aqfer

Aqfer Universal Tag

Fast. Durable. Compliant.

Future-Ready Data Collection

TECHNICAL OVERVIEW

Aqfer Universal Tag (aUT) is a first-party tagging solution that allows for data collection from webpages, widgets on webpages, and advertising creative. aUT lets users actively and intelligently collect and identify data from digital channels while ensuring compliance with all data protection, privacy, and governance requirements.

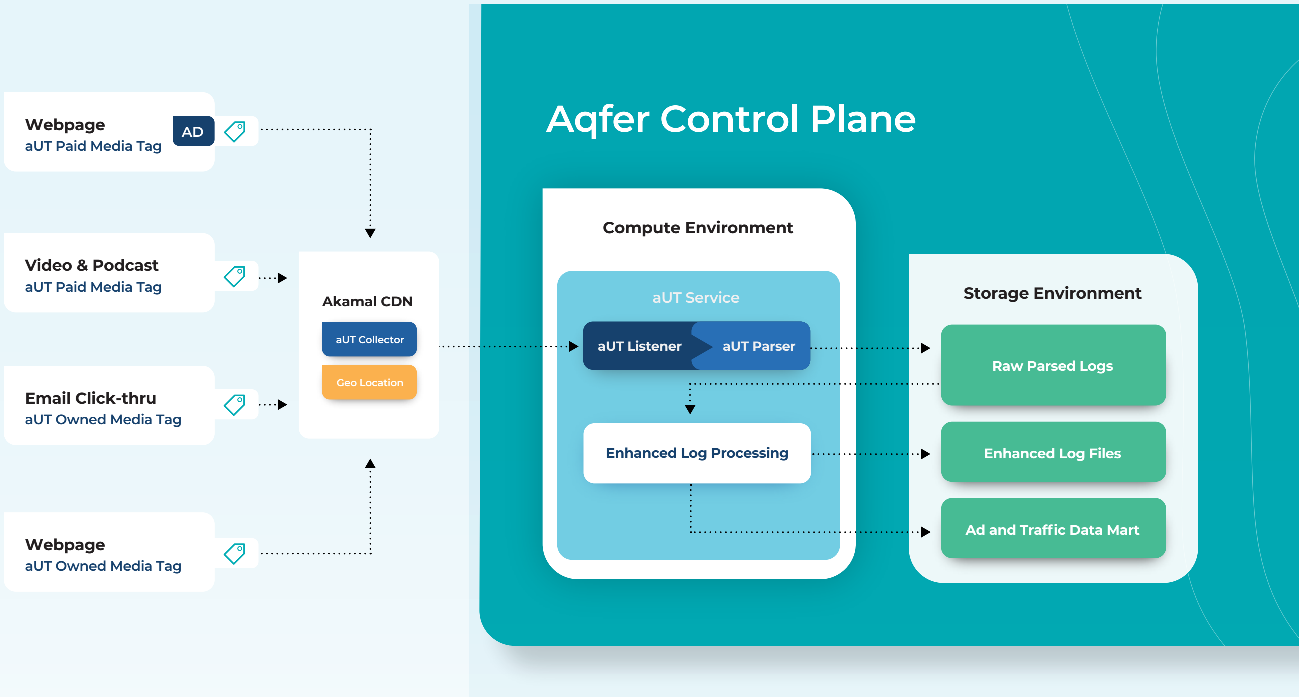
aUT is inexpensive, fast, easy to deploy and operate, has elastic scalability, is readily accepted by a wide range of publishers, and is able to perform privacy governance before data is collected or a cross-border data transfer. Since its inception more than 10 years ago, aUT has delivered billions of owned and paid media tags per day for Aqfer's clients, including many Fortune 50 companies.

The solution supports flexible data gathering and first- and third-party cookie management, offers customizable privacy and security controls, and provides the ability to coordinate the invocation of additional tags (i.e. beacons).

Examples of advanced aUT capabilities include:

- Setting and confirming client-persisted unique identifiers (such as cookies) via HTTP header
- Calculating statistical identifiers for user agents and collecting data about the context in which the tag is invoked
- Recording parameters passed in the query string section of the URL for an HTTP GET request
- Passing information between various services through HTTP requests
- Intelligent management of the insertion of partner tags
- Paid media tracking for impressions, clicks, and engagement across display, video, and audio ads

aUT Components and Architecture



Aqfer Universal Tag has five major architectural components:

aUT Tag

The aUT tag is either an empty image (pixel) or a JavaScript file invoked by a URL. The tag also includes an optional "wrapper," which is JavaScript that can be pasted into a webpage or inline frame (iframe) that invokes additional tags in the browser. This wrapper JavaScript is automatically generated by the aUT Portal.

(Note: Other industry terms for this component include pixel, beacon, and tracker.)

aUT Collector

The aUT Collector consists of logic running on the Akamai Content Delivery Network (CDN) that controls:

- What tag content is downloaded
- What headers are included in the HTTP response to the initial tag request (including SET-COOKIE headers)
- The need for any redirect logic and the destination of the redirect
- The application of any privacy governance rules
- What data is sent back to the aUT Listener in the Download Receipts

aUT Listener

Micro-batches of log records, known as download receipts (DLRs), are sent continuously from the aUT Collector to the aUT Listener, which is hosted on a cloud service provider (CSP) in a region close to the browser. aUT Listener then streams those micro-batches to the aUT Parser. It is located in the aUT Service.

aUT Parser

The aUT Parser converts the log record layouts to an open format. Some clients may have unique, dedicated Akamai CDN configurations while some will share a configuration with other clients. In the latter case, the data is split by the aUT Parser into isolated data stores. These log records are at a 1:1 ratio with all HTTP request activity from the browser for each client and are sometimes referred to as "Parsed Receipts." It is located in the aUT Service.

Enhanced Log Processing

The Enhanced Log Processing (ELP) component utilizes Aqfer's big data processing framework to create logical events out of the detailed Parsed Receipts. For example, a large payload tag may be split into multiple requests. The ELP component stitches those records together into a single business event. Similarly, a redirect to verify cookie acceptance will be merged with the original log record from the cookie-setting response.

These ELP logical event logs are made available to the client, but also processed into a data mart with data structures useful for advertising campaign analytics or web traffic analysis.

How aUT Operates

To capture data using aUT, aUT API calls are invoked by embedding an image or script fragment (i.e. the aUT Tag) into an HTML webpage or by making an HTTP GET request for a specific object from the aUT Collector, which is an HTTP edge-deployed server on the Akamai CDN. The logic for what data is captured and downloaded by aUT Tag is controlled by the aUT Collector.

The aUT API supports a variety of different atomic and container tag types, all of which support a specific combination of behaviors. The aUT Tag also provides a JavaScript data layer that facilitates the collection of data from other webpage data or code.

The data captured by the aUT Tag is then sent in continuous log record micro-batches from the aUT Collector to the aUT Listener. These log record micro-batches are then sent from the aUT Listener to the aUT Parser, which converts the log record layouts into open formats known as Parsed Receipts.

The Parsed Receipts are then sent to aUT's Enhanced Log Processing component, which stitches them together to create logical event logs. These enhanced log files are then sent to a secure data mart in the client's environment in AVRO or Parquet format, and a clone of the file set that is organized and structured for common analytics is sent to a separate secure data mart.

From there, the data can be further analyzed and activated using additional Aqfer solutions or existing solutions found in the client's tech stack ecosystem.

Compliance and Consent "On The Edge"

aUT is deployed as an edge-based tag management solution via Akamai, a global content delivery network (CDN) and cloud services provider. Akamai is the world's largest CDN and the most reliable, widely-used, and geographically-distributed CDN in existence.

Running all code that talks to a consumer browser on the edge via the Akamai CDN has several notable advantages over running entirely on Web browser:

- JavaScript files are much smaller
- Total HTTP requests per tag can be reduced in many scenarios through intelligent JavaScript selection
- Data collection can be prevented when not authorized or desired
- Privacy governance occurs at the edge, which is typically in the same jurisdiction as the consumer
- When the website the tag is placed on uses the same CDN (in this case, Akamai), first-party cookies are more reliable

aUT's edge-based deployment gives clients the ability to make granular decisions about what data to collect (or not collect) based on the consumer's physical location. aUT clients can create and deploy customized aUT Tags that adhere to the data privacy regulations of the region/jurisdiction where the consumer's data is being captured.

aUT Eliminates Cross-Border Data Collection Issues

This essentially creates a “privacy firewall” that prevents unauthorized cross-border data collection or transfer that adheres to prominent consumer privacy regulations. Because the logic and data capture both occur on the edge, the client is never in possession of consumer information they should not have at any point.

For example, if the consumer is based in the E.U., the aUT Tag can be configured to capture only the information allowed per GDPR consumer data privacy requirements. If consent is given by the consumer, standard aUT data is logged; if consent is not given, then no personal/pseudonymous data is logged. This same ability also applies to consumer data privacy laws and regulations currently established by various individual U.S. states (CCPA, for example).

aUT’s privacy framework is also compliant with the IAB’s recently-established Global Privacy Platform protocol.

aUT Tags are editable through Aqfer Portal, so if/when existing privacy requirements change or new legislation is enacted, clients can easily update their existing aUT Tag(s) to match the new requirements. Aqfer Portal also allows clients to save and re-use the aUT Tag Templates they’ve created for easy editing and re/deployment.

Low Latency, High Uptime

aUT provides clients with a low latency tagging solution that simultaneously has extremely reliable uptime thanks to its edge-deployment via the Akamai CDN and an extremely efficient proprietary code.

The Akamai CDN operates over 150,000 servers around the globe, meaning that the consumer’s Web browser and aUT are always operating in extremely close proximity to one another. Additionally, the proprietary aUT code that executes on Akamai’s servers minimizes network round trips and JavaScript size when JavaScript deployment is required. Further, this proprietary code allows complex logic, such as aUT’s privacy governance rules, to be executed in close proximity to the user. Together, these ensure low-latency operation of aUT.

aUT’s edge-deployment via the Akamai CDN also makes it one of the most reliable tagging solutions available on the market. To put things bluntly: essentially, If Akamai isn’t working, the entirety of the Internet isn’t working. Given Akamai’s impressive history of reliable uptime and functionality, aUT’s deployment on its servers makes it one of the fastest-firing and most-reliable first-party tagging solutions available today.

Lasting Durability Thanks to an HTTP Approach

Deployment of the aUT Tag requires a tag-specific subdomain to be configured via the client's Domain Name System (DNS). This is achieved via aUT's intelligent DNS and CDN-based approach which ensures that Web browsers view the aUT Tag as an extension of the client's own infrastructure rather than a third-party tagging solution. It also ensures that cookies placed via the aUT Tag are secure server-side, first-party cookies (i.e., via HTTP Response headers), so that full cookie durability and reliability are maintained.

Just as with other first-party cookies set directly by a website, expiration dates can be set to a maximum. Historically, this maximum has been set to two years, although recent changes have limited that to 400 days. Moreover, aUT's approach has been shown to withstand the scrutiny of Apple Safari's Intelligent Tracking Protection protocol which would otherwise truncate the cookie expiration date to seven days.

Once the aUT Tag-specific subdomain has been configured (often t.brandname.com or a similar pattern), it can be added to the client account in the Aqfer Portal. From here, the specific uses of the aUT Tag can be configured for owned and paid media tracking use cases.

aqfer

To learn more,

visit us at www.aqfer.com

or contact us at info@aqfer.com