required	Description
[publisher_win_price]	No, but highly recommended	The winning price for the impression, $ CPM.
${AUCTION_PRICE}	No, but highly recommended	
[publisher_win_price_encrypted]	No, but highly recommended	The winning price for the impression, encrypted, $ CPM. See below.
${AUCTION_PRICE:B64}	No, but highly recommended	
[click_url]	Yes	Used to register the click with Improve Digital *
[click_url_enc]	Yes	the URL-encoded version of click_url, which can be used to first pass the value through another server that will return a redirect *

Click macro samples:

For troubleshooting purposes, Improve digital can also hold a static notification URL that is called via server to server to provide final price for impression. This static notification URL is not to be confused with the (dynamic) "nurl" field submitted with VAST responses.

Note that the static notification URL should have the bid request ID macro so that the RTB bidder can link the notification to the auction context. All macros listed in the table below are supported for static notification URL.

Macro	Description
${AUCTION_ID}	ID of the bid request.
${AUCTION_BID_ID}	Bid ID of the winning bid.
${AUCTION_IMP_ID}	Impression ID of the winning bid.
${AUCTION_SEAT_ID}	Seat ID used in the winning bid.
${AUCTION_PRICE}	Winning price.
${AUCTION_PRICE:B64}	Winning price in Base64 encoding (see Annex A).

Example: http://server.com/image1&p=${AUCTION_PRICE}&imp=${AUCTION_ID}

4.2 PUBLISHER_WIN_PRICE_ENCRYPTED ENCRYPTION ALGORITHM

The RTB bidder decryption code should decrypt the price using the encryption key and verify the integrity bits with the integrity key. The keys will be provided by the RTB bidder to Improve Digital offline as part of the account setup process. The price is stored as a padded string, and encrypted in the following format:

{initialization_vector (16 bytes)}{encrypted_price (8 bytes)}{integrity (4 bytes)}

The price is encrypted as <price xor HMAC(encryption_key, initialization_vector)> so decryption calculates HMAC(encryption_key, initialization_vector) and xor's with the encrypted price to reverse the encryption. The integrity stage takes 4 bytes of <HMAC(integrity_key, price | | initialization_vector)> where | | is concatenation. The result is encoded as BASE64 with additional substitution: + -> -, / -> .

Example:

Encoding Key: c422fdd0d81f

Integrity Key: fe3fd7dd8731

Price to Encrypt: 12.3

String sent in macro: TIIaiQAAAADrGuxxE_bP1NLLAzt.CDSJCASO4Q=

String for decryption: TIIaiQAAAADrGuxxE_bP1NLLAzt/CDSJCASO4Q=

More detail about the encryption can be found in Annex A

The RTB bidder should include a win notification macro in the creative sent with the bid, like in the following example:

<script src=\"http://adserver.com/ad.js?price=[publisher_win_price]\"></script>

If the bidder wins the auction and the creative is rendered, it will be called as follows:

<script src=\"http://adserver.com/ad.js?price=1.75\"></script>

5.1 USER MATCHING

User Matching is an essential component of RTB, which allows the RTB bidders to identify their users on the Improve Digital platform (360 yield platform) with their own user IDs. Through a pixel API, you can store the User ID on the 360 yield platform. We will then pass the user ID in the bid request.

When Improve Digital recognizes that the RTB bidder will receive a request for a user that has not yet been matched, it will generate a pixel request that piggybacks on the creative of another ad being served. The request will include a callback URL that the RTB bidder should then call in response.

5.2 USER MATCHING API PARAMETERS

The RTB bidder should implement an API that accepts the following parameters on the GET request of the pixel used for user matching:

Parameter	Description
publisher_user_id	Improve Digital's unique identifier of the user.
publisher_dsp_id	Improve Digital's unique identifier of the RTB bidder.
publisher_redirecturl	URL to call back to Improve Digital.
publisher_call_type	It indicates the type of response expected by Improve Digital. It could be js, iframe or redirect. Type js means that the matching call to a bidder is placed inside a JavaScript creative, iframe means that it is placed inside an iframe, and redirect means that it is placed inside an image tag. When it is blank, js is assumed.
gdpr	GDPR specific parameter where 0 means the request is not subjected to GDPR regulation and 1 means the request is subjected to GDPR regulation.
gdpr_consent	Where IAB_consent_string is the URL-safe base64-encoded GDPR consent string. Only meaningful if gdpr=1.

User-matching GDPR specifications for Improve Digital initiated calls:

Upon receiving the consent string, Improve Digital will parse it and, if consent is given to Improve Digital then the match request initiated by improve Digital will contain the following parameters:

&gdpr={0 | 1}

where 0 means the request is not subjected to GDPR regulation and 1 means the request is subjected to GDPR regulation.

&gdpr_consent={IAB_consent_string}

where IAB_consent_string is the URL-safe base64-encoded GDPR consent string. Only meaningful if gdpr=1.

Example:

http://[BIDDER_MATCHING_URL]?publisher_user_id=1234&publisher_dsp_id=12&publisher_call_type=redirect&gpdr=1&gdpr_consent=BOEFBi5OEFBi5AHABDENAI4AAAB9vABAASA&publisher_redirecturl=http://ad.360yield.com/match

When the RTB bidder receives a user match request, a callback URL to the Improve Digital's 360 platform should be generated.

Alternatively, the RTB bidder can initiate a call to Improve Digital's 360 platform (http://ad.360yield.com/match) with the same parameters (plus dsp_callback=1). In this case, the publisher_dsp_id identifier is provided by Improve Digital to the RTB bidder offline.

User-matching GDPR specifications for bidder initiated calls:

Improve Digital will check whether user is a GDPR subject for all Matching requests.

- If user is not a GDPR subject, then nothing changes and match can be processed;
- Improve Digital will check the GDPR related parameters passed in the match requests: both *gdpr* and *gdpr_consent* and
    - If <gdpr>=0, nothing changes and match can be processed
    - If <gdpr>=1, then check <gdpr_consent>:
        - if Improve Digital has consent, then match can be processed
        - if Improve Digital doesn't have consent, then match cannot be processed.

Improve Digital supports the following parameters:

Parameter	Required	Description
publisher_dsp_id	Yes	Improve Digital's unique identifier of the RTB bidder.
external_user_id	Yes	RTB bidder's unique identifier of the user. If you set it to "0", you will disable the user matching for this user. Please note that the external_user_id is limited to max 50 characters.
dsp_callback	No, but highly recommended	By adding **dsp_callback=1** we will identify a matching request initiated by you.
Expiration	No	Expiration date for user match in unix time (seconds) in EST timezone. If omitted or "0", there is no expiration. Expiration cannot be longer than 3 months from current time
gdpr	yes	GDPR specific parameter where 0 means the request is not subjected to GDPR regulation and 1 means the request is subjected to GDPR regulation.
gdpr_consent	yes	Where IAB_consent_string is the URL-safe base64-encoded GDPR consent string. Only meaningful if gdpr=1.

If you do not want to cookie match the user, you can return an external_user_id of "0". If the expiration date is set, it will determine when we can attempt to match the user again. If no expiration date is set, we will attempt to rematch the user in 3 days.

5.3 REDIRECT API IMPLEMENTATION

In the redirect implementation, the API is called as an HTTP request that returns a 301 HTTP redirect to the Improve Digital's 360 Platform.

Secure and non-secure bidder URLs can be supported for piggybacking on SSL and non-SSL pages. The RTB bidder should provide Improve Digital with both URLs.

5.4 EXAMPLE OF USER MATCH TAG WITH REQUEST:

<img
width="0"height="0"src="http://bidder.com/match?publisher_user_id=1234&publisher_

dsp_id=12&publisher_call_type=redirect&publisher_redirecturl=http://ad.360yield.com/match"/>

RTB bidder's user match response:

Location:
http://ad.360yield.com/match?publisher_dsp_id=12&external_user_id=ABCD

Table 1.1

List of possible values passed in the position parameter.

Value	Description
0	Unknown
1	Above
3	Below

Table 1.2

List of creative attributes **not** to be displayed (passed in the battr parameter).

Value	Description
1	Audio Ad (Auto Play)
2	Audio Ad (User Initiated)
3	Expandable (Automatic)
4	Expandable (User Initiated – Click)
5	Expandable (User Initiated – rollover)
6	In Banner Video (Auto Play)
7	In Banner Video (User Initiated)
8	Pop – Over, Under or on Exit
9	Provocative
10	Shaky Flashing
11	Surveys
12	Text Only
13	User Interactive
14	Windows Dialog
15	Has Audio on/off button
16	Ad can be skipped
17	Adobe Flash

Table 1.3

List of possible expandable directions (passed in the expdir parameter).

Value	Description
1	Left
2	Right
3	Up
4	Down
5	Full Screen

Table 1.4

List of possible values for the startdelay parameter (for video banner only).

Value	Description
0	Pre-roll
-1	Mid-roll
-2	Post-roll

Table 1.5

Values passed for categories used for cat, sectioncat and pagecat.
Where the primary category value is passed, all secondary values for that category are assumed to be blocked. Example: IAB1 is sent in the request – all values IAB1-1, IAB1-2, etc. should be blocked.

Value	Description
IAB1	**Arts & Entertainment**
IAB1-1	Books & Literature
IAB1-2	Celebrity Fan/Gossip
IAB1-3	Fine Art
IAB1-4	Humor
IAB1-5	Movies
IAB1-6	Music
IAB1-7	Television
IAB2	**Automotive**
IAB2-1	Auto Parts
IAB2-2	Auto Repair
IAB2-3	Buying/Selling Cars
IAB2-4	Car Culture
IAB2-5	Certified Pre-Owned
IAB2-6	Convertible
IAB2-7	Coupe
IAB2-8	Crossover
IAB2-9	Diesel
IAB2-10	Electric Vehicle

IAB2-11	Hatchback
IAB2-12	Hybrid
IAB2-13	Luxury
IAB2-14	MiniVan
IAB2-15	Motorcycles
IAB2-16	Off Road Vehicles
IAB2-17	Performance Vehicles
IAB2-18	Pickup
IAB2-19	Roadside Assistance
IAB2-20	Sedan
IAB2-21	Trucks & Accessories
IAB2-22	Vintage Cars
IAB2-23	Wagon
IAB3	**Business**
IAB3-1	Advertising
IAB3-2	Agriculture
IAB3-3	Biotech/Biomedical
IAB3-4	Business Software
IAB3-5	Construction
IAB3-6	Forestry
IAB3-7	Government
IAB3-8	Green Solutions
IAB3-9	Human Resources
IAB3-10	Logistics
IAB3-11	Marketing
IAB3-12	Metals
IAB4	**Careers**
IAB4-1	Career Planning
IAB4-2	College
IAB4-3	Financial Aid
IAB4-4	Jobs Fairs
IAB4-5	Job Search
IAB4-6	Resume Writing
IAB4-7	Nursing
IAB4-8	Scholarships
IAB4-9	Telecommuting
IAB4-10	Military
IAB4-11	Career Advice
IAB5	**Education**
IAB5-1	7-12 Education
IAB5-2	Adult Education
IAB5-3	Art History
IAB5-4	College Administration
IAB5-5	College Life
IAB5-6	Distance Learning

IAB5-7	English as a 2nd Language
IAB5-8	Language Learning
IAB5-9	Graduate School
IAB5-10	Homeschooling
IAB5-11	Homework/Study Tips
IAB5-12	k-6 Educators
IAB5-13	Private School
IAB5-14	Special Education
IAB5-15	Studying Business
IAB6	**Family & Planning**
IAB6-1	Adoption
IAB6-2	Babies & Toddlers
IAB6-3	Daycare/Pre School
IAB6-4	Family Internet
IAB6-5	Parenting K-6 Kids
IAB6-6	Parenting Teems
IAB6-7	Pregnancy
IAB6-8	Special Needs Kids
IAB6-9	Eldercare
IAB7	**Health & Fitness**
IAB7-1	Exercise
IAB7-2	A.D.D
IAB7-3	AIDS/HIV
IAB7-4	Allergies
IAB7-5	Alternative Medicine
IAB7-6	Arthritis
IAB7-7	Asthma
IAB7-8	Autism/PDD
IAB7-9	Bipolar Disorder
IAB7-10	Brain Tumour
IAB7-11	Cancer
IAB7-12	Cholesterol
IAB7-13	Chronic Fatigue Syndrome
IAB7-14	Chronic Pain
IAB7-15	Cold & Flu
IAB7-16	Deafness
IAB7-17	Dental Care
IAB7-18	Depression
IAB7-19	Dermatology
IAB7-20	Diabetes
IAB7-21	Epilepsy
IAB7-22	GERD/Acid Reflux
IAB7-23	Headaches/Migraines
IAB7-24	Heart Disease
IAB7-25	Herbs for Health

IAB7-26	Holistic Healing
IAB7-27	IBS/Cohn's Disease
IAB7-28	Incest Abuse Support
IAB7-29	Incontinence
IAB7-30	Infertility
IAB7-31	Men's Health
IAB7-32	Nutrition
IAB7-33	Orthopaedics
IAB7-34	Panic/Anxiety Disorders
IAB7-35	Paediatrics
IAB7-36	Physical Therapy
IAB7-37	Psychology/Psychiatry
IAB7-38	Senior Health
IAB7-39	Sexuality
IAB7-40	Sleep Disorders
IAB7-41	Smoking Cessation
IAB7-42	Substance Abuse
IAB7-43	Thyriod Disease
IAB7-44	Weight Loss
IAB8	**Food and Drink**
IAB8-1	American Cuisine
IAB8-2	Barbecues & Grilling
IAB8-3	Cajun/Creole
IAB8-4	Chinese Cuisine
IAB8-5	Cocktails/Beer
IAB8-6	Coffee/Tea
IAB8-7	Cuisine-Specific
IAB8-8	Desserts & Baking
IAB8-9	Dining Out
IAB8-10	Food Allergies
IAB8-11	French Cuisine
IAB8-12	Health/Lowfat Cooking
IAB8-13	Italian Cuisine
IAB8-14	Japanese Cuisine
IAB8-15	Mexican Cuisine
IAB8-16	Vegan
IAB8-17	Vegetarian
IAB8-18	Wine
IAB9	**Hobbies & Interests**
IAB9-1	Art/Technology
IAB9-2	Arts & Crafts
IAB9-3	Beadwork
IAB9-4	Birdwatching
IAB9-5	Board Games and Puzzles
IAB9-6	Candle & Soap Making

IAB9-7	Card Games
IAB9-8	Chess
IAB9-9	Cigars
IAB9-10	Collecting
IAB9-11	Comic Books
IAB9-12	Drawing & Sketching
IAB9-13	Freelance Writing
IAB9-14	Genealogy
IAB9-15	Getting Published
IAB9-16	Guitar
IAB9-17	Home Recording
IAB9-18	Investors & Patents
IAB9-19	Jewellery Making
IAB9-20	Magic & Illusion
IAB9-21	Needlework
IAB9-22	Painting
IAB9-23	Photography
IAB9-24	Radio
IAB9-25	Roleplaying Games
IAB9-26	Sci-Fi & Fantasy
IAB9-27	Scrapbooking
IAB9-28	Screenwriting
IAB9-29	Stamps & Coins
IAB9-30	Video & Computer Games
IAB9-31	Woodworking
IAB10	**Home & Garden**
IAB10-1	Appliances
IAB10-2	Entertaining
IAB10-3	Environmental Safety
IAB10-4	Gardening
IAB10-5	Home Repair
IAB10-6	Home Theatre
IAB10-7	Interior Decorating
IAB10-8	Landscaping
IAB10-9	Remodelling & Construction
IAB11	**Law, Government & Politics**
IAB11-1	Immigration
IAB11-2	Legal Issues
IAB11-3	U.S. Governmental Resources
IAB11-4	Politics
IAB11-5	Commentary
IAB12	**News**
IAB12-1	International News
IAB12-2	National News
IAB12-3	Local News

IAB13	**Personal Finance**
IAB13-1	Beginning Investing
IAB13-2	Credit/Debt & Loans
IAB13-3	Financial News
IAB13-4	Financial Planning
IAB13-5	Hedge Fund
IAB13-6	Insurance
IAB13-7	Investing
IAB13-8	Mutual Funds
IAB13-9	Options
IAB13-10	Retirement Planning
IAB13-11	Stocks
IAB13-12	Tax Planning
IAB14	**Society**
IAB14-1	Dating
IAB14-2	Divorce Support
IAB14-3	Gay Life
IAB14-4	Marriage
IAB14-5	Senior Living
IAB14-6	Teens
IAB14-7	Weddings
IAB14-8	Ethnic Specific
IAB15	**Science**
IAB15-1	Astrology
IAB15-2	Biology
IAB15-3	Chemistry
IAB15-4	Geology
IAB15-5	Paranormal Phenomena
IAB15-6	Physics
IAB15-7	Space/Astronomy
IAB15-8	Geography
IAB15-9	Botany
IAB15-10	Weather
IAB16	**Pets**
IAB16-1	Aquariums
IAB16-2	Birds
IAB16-3	Cats
IAB16-4	Dogs
IAB16-5	Large Animals
IAB16-6	Reptiles
IAB16-7	Veterinary Medicine
IAB17	**Sports**
IAB17-1	Auto-Racing
IAB17-2	Baseball
IAB17-3	Bicycling

IAB17-4	Bodybuilding
IAB17-5	Boxing
IAB17-6	Canoeing/Kayaking
IAB17-7	Cheerleading
IAB17-8	Climbing
IAB17-9	Cricket
IAB17-10	Figure Skating
IAB17-11	Fly Fishing
IAB17-12	American Football
IAB17-13	Freshwater Fishing
IAB17-14	Game & Fish
IAB17-15	Golf
IAB17-16	Horse Racing
IAB17-17	Horses
IAB17-18	Hunting & Shooting
IAB17-19	Inline Skating
IAB17-20	Martial Arts
IAB17-21	Mountain Biking
IAB17-22	NASCAR
IAB17-23	Olympics
IAB17-24	Paintball
IAB17-25	Power & Motorcycles
IAB17-26	Pro Basketball
IAB17-27	Pro Ice Hockey
IAB17-28	Rodeo
IAB17-29	Rugby
IAB17-30	Running / Jogging
IAB17-31	Sailing
IAB17-32	Saltwater Fishing
IAB17-33	Scuba Diving
IAB17-34	Skateboarding
IAB17-35	Skiing
IAB17-36	Snowboarding
IAB17-37	Surfing / Bodyboarding
IAB17-38	Swimming
IAB17-39	Table Tennis
IAB17-40	Volleyball
IAB17-41	Walking
IAB17-42	Water-skiing / Wakeboarding
IAB17-43	World Soccer
IAB18	**Style & Fashion**
IAB18-1	Beauty
IAB18-2	Body Art
IAB18-3	Fashion
IAB18-4	Jewellery

IAB18-5	Clothing
IAB18-6	Accessories
IAB19	**Technology & Gaming**
IAB19-1	3-D Graphics
IAB19-2	Animation
IAB19-3	Anitvirus Software
IAB19-4	c/c++
IAB19-5	Cameras & Camcorders
IAB19-6	Cell Phones
IAB19-7	Computer Certification
IAB19-8	Computer Networking
IAB19-9	Computer Peripherals
IAB19-10	Computer Reviews
IAB19-11	Data Centres
IAB19-12	Databases
IAB19-13	Desktop Publishing
IAB19-14	Desktop Video
IAB19-15	Email
IAB19-16	Graphics Software
IAB19-17	Home Video / DVD
IAB19-18	Internet Technology
IAB19-19	Java
IAB19-20	Javascript
IAB19-21	Mac Support
IAB19-22	MP3/MIDI
IAB19-23	Net Conferencing
IAB19-24	Net For Beginners
IAB19-25	Network Security
IAB19-26	Palmtops/PDA's
IAB19-27	PC Support
IAB19-28	Portable
IAB19-29	Entertainment
IAB19-30	Shareware/Freeware
IAB19-31	Unix
IAB19-32	Visual Basic
IAB19-33	Web Clip Art
IAB19-34	Web Design / HTML
IAB19-35	Web Search
IAB19-36	Windows
IAB20	**Travel**
IAB20-1	Adventure Travel
IAB20-2	Africa
IAB20-3	Air Travel
IAB20-4	Australia & New Zealand
IAB20-5	Bed & Breakfasts

IAB20-6	Budget Travel
IAB20-7	Business Travel
IAB20-8	By US Locale
IAB20-9	Camping
IAB20-10	Canada
IAB20-11	Caribbean
IAB20-12	Cruises
IAB20-13	Eastern Europe
IAB20-14	Europe
IAB20-15	France
IAB20-16	Greece
IAB20-17	Honeymoons/Getaways
IAB20-18	Hotels
IAB20-19	Italy
IAB20-20	Japan
IAB20-21	Mexico & Central America
IAB20-22	National Parks
IAB20-23	South America
IAB20-24	Spas
IAB20-25	Theme Parks
IAB20-26	Travelling with Kids
IAB20-27	United Kingdom
IAB21	**Real Estate**
IAB21-1	Apartments
IAB21-2	Architects
IAB21-3	Buying / Selling Homes
IAB22	**Shopping**
IAB22-1	Contests & Freebies
IAB22-2	Couponing
IAB22-3	Comparison
IAB22-4	Engines
IAB23	**Religion & Spirituality**
IAB23-1	Alternative Religions
IAB23-2	Atheism / Agnosticism
IAB23-3	Buddhism
IAB23-4	Catholicism
IAB23-5	Christianity
IAB23-6	Hinduism
IAB23-7	Islam
IAB23-8	Judaism
IAB23-9	Latter Day Saints
IAB23-10	Pagan / Wiccan
IAB24	**Uncategorized**
IAB25	**Non Standard Content**
IAB25-1	Unmoderated UGC

IAB25-2	Extreme Graphic / Explicit Violence
IAB25-3	Pornography
IAB25-4	Profane Content
IAB25-5	Hate Content
IAB25-6	Under Construction
IAB25-7	Incentivized
IAB26	**Illegal Content**
IAB26-1	Illegal Content
IAB26-2	Warez
IAB26-3	Spyware / Malware
IAB26-4	Copyright Infrigement

Table 1.6

Values passed to indicate the type of device where the advertisement will be shown.

Value	Description
1	Mobile/Tablet - Version 2.0
2	Personal Computer - Version 2.0
3	Connected TV - Version 2.0
4	Phone - New for Version 2.2.
5	Tablet - New for Version 2.2.
6	Connected Device - New for Version 2.2.
7	Set Top Box - New for Version 2.2.

Table 1.7

Value passed to indicate the options for video bid response protocols.

Value	Description
1	VAST 1.0
2	VAST 2.0
3	VAST 3.0
4	VAST 1.0 Wrapper
5	VAST 2.0 Wrapper
6	VAST 3.0 Wrapper

Table 1.8

This is a list of API frameworks. Currently Improve Digital supports VPAID 1.0, VPAID 2.0 and MRAID-2.

Value	Description
1	VPAID 1.0
2	VPAID 2.0
3	MRAID-1
4	ORMMA
5	MRAID-2

Table 1.9

The following table lists the various video playback methods.

Value	Description
1	Auto-play sound on
2	Auto-play sound off
3	Click-to-play
4	Mouse-over

Table 1.10

The following table lists the options to indicate how the geographic information was determined.

Value	Description
1	GPS/Location Service
2	IP Address

Table 1.11

List of Improve specific consent values regarding ext.*improve_consent*.

Value	Description
0	No consent - Bid requests is sent without the personal data fields. User matching with 3rd parties will not take place.
1	Consent - Bid requests is sent with the personal data fields. User matching with 3rd parties will take place.
2	Legitimate interest - Bid requests is sent with the personal data fields. User matching with 3rd parties will take place.
3	Unknown consent and user in EU - Bid requests is sent without the personal data

	fields. User matching with 3rd parties will not take place.
4	User not in EU - Bid requests is sent with the personal data fields. User matching with 3rd parties will take place.
9	Unconfirmed legitimate interest from the publisher - Bid requests is sent with the personal data fields. User matching with 3rd parties will take place.

Annex A

Annex A: De-/Encryption of the winning price

To understand the encryption of the publisher_win_price, Improve Digital is providing a sample implementation in PHP.

Encrypting the publisher_win_price works as follows. Please note that the actual implentation on Improve Digital's side might be different from this, but it is compatible:

```
<?php

function _xor($text,$key){
  $outText = '';
  for($i=0;$i<strlen($text);) {
    for($j=0;($j<strlen($key) && $i<strlen($text));$j++,$i++) {
      $outText .= $text{$i} ^ $key{$j};
    }
```

```
 }
 return $outText;
}

$encoding_key = 'c422fdd0d81f';  // Encoding key and integrity key will
$integrity_key = 'fe3fd7dd8731'; // be exchanged between you and Improve Digital

$algo = 'sha1';                  // HMAC algorithm used
$price = 0.43;                   // Price to be encrypted. Up to 8 Bytes, treated as string

// 1. Create a (hopefully) unique 16-byte initialization string:
// This is an example and can be replaced by something faster if needed
$initialization_vector = substr(hash("sha256",
microtime(TRUE).rand(0,9999).time()),0,16);

// 2. Encrypt the price:
// The encrypted price is the result of a bitwise XOR (^) of the price and a HMAC-
Hash of
// the initialization string and the encoding key. Since xor does not bloat or shrink the
// encrypted string, we are already changing the input to 8 bytes.
//
// Common pitfalls:
// - Price to be encrypted MUST be a string. It will most likely behave unexpected if
//   treated as float
// - Hash has to be RAW output (TRUE Parameter). If missed out, lowercase hexits will
be
//   used and cause decryption to fail.
$encrypted_price = _xor( substr(number_format($price,8),0,8), hash_hmac($algo,
$initialization_vector,$encoding_key, TRUE ));

// 3. Create the integrity
// Another hash to be created to allow verification of the decrypted price. Integrity
// key instead of encryption key is used
// Only the first 4 Bytes are being used so the rest is omitted immediately.
$integrity = substr(hash_hmac($algo,
substr(number_format($price,8),0,8).$initialization_vector, $integrity_key, TRUE),0,4);

// 4. Glue the parts togetger
// 16 byte initialization string + 8 bytes encrypted price + 4 bytes of integrity will be
// base64-encoded
$out =  base64_encode($initialization_vector.$encrypted_price.$integrity);

// 5. Replace / with . and + with - to make the encoded string URL-safe.
```

```
$urlsafe = str_replace('/','_',str_replace('+', '-', $out));

echo $urlsafe; // Done
```

The previous snippet allows to create as many encrypted strings as you need for testing your decryption algorithm.

A sample implementation of the decrypter could look like this. You need to implement this logic into your adserving system to work with price encryption. There are solutions written in JavaScript. However, using them is rendering the encryption obsolete, because encryption key, integrity key and algorithm are visible to everyone. We recommend using these solely for testing.

```
<?php

function _xor($text,$key){
  $outText = '';
  for($i=0;$i<strlen($text);) {
    for($j=0;($j<strlen($key) && $i<strlen($text));$j++,$i++) {
      $outText .= $text{$i} ^ $key{$j};
    }
  }
  return $outText;
}

$encoding_key = 'c422fdd0d81f';     // Encoding key and integrity key will
$integrity_key = 'fe3fd7dd8731';    // be exchanged between you and Improve Digital

$algo = 'sha1';                     // HMAC algorithm used
$encrypted_string = 'NzgwMGE2YTBkYWI4NTk4Mukp8CTdA5.jexi3bg==';  // String to be
decrypted,
// usually from $_GET[]
// NOTE: Padding (symbols //'=') will be removed by
//encoder, so actual string to
//be decrypted will be:
//'NzgwMGE2YTBkYWI4NTk4Mukp8CTdA5.jexi3bg'
// Replace '_' with '/' and '-' with '+'
// This is done to not have non-urlsafe characters in the GET-parameter
$url_unsafe = str_replace('_','/',str_replace('-', '+', $encrypted_string));
//add padding, since it was removed by encoder
//note, code to add padding should be here

// Split the encrypted string into it's bits. 16, 8 and 4 bytes.
```

```
$initialization_vector = substr(base64_decode($url_unsafe),0,16);
$encrypted_price = substr(base64_decode($url_unsafe),16,8);
$integrity = substr(base64_decode($url_unsafe),24,4);

// Decrypt and generate integrity bits.
$decrypted_price = (string) _xor( $encrypted_price, hash_hmac($algo,
$initialization_vector,$encoding_key, TRUE ));
$integrity_check = substr(hash_hmac($algo, $decrypted_price.$initialization_vector,
$integrity_key, TRUE),0,4);

// Validate integrity
if ($integrity == $integrity_check) { echo "Integrity passed: "; }
else { echo "Integrity failed: "; }

// Echo decrypted price
echo $decrypted_price;
```