



TAG TrustNet Member Requirements
Content Verification providers (CV)

August 2021

Required Agreements

- TAG TrustNet Membership Agreement (signed with TAG)
- TAG TrustNet Licensing and Service Level Agreement (signed with Fiducia)

General Requirements

- Content Verification providers are required to receive Verified by TAG (<https://www.tagtoday.net/verified-by-tag>) status before applying for TAG TrustNet Membership.
- Content Verification providers are required to support a log level data product available to its clients compliant with specifications set out below, specifically the 'required' fields.

Log Level Data Accessibility Requirements

- Log level data access should be provided to clients promptly upon request by the contract owner.
- Log level data files should be provided with comprehensive documentation with detailed descriptions of all data fields provided, required data dictionaries.
- Impression events should be reported in compliance industry guidelines, e.g. IAB begin to render:
 - [http://www.mediaratingcouncil.org/Desktop-Display-Impression-Measurement-Guidelines-US%20\(MMTF%20Final%20v1.1\).pdf](http://www.mediaratingcouncil.org/Desktop-Display-Impression-Measurement-Guidelines-US%20(MMTF%20Final%20v1.1).pdf),
 - https://www.iab.com/wp-content/uploads/2016/12/Digital-Video-Impression-Measurement-Guidelines_1.1.pdf,
 - [http://www.mediaratingcouncil.org/Mobile%20In-App%20Measurement%20Guidelines%20\(MMTF%20Final%20v1.1\).pdf](http://www.mediaratingcouncil.org/Mobile%20In-App%20Measurement%20Guidelines%20(MMTF%20Final%20v1.1).pdf)

Log Level Data Ingestion Automation (Optional)

- To simplify the activation of a Content Verification providers log level data in TAG TrustNet for clients, provider should support the following mechanism:
 - Upon a client's request for a log level data feed enablement for an owned seat or account ID:
 - Start continuous upload of seat or account ID log files into TAG TrustNet Node Amazon S3 storage bucket provided by Fiducia, or
 - Enable seat ID or account ID log data in the data view shared with Fiducia Snowflake account using Snowflake Data Exchange;
 - Fiducia will configure a dedicated instance of TAG TrustNet Node for each Content Verification Provider, which will automatically share provided verification log level data with TAG TrustNet Nodes of Seat Id or account ID owners;
 - Data will be protected from unauthorised access end-to-end using encryption in transit and at rest.

Compliance with Data Protection Laws

- Log level data provided for ingestion into TAG TrustNet shall not include any Personal Data (as defined below) and, as such, should fall outside of the scope of any data protection laws, including, without limitation, the GDPR and the CCPA. All Personal Data, and any data fields which represent pseudonymous data, shall be removed from the data before it is ingested into TAG TrustNet. "Personal Data" means any information defined as "personal data," "personal information," "personally identifiable information," "nonpublic personal information," or other similar term under any applicable data protection laws.

Log Level Data Technical Requirements

The tables below list the type of data files required, the frequency, and format.

	Log Files Data Required	Frequency
Content Verification Provider	Impressions, Data Dictionaries	New log file entries shall become available continuously to Fiducia within 24 hours

Technical Requirements

- Content Verification Provider should not change data record contents in internal systems in a way that they will become out of sync with log level data provided to a client. If data restatement is required, then the account owners and TAG TrustNet should be informed in a timely fashion so impression events can be reprocessed.
- Impression log file records and database records provided to a client are deemed immutable in TAG TrustNet for the purpose of ad delivery audit.
- Impression log file records should be included in the log files no later than 48 hours after the impression event. Any impression log file record delivered beyond this time limit will be ignored for the purpose of ad delivery audit in TAG TrustNet.
- Timestamps for impression events should be determined server-side using an authoritative time source.
- Timestamps should always be reported in UTC time zone.
- If impression records are reported via database (e.g. Snowflake), they should contain both the impression timestamp and timestamp of data record insertion into the log database.
- As part of a Content Verification Provider log file delivery, data dictionaries allowing the mapping of impression record data fields to their meaning should be provided at least every 24 hours..
- Content verification provider should make sure that verification tags are installed in DSPs and ad servers with passthrough of variables required to fill log level data fields described below, especially "DSP Impression ID Passthrough".

Required and Recommended Data Fields

The following table details the required and recommended fields for impression events, with references to the OpenRTB specs where appropriate.

Field	Status	Description
Event Type	Required	Detailed type of the reported event: pre-bid check, ad blocking wrapper loaded, impression begin to render, click, conversion, etc. This may be reported as different events for subsequent matching or may be flagged as fields in the single impression event.
Timestamp	Required	The date and time of the impression event. Has to be reported in sync with authoritative time source in UTC time zone.
Account ID	Required	Content Verification Provider partner Account ID
Seat ID	Recommended	Partner's DSP seat ID

Country	Recommended	The country where the ad was served. For oRTB 2.x: <code>bidrequest.geo.country</code> , oRTB 3.x: <code>request.context.geo.country</code> .
Device Type	Recommended	The oRTB type of the device if available (oRTB 2.x: <code>bidrequest.device.devicetype</code> , oRTB 3.x: <code>request.context.device.type</code>). See device type in oRTB 2.5 table 5.21 or List: Device Types in oRTB 3.x.
OS Type	Recommended	OS type. This may differ by data provider and require creation of mapping dictionary.
Browser Type	Recommended	Browser type. This may differ by data provider and require creation of mapping dictionary.
City	Recommended	City.
Campaign ID	Required	The campaign ID passed from the DSP.
Insertion Order Number	Recommended	The insertion order number passed from the DSP.
Creative ID	Required	The creative ID passed from the DSP.
Verification Tag Type	Required	Vendor-specific type of verification tag used for the event (pixel, JS, VAST pixel etc).
Page URL	Required	Publisher site URL determined by verification provider.
Site Domain	Required	The publisher site domain (oRTB 2.x: <code>bidrequest.site.domain</code> , oRTB 3.0: <code>request.context.site.domain</code>).
App Bundle	Required	The app bundle (oRTB 2.x: <code>bidrequest.app.bundle</code> , oRTB 3.0: <code>request.context.app.bundle</code>).
App Store URL	Required	The app store URL (oRTB 2.x: <code>bidrequest.app.storeurl</code> , oRTB 3.0: <code>request.context.app.storeurl</code>).
DSP Impression ID Passthrough	Required	Passthrough variable filled by a DSP for verification provider tag with: <ul style="list-style-type: none"> The oRTB ID of the impression request and/or bid request using macro oRTB 2.x: <code>bidrequest.imp.id</code> and <code>bidrequest.id</code> oRTB 3.x: <code>bidrequest.item.id</code> and <code>bidrequest.id</code>; Vendor-specific DSP unique impression ID, e.g. <code>#{AUCTION_ID}</code> for Google Display Video 360.
Measurable	Required	Whether the impression is measurable for viewability.
inView	Required	Whether the impression was viewable and which viewability specification was applied (IAB, GroupM, display/video etc).

GIVT/SIVT	Required	Whether the impressions was classified as general or sophisticated invalid traffic.
Blocked Impressions	Required	Whether the impressions was blocked via blocking tag and the reason.
Monitored Impressions	Required	Whether the impressions was monitored for GIVT/SIVT and brand safety.
Brand Safety Score	Required	The impression's brand safety classification.