Delivery and Security Service

Ion, DSA, GTM, Media, Kona
Delivery of Web Properties via the Akamai Platform:

- The end user request accesses the Akamai edge server that is closest to the end user. Where the end user is located in the EU, an edge server in the EU will answer the request (grey lines).

- The edge server transmits the request via the Akamai Platform to the origin server of the customer. On the way back to the end user, the origin server forwards the web properties via the Akamai Platform back to the end user (orange lines).

- The customer chooses the security of its web properties. For sensible web properties, Akamai recommends to choose the Akamai Enhanced TLS Platform for transmission.

- On the Enhanced TLS Platform, the TLS connection is terminated for an instance by Akamai at the edge server to perform routing and mapping and security checks. Immediately thereafter the TLS connection is re-established.
Delivery of Web Properties via the Akamai Platform:

- The customer determines whether the web properties are cached/stored on the edge servers or not.

- Where customer’s web properties consist of personal data, Akamai recommends to choose a no-cache configuration for such data, to avoid the accessibility of such data by all end users. Such configuration ensures that the web properties transmit the Akamai edge servers only without being stored.

- Cached data elements instead are stored on the edge server and accessible by every end user for the cache period determined by the customer in the service configuration.
Delivery of Web Properties via the Akamai Platform:

- Where malicious activities are recognized at the edge server, the request is blocked (red lines).
- Where the web properties are safe, they are transmitted via the Akamai Platform (grey lines).
- As Akamai does not know when, and where an end user request hits an edge server, it does not control which server delivers which web properties or when and where a TLS termination occur.
Delivery of Web Properties via the Akamai Platform:

• So, by nature of the Akamai Platform the Privacy by Design principle is met: Where an end user located in the EU is requesting web properties of a customer, the web properties and the embedded personal data (if any) are processed on Akamai servers deployed in the EU, except for corner cases like e.g. BGP high jacking or congestions of all EU internet connections.

• With more than 100,000 Akamai servers deployed in the EU region, a fast reliable and secure delivery is ensured within region per default.
Security of Web Properties via the Akamai Platform:

- For Akamai’s service Kona, customer security rules, Akamai rules and Akamai’s threat intelligence are applied locally at the edge server.

- When an end user request hits an edge server, the security analytics are performed on the edge server:
  - safe requests being transmitted;
  - malicious requests being blocked;
  - suspicious requests being analyzed

- For safe requests by end users located in the EU, the customer’s web properties are processed in the EU. No data is transferred outside the EU, except for corner cases.

- Suspicious requests are transferred to the US for analytics on Akamai’s security systems deployed in the USA.

- For all Akamai services log processing and support service processing are outlined on slide 30 ff.
Akamai Platform Data Flow:

1. **User Agents**
   - Browsers
   - Mobile apps
   - IoT devices

2. Akamaized domains
   - www.customer.com
   - api.customer.com
   - login.customer.com

3. Akamai Enhanced TLS
   - Optional
   - Load Balancing
   - Kona (WAF)
   - Client Reputation
   - Bot Manager

4. Customer managed Edge services
   - Request is processed as configured by the customer.
   - E.g., if customer uses Kona, the request will be checked for matches with known attack patterns and malicious requests can be blocked.
   - If customer uses Bot Manager, the request will be checked for known bot patterns and blocked, or allowed or delivered with alternate content.

5. The server re-encrypts the request and sends it to the customer Origin.
   - The request content is now encrypted and is not retained on the server.

6. The server re-encrypts the response and sends it to the customer Origin.
   - The response from the Origin is sent to the Akamai Edge server over encrypted channel.

7. Origin (customer) domains
   - origin.customer.com
   - origin.api.customer.com
   - origin.login.customer.com

8. Origin (customer infrastructure)
   - The response from the Origin is sent to the Akamai Edge server over encrypted channel.


10. The request is directed to the Akamai Edge server.

11. The Akamai server terminates TLS connection and decrypts the request in a memory for processing.

12. The server checks customer configuration to know how the request should be processed.

13. The Akamai server terminates TLS connection and decrypts the request in a memory for processing. Then customer configuration is checked to determine whether the response should be cached for future requests. If the response should not be cached, it is immediately re-encrypted, never stored on a disk. Then the response is sent to the end user over encrypted channel.

© 2021 Akamai | Global Data Protection Office | AKAMAI CONFIDENTIAL, NDA REQUIRED
Enterprise Application Access

EAA
Enterprise Access Accelerator:

Based on the Zero Trust principle, EAA’s purpose is to ensure that only authorized and authenticated individuals access the applications they need to access.

The EAA Client (running on user’s computer) connects to the EAA Cloud (i.e., a proxy that runs in the cloud).

The EAA Connector runs behind the customer’s firewall in the customer’s data center and continuously makes “outbound” connections through the firewall to the EAA Cloud, checking for incoming Client connections.

When the Connector detects an inbound connection from an EAA Client to the EAA Cloud, the Connector performs the dual tasks of (i) **Authentication** (i.e. “who are you?”) and (ii) **Authorization** (i.e. “what are you permitted to do upon access?”).

The Connector relies on the customer’s employee directory and IDT to authenticate and authorize.

Then, the Connector “stitches together” the two connections, providing a tunnel through the firewall and into the customer’s networks so that the user can access authorized resources.
Enterprise Access Accelerator:

**Front End Authentication**: Occurs between the user’s browser and the EAA Cloud server to which the user connects to use the EAA service. Usually, this step prompts the user for a username and password (if the user has not already authenticated to the EAA SSO service).

**Back End Authentication**: Occurs between the EAA Cloud and the Application server. This process uses the authentication method that the requested application is programmed to accept (e.g., Kerberos, SAML, etc.).

**Authorization**: Whereas Authentication confirms who the requestor is, Authorization confirms which resources the requestor is permitted to access.

The Front End Authentication ensures that EAA collects the information needed to craft the proper Back End authentication method – so the user only logs in once.
Enterprise Access Accelerator:

- The Customer's directory with the employee corporate contact details gets copied into the EAA Cloud.
- The EAA Cloud runs on AWS and EAA can be configured so that the customer's employee directory in the EAA Cloud is stored in region.
- With this Privacy by Design feature, EU personal data for legitimate access is processed within the EU only.
- Logs of malicious events (e.g. brute force attack) are transferred to the USA and analyzed in Akamai's security analytic systems. Such events are not performed by individuals, but by bots, so the related IP addresses are not to be classified as personal data.
Enterprise Threat Protector

ETP
Enterprise Threat Protector:

ETP offers different use cases:

- DNS based threat detection only (for companies with full security stack inside).
- DNS+suspicious Web Traffic via Security Proxy (companies who are in the cloud transformation phase or have completed this phase).
- DNS + all Traffic via Security Proxy (companies who want additional visibility and security on top of cloud security).

ETP protects at 3 layers:

- DNS inspection at DNS servers
- URL inspection at ETP Proxy Platform
- Payload analysis at ETP Proxy Platform.

Malicious traffic is determined in accordance with

- Customer rules,
- Akamai rules, if desired,
- Akamai’s threat intelligence.

Recognized malicious traffic is blocked at the Akamai Platform.
Safe traffic is forwarded to the internet.
Enterprise Threat Protector:

- By nature of the Akamai Platform, end user requests within the EU are answered by DNS servers deployed in the EU.
- Akamai’s threat intelligence is applied locally at the edge server. Safe traffic is forwarded to the internet.
- Logs are generated on the edge server when performing ETP services and transferred to Akamai’s log collection system in the USA for traffic and security analytics.
Enterprise Threat Protector:

- Data elements embedded in the logs:
  - End user IP address
  - Time stamp
  - DNS data
  - Browser data
  - Network data

- The end user IP address may relate to a corporate proxy. So, it is not necessarily to be classified as personal data.
Edge DNS

GTM
Edge DNS and GTM:

- Edge DNS and GTM are Akamai’s external authoritative DNS services.
- Edge DNS provides DDoS resilient zone management.
- GTM provides secure and extensible layer 3 global service load balancing.
- Personal Data processed is end user IP address. IP address might relate to a corporate proxy and may not necessarily be classified as personal data.
- The customer determines security rules to apply. Akamai may apply additional rules. Finally Akamai’s threat intelligence is applied and the rules and the intelligence are rolled out to the DNS servers.
- In accordance with the rules and the intelligence, safe requests are forwarded to the internet and malicious requests are blocked.
Bot Manager Premier

Account Protector and Page Integrity Manager
Data is collected to determine whether access has been made by a **human or a bot.**

- Data elements include network, browser and behavior data.
- Akamai’s threat intelligence is applied.
- End User IP Addresses are **pseudonymized data** for Akamai.
- Akamai does **not identify the end users** as this is not required for the bot detection.
- Akamai is **not creating end user profiles.**

Web property’s access is **forwarded or blocked,** in accordance with the customer’s security rules, Akamai’s rules and Akamai’s treat intelligence.

The cookie technology used is **strictly necessary** for the operation of the customer’s website and offering of its services.

Bot Manager Premier has been developed with **Privacy by Design** in mind.

The log files collected are **transferred to the US and stored there for 90 days** for **security analytic purposes.**

Details are outlined in the **Privacy by Design BMP Whitepaper.**
Prolexic

DDoS Protection
**Prolexic Services:**

- Prolexic is a DDoS mitigation solution.
- The personal data element processed, is the end user IP address.
- When the service is enabled, the inbound traffic to the customer is directed to a scrubbing center on the Prolexic platform.
- There the traffic is analyzed for layer 3, 4 and 7 attacks. The traffic remains encrypted at all times. TLS termination is not required.
- Safe traffic is forwarded to the customer’s infrastructure.
- Malicious traffic is blocked and further analyzed.
- The security event logs are transferred to Akamai’s security systems in the USA for further analytics. IP addresses belong to devices used by bots, not by humans. Logs are stored in the USA for 90 days.
Prolexic Services:

- Scrubbing Centers are deployed on the Prolexic Platform in the EU, Asia, the USA and the Americas to ensure global coverage and best protection against DDoS attacks.

- While per default for EU based end users scrubbing centers in the EU are chosen, depending on the workload a failover to scrubbing centers in other regions may occur, in particular in case of large attacks, to ensure the availability of the customer website.

- Akamai does not limit the usage of scrubbing centers to one region to ensure best mitigation of DDoS attacks.
Akamai Identity Cloud

AIC/CIAM
Akamai Identity Cloud Services:

- **AIC** is an **end user identity management service** on top of Akamai’s web performance services.

- Personal data elements processed relate to the **identity of the end user**, e.g.:
  - Name
  - Email
  - Address
  - Phone number
  - Age
  - Gender
  - Shopping history (e.g. shoe size, preferred toothpaste).

- Personal data elements is collected by the customer, not by Akamai. Akamai is *hosting and securing* the Akamai Identity Cloud only.

- The Akamai Identity Cloud runs on **AWS** as Akamai’s sub-processor.

- The **customer** determines via the service configuration the **storage location of the end user identities** (USA, EU or APJ).
Akamai Identity Cloud Services:

- Akamai’s web performance service ensures availability and security of the customer web properties via the Akamai’s Platform.
- Logs are created as outlined in the slides on Log Processing.
- For details how AIC assist to comply with data subject rights and other privacy requirements see this AIC Privacy Whitepaper.
Access Controls:

- **Limited access** to end user identities for the customer employees based on roles, responsibilities and application type/use.

- Access only in accordance with need to have principle.

- Fine-grain control down to the level of individual data record fields and columns.

- Access is **logged** and can easily be tracked in case of abuse.

- These controls meet the Privacy by Design principle.
mPulse

Web Performance Services
mPulse Service:

- mPulse is a web performance analytic service.

- Personal data element processed is the end user IP address.

- The end user IP address is anonymized at the edge server. No personal data is processed anymore.

- Where the edge server is deployed in the EU, personal data is processed only in the EU.

- The data is then transferred to the mPulse portal deployed in the USA and analyzed there.

- Analytic reports are created and made available to the customer via Akamai's Control Center.

- Details are outlined in the whitepaper mPulse Compliance with global data protection laws.
Log Processing

Applicable for all Akamai services
Traffic and Security Analytics

- Log files consisting of logged data **collected at the edge server** the moment a request hits the edge server.

- The logs are **transferred** from the edge servers to Akamai’s **log collection system** deployed in the USA, for traffic analytics, routing and mapping purposes.

- From their logs are **forwarded** to Akamai’s **security analytic system**, deployed in the USA, for security analytics.

- **Reports** of the analytics are created, which are made available to customers in Akamai’s Control Center. For some services Akamai also makes available the logs to the customer.

- **Log Retention periods:**
  - **Couple of hours** on the edge server.
  - **40 days** on the log delivery system.
  - **90 days** on the security analytic system.

  Where required from a security perspective, logs are retained for **180 days** (e.g., to track a new attack vector across the regions).
Support Services

Applicable for all Akamai services
In case of a service incident, the customer creates a support ticket.

The ticket is stored in Akamai’s Salesforce Platform, which is deployed in the USA.

Akamai’s AkaTech team handles the incident by pulling logs related to the incident from the log collection system or the edge server.

Logs consist of end user IP address.

Logs with embedded end user IP address are stored in the ticket (= in the USA) and made available to the customer.

End user IP addresses are deleted 14 days after ticket closure.
Risks of Access to Logs by 3rd Parties:

- The data transferred by Akamai to the USA is in most of the cases the end user IP address.

- Akamai is not classified as an e-communication service provider under US laws. So, FISA 702 is not applicable to Akamai. In addition, the US government confirmed that they are not interested in accessing IP addresses or other meta data for surveillance purposes. [https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF](https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF)

- In addition, Akamai cannot single out specific web properties transmitting its platform. The web properties are encrypted and only Akamai customers' control what data elements their web properties consist of and how they are encrypted.

- There are more easy ways to access the web properties transmitting the Akamai Platform, e.g. requesting the data from an ISP, who not only process the end user IP address, but also the related end user contact details. So, even where Akamai would be subject to access requests, since there are more easy ways to get the data, such data will likely be requested from other parties.

- While Akamai regularly receives law enforcement request, it does not hold the requested data: contact details related to end user that accessed an (Akamai edge server) IP address at a certain point in time. As Akamai stores logs only for 40 days on its data collection system, in most of the cases Akamai has already deleted the logs relating to the access at the time of the request receipt. Even where Akamai still retains the logs, as it is not an ISP, Akamai does not hold contact details of its customer’s end users.

- So, all Akamai can do, is look up the logs related to the time of the request, look up to which of its customers the logs relate to, notify that customer about the law enforcement request and ask them to handle the request and clarify back to law enforcement Akamai’s role.
Risks of Access to Logs by 3rd Parties:

- Finally, Akamai does not voluntarily allow 3rd parties to access data processed on its systems and challenges any non-legitimate request. A wire tap requested by 3rd parties to be implemented, would require tapping all Akamai server and all logs during a given time period, irrespective of the customer the logs relate to. Such a request is excessive, not legitimate and would be challenged by Akamai.

- Security wise, Akamai protect the logs transferred to the USA by strict access controls against unauthorized access. An overview of the controls has been shared with the customer.

- In addition to the access controls, an end user IP address in the logs is a pseudonymized data element for Akamai, as Akamai does not identify the end users via the IP address they use.

- Please also take a look at our publicly facing data transfer statement: [www.akamai.com/compliance/privacy](http://www.akamai.com/compliance/privacy).