Attestation of Compliance

PCI DSS 3.2.1

June 2020

(Amended October 2020)

Introduction

The attached document is Akamai's Attestation of Compliance with the Payment Card Industry Data Security Standard (PCI DSS) version 3.2.1. This document serves as a declaration of our compliance status, and evidence that Akamai, as a third-party service provider, has the ability to protect sensitive data including but not limited to cardholder data. It also demonstrates our commitment to our customers who rely on our Secure Content Delivery Network with Enhanced TLS ("Secure CDN"), Page Integrity Manager, mPulse web performance management, and Bot Manager Premier bot defense solutions for their business, as well as their own compliance initiatives.

PCI DSS and Akamai Services

Akamai's services that may be used in a PCI DSS compliant manner include the following:

- Secure CDN with Enhanced TLS, and the services running on it;
- Cloud security products such as and Kona Site Defender and Bot Manager, when running on the Secure CDN;
- Page Integrity Manager;
- Bot Manager Premier, which also includes components running on the Secure CDN, and additional intelligence currently utilizing Amazon Web Services (AWS), and which requires the use of JavaScript within the PCI DSS cardholder data environment; and
- mPulse digital performance management services, which also utilize the Secure CDN, AWS, and JavaScript in the cardholder data environment;

Secure CDN with Enhanced TLS

Akamai's Secure CDN with Enhanced TLS[1] is the core component of its PCI compliant content delivery services. The servers in this network are physically secured against intrusion while being widely distributed around the globe to ensure availability and maximize origin offload. The

[1] Akamai now offers two levels of TLS delivery over its Secure CDN: Enhanced TLS, which is Akamai's longstanding secure CDN, and Standard TLS, a newer CDN offering intended for less sensitive data, that permits customers to provision their own TLS certificates and deliver traffic over HTTPS. Only Enhanced TLS is approved for use with cardholder data in accordance with PCI DSS. Unless otherwise noted, references to the Secure CDN refer to the Secure CDN with Enhanced TLS.

Secure CDN also provides customers with custom TLS certificates with the flexibility to configure them to satisfy various security and business requirements. The Secure CDN is not typically sold as an independent service but is instead a feature included with most of Akamai's web performance and cloud security products, as described below.

Web Performance Solutions

Akamai's web performance solutions, including Ion and legacy CDN solutions such as Terra Alta or Dynamic Site Delivery, typically have the option of having their content delivered securely, in which case that content is delivered via the Secure CDN, and may be used in a PCI DSS compliant manner. Additional products, such as mPulse digital performance management, Cloudlets, and dynamic content delivery options such as adaptive image compression and pre-fetching options, have all been designed to work on Akamai's Secure CDN servers, and may be configured to be fully compliant with PCI DSS.

Cloud Security Products

As with the web performance solutions, Akamai's Kona Site Defender and Bot Manager cloud security products may be configured to operate over the Secure CDN in a PCI DSS compliant manner. In addition, the web application firewall (WAF) components of Kona Site Defender and Web Application Protector may be used by customers to help satisfy their obligations under PCI DSS Requirement 6.6, which encourages the use of a WAF, provided that the WAF is configured appropriately in the customers' environment in a manner that their PCI DSS qualified security assessors agree is appropriate under the circumstances.

With this amendment to Akamai's Attestation of Compliance, the Page Integrity Manager solution is now included within Akamai's PCI DSS assessment.

Akamai's Prolexic DDoS mitigation solutions are not included in Akamai's PCI DSS assessment, but are designed to have no access to or impact on cardholder data and are therefore readily available to protect customers and their PCI DSS compliant Internet properties from attacks.

Note on Amazon Web Services

mPulse and Bot Manager Premier rely in part on infrastructure provided by Amazon Web Services (AWS). Cardholder data is never transmitted to or stored by systems in the AWS infrastructure, so those systems are not in scope for Akamai's PCI DSS assessment and have no impact on the PCI DSS compliance of our customers.

Non-Compliant Services

Other Akamai services, such as Standard TLS (as opposed to Enhanced TLS), the NetStorage network for storing large files, and Akamai Identity Cloud solutions, are not PCI DSS compliant. Customers should not use these services within their cardholder data environments.

Customer Responsibilities

While the products and services described above may be configured to be PCI DSS compliant, customers are required to configure the PCI DSS compliant portions of their web properties properly in accordance with Akamai's Responsibility Matrix, described below. Customers may also request a copy of our PCI DSS Customer Configuration Guide for suggestions about how to configure their properties in a PCI DSS compliant manner.

Additional Notes

- The cover page of the Attestation of Compliance is dated "June 2018." This is the effective date of the PCI DSS version 3.2.1 standard. The effective date of Akamai's Attestation of Compliance itself is June 26, 2020.
- In addition to the Attestation of Compliance, we have also published, at http://akamai.me/matrix, a Responsibility Matrix, which spells out the PCI DSS requirements in detail, and indicates whether Akamai or its customers are to be responsible for satisfying each requirement in order to be compliant. The Responsibility Matrix was reviewed by our PCI DSS assessors in this form, and Akamai is unable to make any modifications.
- Our customers' account and professional service teams can offer general guidance as to how our solutions may be configured for compliance, but the ultimate determination of whether a solution is compliant with PCI DSS will be made by our customers and their Qualified Security Assessors.

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information					
Part 1a. Service Provider Organization Information					
Company Name:	Akamai Technologies, Inc. and its direct and indirect subsidiaries		DBA (doing business as):	N/A	
Contact Name:	Fadi Saba		Title:	Sr. Director of Information Security	
Telephone:			E-mail:		
Business Address:	145 Broadway		City:	Cambridge	
State/Province:	MA	Country:	USA	ZIP	02142
URL:	https://www.akamai.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Specialized Security Services, Inc.				
Lead QSA Contact Name:	Thomas P. Sipes		Title:	SVP, Compliance and Security Services	
Telephone:	972-378-5554		E-mail:	tsipes@s3security.com	
Business Address:	4975 Preston Park Boulevard, Suite 510		City:	Plano	
State/Province:	Texas	Country:	USA	Zip:	75093
URL:	http://www.s3security.com				

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	Akamai Secure Content Delivery Network with Enhanced TLS and services running on this network, including: Web performance solutions: Ion with Enhanced TLS, China CDN for Ion, Dynamic Site Accelerator with Enhanced TLS, and China CDN for Dynamic Site Accelerator. Legacy web performance solutions when configured with Secure Delivery or with Enhanced TLS: Alta, Terra Alta, Rich Media Accelerator, Aqua Mobile, DSA Premier with Enhanced TLS, Dynamic Site Delivery, Web Application Accelerator, Ion Standard, Ion Media Advanced, Ion Premier, and additional Web Performance products associated with the above, when configured to run on the Secure CDN with Enhanced TLS Web Security solutions: Client Reputation, Kona Site Defender, Kona DDoS Defender, Web Application Firewall, Web Application Protector, and Page Integrity Manager (all when configured with "Secure Delivery" or with "Enhanced TLS"). JavaScript engines for the mPulse and Bot Manager Premier services. AMENDED – Specialized Security Services, Inc. assessed the Page Integrity Manager solution that is an additional client service within the Akamai Secure Content Delivery Network with Enhanced TLS. This amendment started on August 24, 2020 with the amended ROC being completed September 14, 2020. “The above services are collectively referred to as the “Assessed Services”.

Type of service(s) assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (specify):		

☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☒ Others (specify): Akamai Secure Content Delivery Network with Enhanced TLS (SCDN), services running on the SCDN, mPulse JavaScript engine, Bot Manager Premier JavaScript engine, and Page Integrity Manager		

***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

Part 2a. Scope Verification *(continued)*			
Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):			
Name of service(s) not assessed:	Content Delivery Network (Non-Secure), including Secure Content Delivery Network with Standard TLS, NetStorage, Prolexic DDoS mitigation services, Edge DNS, Enterprise Application Access (EAA) and other services that do not interact with cardholder data.		
Type of service(s) not assessed:			
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):	
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch	
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services	
☐ Billing Management	☐ Loyalty Programs	☐ Records Management	
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments	
☐ Network Provider			
☒ Others (specify): Content Delivery Network (Non-Secure)			
Provide a brief explanation why any checked services were not included in the assessment:	Akamai directs all clients who may transmit managed cardholder data to use the Akamai Secure Content Delivery Network with Enhanced TLS.		

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Akamai Technologies, Inc.'s customers are instructed that only products running on the Akamai Secure Content Delivery Network with Enhanced TLS, Page Integrity Manager, and the JavaScript engines of the Bot Manager Premier and mPulse services (used to collect data for processing outside the cardholder data environment) are in scope for this PCI assessment. No other systems are intended or should be used for the transmission, processing, or the storage of cardholder data. Additional Akamai services, such as Prolexic DDoS mitigation services and SureRoute IP content delivery service, have no access to customers' cardholder data and are therefore out of scope for this PCI assessment. These services are nevertheless acceptable to use in a customers' cardholder data environment. Akamai's EAA service has no access to customers' cardholder data if configured per the Customer Configuration Guide and are therefore out of scope for this PCI assessment. These services are nevertheless acceptable to use in a customers' cardholder data environment. The Akamai Secure Content Delivery Network with Enhanced TLS is Akamai's secure platform on which its web performance and web security services may be used on Internet properties that transmit sensitive data such as cardholder data. These services (such as Ion and Kona Site Defender) and related products, when running on the Akamai Secure Content Delivery Network with Enhanced TLS in accordance with the Responsibility Matrix required by PCI DSS requirement 12.8.5, may be used in customers' cardholder data environment in a manner consistent with the requirements of PCI DSS.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Not applicable

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
Example: Retail outlets	*3*	*Boston, MA, USA*
Corporate Office	1	Cambridge, MA, USA
Data Center	1	Billerica, MA, USA
Data Center	1	Chicago, IL, USA

Data Centers		Global

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Not applicable			☐ Yes ☐ No	

Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	Akamai does not store or process any cardholder data and only transmits data that is already encrypted using client supplied encryption methodologies. Within the Akamai Secure Content Delivery Network with Enhanced TLS, Akamai transports the original web-based information across the Akamai's EdgeSuite SSL ("ESSL") network using TLS. This data is then staged on an ESSL endpoint where it is presented to the requesting browser. The JavaScript engines can be used within both customer sites that are served over the Secure Content Delivery Network with Enhanced TLS and sites served directly from the customer origin. The Bot Manager Premier service provides detection and prevention against unauthorized bots while the mPulse solution monitors the customer origin and provides optimization. The Page Integrity Manager service provides detection and prevention of a web page being altered during the process of delivery to the requesting party by comparing expected values with current values.
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

Part 2f. Third-Party Service Providers		
Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?		☐ Yes ☒ No
If Yes:		
Name of QIR Company:	Not applicable	
QIR Individual Name:	Not applicable	
Description of services provided by QIR:	Not applicable	
Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?		☒ Yes ☐ No
If Yes:		
Name of service provider:	**Description of services provided:**	
Salesforce	Platform extension services	
Amazon Web Services	Platform extension services	
Microsoft Azure	Platform extension services	
Note: *Requirement 12.8 applies to all entities in this list.*		

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

Name of Service Assessed:	Secure Content Delivery Network with Enhanced TLS, JavaScript engines for Bot Manager Premier, mPulse, and Page Integrity Manager

PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☒	☐	1.1.3 – Akamai does not process cardholder data within the Assessed Services. 1.2.3 – Akamai does not permit the use of wireless technologies in any portion of the Assessed Services. 1.3.6 – Akamai does not store cardholder data in any portion of the Assessed Services.
Requirement 2:	☐	☒	☐	2.1.1.a – Akamai does not permit wireless services in any portion of the Assessed Services. 2.2.1 - Akamai does not permit the use of wireless technologies in any portion of the Assessed Services. 2.2.3 – Akamai does not utilize insecure protocols within the Assessed Services. 2.6 – Akamai is not a shared hosting provider.
Requirement 3:	☐	☐	☒	3.0 (all) – Akamai does not store or process cardholder data in any portion of the Assessed Services.
Requirement 4:	☐	☒	☐	4.1.1 - Akamai does not permit the use of wireless technologies in any portion of the Assessed Services. 4.2 – Akamai does not receive cardholder data from any customer's via end-user messaging.
Requirement 5:	☒	☐	☐	

Requirement 6:	☐	☒	☐	6.4.3 – Akamai Technologies, Inc. does not use cardholder data for testing or development in any portion of the Assessed Services.
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.1.5 – Akamai does not allow vendors access to the Assessed Services. 8.5.1 – Akamai does not remotely access any customer premises networks. 8.7 – Akamai does not store or process cardholder data in any portion of the Assessed Services.
Requirement 9:	☐	☒	☐	9.5 – Akamai does not store cardholder data on any form of media. 9.6 – Akamai does not externally distribute media in any manner. 9.7 – Akamai does not store cardholder data on any form of media. 9.8 - Akamai does not store cardholder data on media or hardcopy material. 9.9 – Akamai does not use or support the use of PED devices.
Requirement 10:	☐	☒	☐	10.2.1 - Akamai does not store nor have access to cardholder data on any form of media.
Requirement 11:	☐	☒	☐	11.1 - Akamai does not permit the use of wireless technologies in any portion of the Assessed Services.
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	Akamai is not a shared hosting provider.
Appendix A2:	☐	☐	☒	Akamai does not use any POS systems.

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	*May 21, 2020* *Amended September 14, 2020*	
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes	☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *May 21, 2020, Amended September 14, 2020.*

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (***check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Akamai Technologies, Inc.* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)	
☐	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Specialized Security Services, Inc. (3765-01-13)*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* 10/05/2020
Service Provider Executive Officer Name: Fadi Saba	*Title: Sr. Director of Information Security*

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	Specialized Security Services, Inc. performed the security assessment and prepared the Report on Compliance in accordance with the PCI DSS 3.2.1 Guidelines.

Signature of QSA's Executive Officer ↑	*Date:* 10/8/2020
QSA's Executive Officer Name: Mitchelle Schanbaum	*QSA Company:* Specialized Security Services, Inc.
Signature of QSA ↑	*Date:* 10.8.2020
QSA Name: Thomas P. Sipes	*QSA Company:* Specialized Security Services, Inc.

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	Not applicable

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.