Akamai and FedRAMP

The Akamai Intelligent Platform™ has a Federal Risk and Management Program (FedRAMP) Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO), which is the most technically rigorous authorization to obtain. This is the first — and presently, only — JAB P-ATO granted to a globally distributed, publicly shared cloud services platform. U.S. government agencies can leverage Akamai cloud services directly or use them to front-end other FedRAMP-compliant data center solutions. This model offers a unique end-to-end FedRAMP-compliant solution that is designed to make it easier for agencies to use shared cloud services in support of their computing initiatives.

About FedRAMP

FedRAMP is a U.S. government-wide program that standardizes the approach to security assessment, authorization, and continuous monitoring for cloud products and services. The JAB comprises the Chief Information Officers of the Departments of Defense (DoD) and Homeland Security (DHS) and the General Services Administration (GSA), who lead the management of the program with the National Institute of Standards and Technology (NIST).

FedRAMP Federal Risk Authorization Management Program

Akamai Components and Boundaries

Throughout the FedRAMP System Security Plan (SSP) documentation and control responses, the use of the system name, Akamai Content Delivery Network (CDN), is inclusive of the system components and boundaries used to provide customer-facing services as well as Akamai internal mechanisms used to manage and maintain the Akamai CDN. Both customer-facing services and Akamai internal mechanisms that constitute the accreditation boundary are described in the "Akamai CDN System Security Plan (SSP) document" located in the FedRAMP repository.

Akamai provides the following services:

- **Content Delivery:** The Akamai Intelligent Platform™ optimally resolves end-user requests for content using a massive server infrastructure with more than 240,000 servers deployed in more than 130 countries worldwide.
- **Secure Content Delivery:** Information that is protected by the Transport Layer Security (TLS) protocol is delivered from a dedicated, highly secure portion of the Akamai CDN over HTTPS. The Secure CDN was designed by Akamai's security experts to meet robust levels of physical, network, software, and procedural security.
- **NetStorage:** This secure, cloud-based solution was designed to meet the needs and requirements of high-performance storage. As a key element of the Akamai product portfolio, NetStorage is built for constant availability, offering many essential features to optimize reliability for the end user, including geo-replicated storage of digital content (including images, streaming media files, software, documents, and other objects). The upload to NetStorage is done via either FTP/RSync/SCP/SSH/SFTP.
- **Media Services Live:** Akamai's purpose-built architecture offers several key capabilities, known as liveOrigin™, that operate in concert to bring the TV experience to online audiences at scale. These capabilities bridge the gap between live streaming and broadcast, to provide unmatched consistency, quality, and reliability of viewing experience.

Service Name
Akamai Content Delivery Network (Akamai CDN)

Service Model
Infrastructure-as-a-Service (IaaS)

Deployment Model
Public Cloud

Impact Level
Moderate

Authorization Date
August 22, 2013
(JAB Provisional Authorization)

Package ID
MF1206061353

3PAO Knowledge Consulting Group, Inc. (KCG) FedRAMP Accredited

Contact Information
See the FedRAMP Marketplace.
Link to:
https://marketplace.fedramp.gov/#/product/content-delivery-services?sort=productName)
for more detail.

For additional information or questions related to Akamai's FedRAMP authorization, contact **fedramp_info@akamai.com**.

Federal Risk and Management Program (FedRAMP)

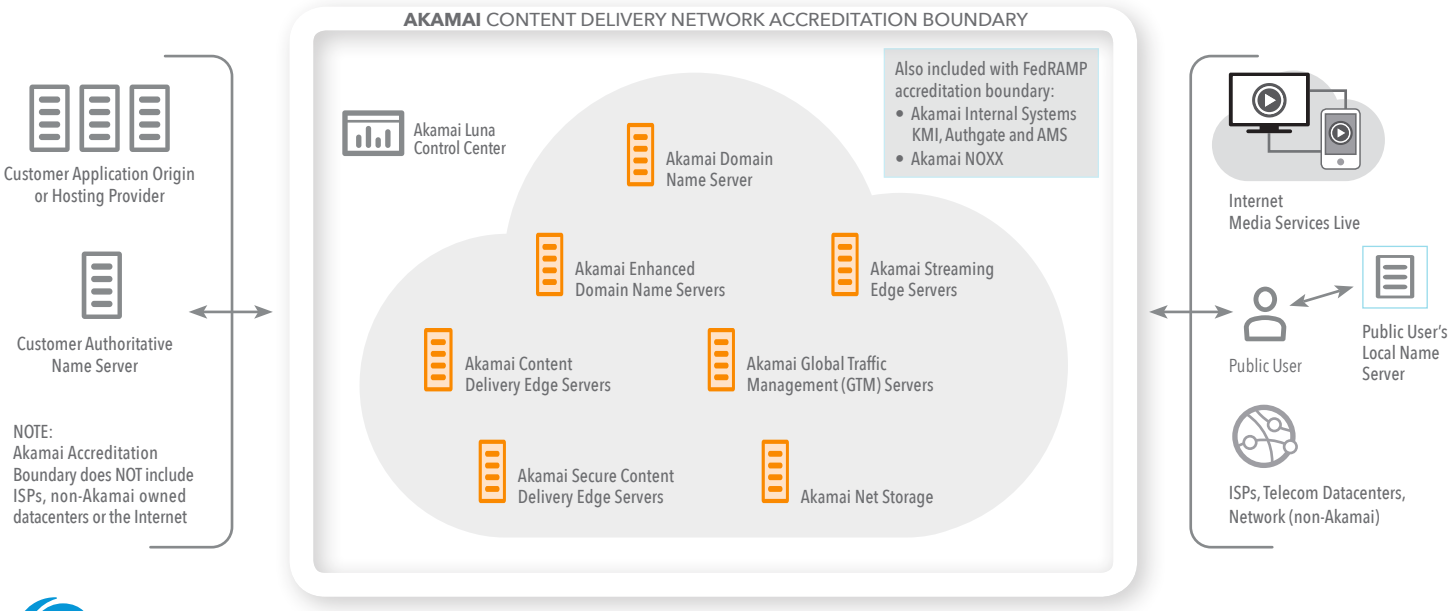
- **Global Traffic Management Service:** Global traffic management (GTM) can be combined easily with other Akamai services to provide powerful and highly available web delivery solutions. GTM offers different modules for traffic control in a variety of situations. All modules are built on a common fault-tolerant, globally distributed name server infrastructure.
- **Enhanced Domain Name System:** Akamai's Enhanced Domain Name System (DNS) service provides websites with a robust, reliable, and scalable outsourced DNS solution designed to dependably direct end users to website applications. Using a secondary DNS approach, Enhanced DNS makes it possible for organizations to leverage a distributed network of DNS servers while retaining their existing management and update processes for DNS zone administration; customers using Enhanced DNS can enable DNSSEC.
- **Luna Control Center:** As the Akamai customer portal interface, the Luna Control Center offers flexible organization, interactive reporting, and diagnostic tools to proactively research, troubleshoot, and resolve anomalies. Accessed via HTTPS, customers can monitor activity, configure and administer Akamai solutions, deploy and manage content, analyze business-critical information, resolve issues, plan events, and collaborate with the Akamai team.

The following Akamai internal mechanisms are also included in the Akamai CDN accreditation boundary:

- **Key Management Infrastructure:** The KMI is Akamai's standardized system for the generation of escrow, distribution, and access control for private information.
- **Authgate:** Akamai's authorization gateway verifies that users are connected to the Akamai corporate network. It also verifies that they are connected to a computer with an Akamai certificate, have an SSH key that matches their identity, and can connect to the machine they wish to access.
- **Alert Management System:** The AMS oversees Akamai's deployed networks in real time and sends alerts to Akamai's Network Operations Control Center (NOCC), which runs continuously. Logs are stored for forensic purposes and are accessible via a reporting tool.
- **Akamai's Domain Name Servers:** Akamai operates a dynamic DNS that returns answers computed on the fly. A typical use is to return the IP address of a server that is assigned dynamically, given current conditions on the Internet.
- **Network Operations Command Center:** The Akamai NOCC is distributed across four locations: Cambridge, Bangalore, Krakow, and Santa Clara. It enables proactive monitoring and troubleshooting of all servers in the global Akamai network.

Summary

Akamai's achievement within the FedRAMP program allows the U.S. government to leverage secure, commercially available cloud services without having to build government-only clouds. Public sector organizations of all types can trust the Akamai Intelligent Platform™ as the secure foundation for their cloud computing projects. Public sector entities can also leverage Akamai's accredited services to meet IPv6, HTTPS, and DNSSEC OMB mandates.



Akamai

As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai, please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 04/18.