Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Eigen Development, Ltd.

Date of Report as noted in the Report on Compliance: February 11, 2026

Date Assessment Ended: February 10, 2026

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures (*"Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information

Part 1a. Assessed Entity (ROC Section 1.1)

Company name:	*Eigen Development, Ltd.*
DBA (doing business as):	*Shift4*
Company mailing address:	*300 - 1807 West 10th Avenue, Vancouver, BC, V6J 2A9, Canada*
Company main website:	*https:// www.eigendev.com*
Company contact name:	*Oren Gur*
Company contact title:	*SVP, Enterprise Security & CISO*
Contact phone number:	*+972529245381*
Contact e-mail address:	*oren.gur@Shift4.com*

Part 1b. Assessor (ROC Section 1.1)

Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.

PCI SSC Internal Security Assessor(s)	
ISA name(s):	*N/A*
Qualified Security Assessor	
Company name:	*Kyte Consultants Ltd*
Company mailing address:	*170, Pater House, Psaila Street, Birkirkara BKR 9077, Malta*
Company website:	*https://kyte.global/*
Lead Assessor name:	*Anis Mesmouki*
Assessor phone number:	*+356 27595000*
Assessor e-mail address:	*anis@kyte.global*
Assessor certificate number:	*206-063*

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	*Merchant Servicer (MiraServ, MiraPay, & MiraBatch)*	
Type of service(s) assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web-hosting services ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Multi-Tenant Service Provider ☐ Other Hosting (specify):	**Managed Services:** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☒ POI / 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): N/A		

Note: *These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	*Not Applicable*

Type of service(s) not assessed:

Hosting Provider: □ Applications / software □ Hardware □ Infrastructure / Network □ Physical space (co-location) □ Storage □ Web-hosting services □ Security services □ 3-D Secure Hosting Provider □ Multi-Tenant Service Provider □ Other Hosting (specify):	**Managed Services:** □ Systems security services □ IT support □ Physical security □ Terminal Management System □ Other services (specify):	**Payment Processing:** □ POI / 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): *N/A*		

Provide a brief explanation why any checked services were not included in the Assessment:	*N/A*

Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	*The entity's primary business includes transaction processing for different merchant customers. The entity deals with card not present online card details.* *The entity receives CHD via its eCommerce, mail order/telephone order, or card-present payment channels and SFTP servers from its customers in multiple forms, such as direct payments, APIs, batch processes, etc.* *Client stores CHD for processing of the initial transaction and the convenience of their merchant*

	customers to facilitate account research, billing history, and charge-back/refund functions.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	*N/A*
Describe system components that could impact the security of account data.	*The entity is responsible for the CDE environment, which communicates between its clients and service providers and therefore can affect the security of the networks.* *The entity's CDE environment is comprised of an entirely on-prem environment that is made up of Ubuntu virtual machines running off of Dell Chassis, and HP switches. The Ubuntu virtual machines act as firewalls, web servers, application servers, databases, IDS/IPS, logs servers, etc.* *Potentially, any system component within the CDE could impact the security of CHD if compromised.*

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card 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 POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	***Payment Channels:*** • *Card-Present (POS, Card Swipe/Non POS-Direct)* • *Card-not-present (MOTO and eCommerce)* ***People Reviewed:*** • *System Administrators* • *Information Security Managers* • *Database Administrators* • *Developers* • *Client Services and Support Staff* • *Facilities Manager* ***Processes Reviewed:*** • *Card-present via MiraServ P2PE validated and* • *PA-DSS validated* • *Card-not-present MiraPay eCommerce hosted,* • *iFrame and API solution for merchants to customize their eCommerce* • *MOTO channel* • *Mira-Batch via encrypted files that are sent to the acquiring bank* ***Technologies reviewed:*** • *eCommerce systems* • *Web Services* • *API Connections* • *DMZ Segments* • *Network VLANs* • *IDS/IPS* • *Firewalls* • *Routers* • *Switches* • *Ubuntu Servers* • *Anti-Malware Solution* • *SIEM and FIM solutions* ***Locations reviewed:*** • *Corporate Offices – Vancouver, BC* • *Data Centers – Vancouver, BC and Calgary, AB*

Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☒ Yes ☐ No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	**Total Number of Locations** (How many locations of this type are in scope)	**Location(s) of Facility** (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Data center	*2*	*Vancouver, BC, Canada* *Calgary, AB, Canada*
Corporate Office	*1*	*Vancouver, BC, Canada*

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions*?

☒ Yes ☐ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
MiraServ	*6.31*	*PA-DSS v3.2* *P2PE v3.1*	*16-01.00282.003* *2023-00282.008*	*October 28, 2022* *March 10, 2026*

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers
*(***ROC Section 4.4***)*

For the services being validated, does the entity have relationships with one or more third-party service providers that:

- Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☐ Yes ☒ No
- Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☐ Yes ☒ No
- Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☐ Yes ☒ No

If Yes:

Name of Service Provider:	**Description of Services Provided:**
N/A	*N/A*

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either “Not Applicable” or “Not Tested,” complete the “Justification for Approach” table below.

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: Digital Payment Service

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	☒	☒	□	□	□
Requirement 2:	☒	☒	□	□	□
Requirement 3:	☒	☒	□	□	□
Requirement 4:	☒	☒	□	□	□
Requirement 5:	☒	☒	□	□	□
Requirement 6:	☒	☒	□	□	□
Requirement 7:	☒	□	□	□	□
Requirement 8:	☒	☒	□	□	□
Requirement 9:	☒	☒	□	□	□
Requirement 10:	☒	☒	□	□	□
Requirement 11:	☒	☒	□	□	□
Requirement 12:	☒	☒	□	□	□
Appendix A1:	□	☒	□	□	□
Appendix A2:	□	☒	□	□	□

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	*1.2.6.a - Insecure ports, protocols, services are not used* *1.2.6.b - Insecure ports, protocols, services are not used* *2.3.1.a - Wireless is not used to connected to the CDE or transmit CHD* *2.3.1.b - Wireless is not used to connected to the CDE or transmit CHD* *2.3.1.c - Wireless is not used to connected to the CDE or transmit CHD* *2.3.2 - Wireless is not used to connected to the CDE or transmit CHD* *3.3.3.a - Entity is not an issuer or supports issuing services* *3.3.3.b - Entity is not an issuer or supports issuing services* *3.4.2.c - PAN is prohibited from being relocated from the database* *3.5.1.c - Hashing or truncation not used* *3.5.1.1.a - Hashing or truncation not used* *3.5.1.1.b - Hashing or truncation not used* *3.5.1.1.c - Hashing or truncation not used* *3.5.1.1.d - Hashing or truncation not used* *3.5.1.2.a - Disk-level encryption not used* *3.5.1.2.b - Disk-level encryption not used* *For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.* *3.5.1.3.a - Disk-level encryption not used* *3.5.1.3.b - Disk-level encryption not used* *3.7.9 - Keys are not shared with customers* *4.2.1.2 - Wireless is not used to transmit CHD or connected to the CDE* *4.2.2.a - End-user messaging is not used to transmit CHD* *4.2.2.b - End-user messaging is not used to transmit CHD* *5.2.1.b - No systems are defined as not at-risk* *5.2.3.a - No systems are defined as not at-risk* *5.2.3.b - No systems are defined as not at-risk* *5.2.3.c - No systems are defined as not at-risk* *5.2.3.1.a - No systems are defined as not at-risk* *5.2.3.1.b - No systems are defined as not at-risk* *5.3.3.a - Removable media is not used* *5.3.3.b - Removable media is not used* *5.3.3.c - Removable media is not used* *6.4.1 - This requirement is superseded by Requirement 6.4.2 after 31 March 2025* *6.5.2 - Entity had no significant changes this assessment period* *8.2.2.a - Entity does not make use of shared, group or generic accounts.* *8.2.2.b - Entity does not make use of shared, group or generic accounts.* *8.2.2.c - Entity does not make use of shared, group or generic accounts.* *8.2.3 - Entity does not have remote access to customers environment* *8.2.7 - Third parties do not have access to system components* *8.3.10 - This requirement for service providers is superseded by Requirement 8.3.10.1* *8.5.1.c - MFA cannot be bypassed*

	8.6.2.a - System and application accounts do not have interactive login *8.6.2.b - System and application accounts do not have interactive login* *8.6.3.a - System and application accounts do not have interactive login* *8.6.3.b - System and application accounts do not have interactive login* *8.6.3.c - System and application accounts do not have interactive login* *9.4.1 - Entity does not have media with CHD* *9.4.1.1.a - Entity does not have media with CHD* *9.4.1.1.b - Entity does not have media with CHD* *9.4.1.2.a - Entity does not have media with CHD* *9.4.1.2.b - Entity does not have media with CHD* *9.4.2.a - Entity does not have media with CHD* *9.4.2.b - Entity does not have media with CHD* *9.4.3.a - Entity does not have media with CHD* *9.4.3.b - Entity does not have media with CHD* *9.4.3.c - Entity does not have media with CHD* *9.4.4.a - Entity does not have media with CHD* *9.4.4.b - Entity does not have media with CHD* *9.4.5.a - Entity does not have media with CHD* *9.4.5.b - Entity does not have media with CHD* *9.4.5.1.a - Entity does not have media with CHD* *9.4.5.1.b - Entity does not have media with CHD* *9.4.6.a - Entity does not have media with CHD* *9.4.6.b - Entity does not have media with CHD* *9.4.6.c - Entity does not have media with CHD* *9.4.7.a - Entity does not have media with CHD* *9.4.7.b - Entity does not have media with CHD* *9.5.1 - Entity does not manage POI devices* *9.5.1.1.a - Entity does not manage POI devices* *9.5.1.1.b - Entity does not manage POI devices* *9.5.1.1.c - Entity does not manage POI devices* *9.5.1.2.a - Entity does not manage POI devices* *9.5.1.2.b - Entity does not manage POI devices* *9.5.1.2.1.a - Entity does not manage POI devices* *9.5.1.2.1.b - Entity does not manage POI devices* *9.5.1.3.a - Entity does not manage POI devices* *9.5.1.3.b - Entity does not manage POI devices* *10.4.2.a - All systems and associated logs are reviewed as defined in Requirement 10.4.1* *10.4.2.b - All systems and associated logs are reviewed as defined in Requirement 10.4.1* *10.4.2.1.a - All systems and associated logs are reviewed as defined in Requirement 10.4.1* *10.4.2.1.b - All systems and associated logs are reviewed as defined in Requirement 10.4.1* *10.7.1.a - This requirement is superseded by requirement 10.7.2* *10.7.1.b - This requirement is superseded by requirement 10.7.2* *11.2.1.d - Automated monitoring is not used* *11.2.2 - Wireless is not used to connected to the CDE or transmit CHD* *11.3.1.2.c - Account used for authenticated scanning does not allow interactive login* *11.3.1.2.d - All systems have authenticated scans performed against them* *11.3.1.3.a - No significant changes this assessment period* *11.3.1.3.b - No significant changes this*

	assessment period 11.3.1.3.c - No significant changes this assessment period 11.3.2.1.a - No significant changes this assessment period 11.3.2.1.b - No significant changes this assessment period 11.3.2.1.c - No significant changes this assessment period 11.4.7 - Entity is not a multi-tenant service provider 11.6.1.c - Mechanism functions are performed in accordance with the defined frequency 12.3.2 - Customized approach not used 12.5.3.b - Not applicable - Client had no significant changes. 12.8.1.b - Per FAQ-1284, Client does not make use of any service providers that are not considered Acquirers. 12.8.2.b - Per FAQ-1284, Client does not make use of any service providers that are not considered Acquirers. 12.8.3.b - Per FAQ-1284, Client does not make use of any service providers that are not considered Acquirers. 12.8.4.b - Per FAQ-1284, Client does not make use of any service providers that are not considered Acquirers. 12.8.5.b - Per FAQ-1284, Client does not make use of any service providers that are not considered Acquirers. 12.10.1.b - Entity has had no security incidents within the past year 12.10.7.b - PAN was not identified to be stored outside the database. A1.1.1 - Entity is not a multi-tenant service provider A1.1.2.a - Entity is not a multi-tenant service provider A1.1.2.b - Entity is not a multi-tenant service provider A1.1.3 - Entity is not a multi-tenant service provider A1.1.4 - Entity is not a multi-tenant service provider A1.2.1 - Entity is not a multi-tenant service provider A1.2.2 - Entity is not a multi-tenant service provider A1.2.3 - Entity is not a multi-tenant service provider A2.1.1 - Entity does not manage POI devices A2.1.2 - Entity does not manage POI devices A2.1.3 - Entity does not manage POI devices
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	*Not Applicable.*

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	*October 27, 2025*
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	*February 11, 2026*
Were any requirements in the ROC unable to be met due to a legal constraint?	□ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes □ No

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated February 11.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

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

☒ **Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *Eigen Development, Ltd.* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.

☐ **Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements.

Target Date for Compliance: *YYYY-MM-DD*

An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.

☐ **Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.

This option requires additional review from the entity to which this AOC will be submitted.

If selected, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

26 February 2026 | 4:40 AM PST

Signature of Service Provider Executive Officer ↑	Date: *February 11, 2026*
Service Provider Executive Officer Name: *Oren Gur*	Title: *SVP, Enterprise Security & CISO*

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Anis Mesmouki 11 February 2026 | 7:26 AM PST

Signature of Lead QSA ↑	Date: *February 11, 2026*
Lead QSA Name: *Anis Mesmouki*	

26 February 2026 | 4:58 PM CET

Signature of Duly Authorized Officer of QSA Company ↑	Date: *February 11, 2026*
Duly Authorized Officer Name: *Trevor Axiak*	QSA Company: *Kyte Consultants Ltd*

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement	
If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement below. For any “No” responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	**Description of Requirement**	**Compliant to PCI DSS Requirements** (Select One)		**Remediation Date and Actions** (If “NO” selected for any Requirement)
		YES	**NO**	
1	Install and maintain network security controls	□	□	
2	Apply secure configurations to all system components	□	□	
3	Protect stored account data	□	□	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	□	□	
5	Protect all systems and networks from malicious software	□	□	
6	Develop and maintain secure systems and software	□	□	
7	Restrict access to system components and cardholder data by business need to know	□	□	
8	Identify users and authenticate access to system components	□	□	
9	Restrict physical access to cardholder data	□	□	
10	Log and monitor all access to system components and cardholder data	□	□	
11	Test security systems and networks regularly	□	□	
12	Support information security with organizational policies and programs	□	□	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	□	□	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	□	□	

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/