Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0

Revision 2

Publication Date: August 2023

PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Ezetap Mobile Solutions Private Limited

Assessment End Date: 24th November 2023

Date of Report as noted in the Report on Compliance: 24th November 2023

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:	Ezetap Mobile Solutions Private Limited
DBA (doing business as):	Razorpay POS
Company mailing address:	SJR Cyber Laskar, Hosur Road, Bengaluru, Karnataka, India 560030
Company main website:	https://razorpay.com/pos/
Company contact name:	Hilal Lone
Company contact title:	Senior Director, Information Security and Compliance
Contact phone number:	+91 7006717459
Contact e-mail address:	hilal.lone@razorpay.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):	Not Applicable
Qualified Security Assessor	
Company name:	Panacea InfoSec Pvt. Ltd.
Company mailing address:	3rd Floor Plot no. 226, Pocket A2, Sector 17, Delhi, India - 110075
Company website:	www.panaceainfosec.com
Lead Assessor name:	Raghvendra Shukla
Assessor phone number:	+91-8929627083
Assessor e-mail address:	raghvendra@panaceainfosec.com

Assessor certificate number:	206-005

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:	Acquiring POS Services

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☒ Applications / software	☐ Systems security services	☒ POI / 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-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service 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): Not Applicable		

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): Not Applicable		
Provide a brief explanation why any checked services were not included in the Assessment:	Not Applicable	

Part 2b. Description of Role with Payment Cards (ROC Section 2.1)

Describe how the business stores, processes, and/or transmits account data.	Ezetap Mobile Solutions Private Limited hereafter referred as “Ezetap” is POS application provider where entity provides the application to it’s merchants which is deployed on the POS machines for processing the transactions. Ezetap provides both software as a service (SaaS) and platform as a service (PaaS) to it’s merchants where entity only provides application to merchants in case of SaaS and software along with hardware in case of PaaS. Ezetap further facilitates multiple type of transactions which includes card present

	transactions, card not present transactions, wallet transactions, EMI and UPI **CHD Transmission and Processing:** Ezetap provides following line of services as part of payment processing which are as follows: • Android POS – This is an android application which is deployed on the various POS devices like PAX A910, A920, A50, etc. • Merchant Mobile Application – Ezetap enables merchants to accept the card through mPOS D180 device. D180 device connects with mobile phone through Bluetooth. Merchant downloads the mPOS and Service application on it's mobile phone where mPOS works as front-end application and Service application works as back-end. Service application is responsible for sending the entire transaction payload to Ezetap servers. • Merchant Kiosk – In this scenario, D200 device is connected to merchant kiosk machine and payment data is dealt in following manner: ○ Java SDK - Merchant Kiosk is wired to D200 device for accepting the payments. Kiosk will send the command to D200 device and end-merchant will dip the card and enter the PIN on the device in order to process the transaction. The transaction is directly forwarded to Ezetap servers in the back-end. ○ P2P SDK - Merchant Kiosk will be directly connected Ezetap servers for any kind of action. Ezetap servers will further command D200 devices basis on the command received from kiosk to accept the payment from end merchant. End-customer will dip the card and enter the PIN on the device in order to process the transaction. The transaction is directly forwarded to Ezetap servers in the back-end. • POG Devices – Merchants are given POG devices which are responsible for card reading. Merchant installs MPOS application, Service Application and MPP Application on their mobile phone. POG device connects with merchants mobile phone through Bluetooth. Applications installed on merchants mobile phone works as follows: ○ MPOS application – This application acts as the front end. ○ Service Application – This application is responsible for checking the status post transaction is processed. ○ MPP Application – MPP is a third-party application on which user enters the PIN. MPP takes full card from

	POG device and sends the entire payload to Ezetap servers. • CNP Flow – In this flow, merchants can send the payment links to the merchants through SMS where merchant will click on the link received in SMS following making the payment. Merchant enters card details PAN, Expiry date and CVV2 on the webpage. These details are sent over HTTPS TLS v1.3 to the payment processor for further processing of the transaction. • Entity also provides closed loop wallet services to the merchants. All the transactions are sent to Ezetap API servers from respective flows mentioned. POS devices facilitating card present transactions are injected with IPEK keys (or TMK). Device further generates DUKPT (Derived Unique Key Per Transaction), the entire payload is encrypted with DUKPT and sent to Ezetap API servers. These IPEK keys are also loaded on the HSM which will help in generating DUKPT in real time. DUKPT is then used to decrypt the payload and is further encrypted as per agreement with respective PGs on-boarded by the merchant. Based on the configuration on its API server, the transaction request is forwarded to payment processor for transaction processing. The transaction request is sent either over HTTPS TLS v1.3, IPSec or over MPLS network to payment processor based on agreed communication channel. **Card Storage:** Entity stores the full card number in encrypted format. The card is encrypted using AES 256 bit encryption algorithm in the internal database.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	All the transactions are sent to Ezetap API servers from respective flows mentioned. POS devices facilitating card present transactions are injected with IPEK keys (or TMK). Device further generates DUKPT (Derived Unique Key Per Transaction), the entire payload is encrypted with DUKPT and sent to Ezetap API servers. These IPEK keys are also loaded on the HSM which will help in generating DUKPT in real time. DUKPT is then used to decrypt the payload and is further encrypted as per agreement with respective PGs on-boarded by the merchant. Based on the configuration on its API server, the transaction request is forwarded to payment processor for transaction processing. The transaction request is sent either over HTTPS TLS v1.3, IPSec or over MPLS network to payment processor based on agreed communication channel.

	Ezetap stores the full card number in encrypted format. The card is encrypted using AES 256 bit encryption algorithm in the internal database.
Describe system components that could impact the security of account data.	The system componenets are as follows: Database: Ezetap stores the full card number in encrypted format. The card is encrypted using AES 256 bit encryption algorithm in the internal database.

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.*	The assessment focused on below mentioned environment and technologies: • Application Infrastructure • Database Infrastructure • Logging and Monitoring Solution • Remote authentication - Palo Alto VPN • Amazon Web Services (AWS) Cloud Infrastructure • Classical Infrastructure management - EC2 • Containerized Infrastructure management - EKS • AWS IAM (Identity and Access Management) Console • AWS Network Security Groups, Route Tables, NACL and VPC peering rules review • SIEM – Wazuh • Anti virus - SophosAV
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*
Cloud data center – Amazon Web Services (Reviewed via the AWS AOC)	1	Mumbai, Maharashtra, India
Head Office	1	SJR Cyber Laskar, Hosur Road, Bengaluru, Karnataka, India 560030"

Data center (STT Global) – STT Data center (reviewed by the STT AOC)	1	Mumbai, Maharashtra, India

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
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD

♦ 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, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

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:**
Amazon Web Services, Inc.	Cloud hosting services
STT Global Data Center	Data Center for HSM hosting

***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: Acquiring POS Services

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method(s) Was Used	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
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 - Not Applicable as there is no services, protocols and ports are in use which is considered to be insecure. 1.3.3 - Not Applicable as wireless network is not present in scoped environment. 2.2.5 - Not Applicable as ezetap doesn't utilize any insecure services across the scoped environment. 2.3.1, 2.3.2 - Not Applicable as wireless network is not present in scoped environment. 3.3.1 - Not Applicable as SAD is not retained after authorization 3.3.2 - Not Applicable as SAD is not getting stored post authorization. 3.3.3 – Not Applicable as Ezetap do not support the issuing services. 3.4.2 – Not Applicable as this requirement is best practice. 3.5.1.1 – Not Applicable as this requirement is best practice. 3.5.1.2 – Not Applicable as there is no removable media in scoped environment. 3.5.1.3 - Not Applicable as disk encryprion is not used in the Ezetap scoped environment. 3.7.9 - Not Applicable as Ezetap do not share any cryptographic keys with customer. 3.6.1.3, 3.7.6 Not Applicable as there is no cleartext key in the scoped environment 4.2.1.1 - Not Applicable as this requirement is best practice. 4.2.1.2 - Not Applicable as Ezetap doesn't utilize wireless networks for transmitting cardholder data across Ezetap scoped environment. 4.2.2 - Not Applicable as PAN is not shared via any end user message technology. 5.2.3 - Not Applicable as there are no systems present in the scoped environment which can not be commonly affected by malware. 5.2.3.1, 5.3.2.1 - Not Applicable as these requirementa are best practice. 5.3.3 - Not Applicable as there is no removable media allowed in Ezetap scoped environment. 5.4.1- Not Applicable as this requirement is best practice. 6.3.2, 6.4.1, 6.4.2, 6.4.3- Not Applicable as these requirements are best practice. 6.5.2 - Not Applicable as there is no significant change. 7.2.4, 7.2.5, 7.2.5.1 Not Applicable as these requirements are best practice. 8.2.3 - Not Applicable as Ezetap is not accessing their customer premises. 8.2.7 - Not Applicable as there are no third parties having access to scoped environment.

	8.3.10, 8.3.10.1, 8.4.2, 8.5.1, 8.6.1 8.6.2, 8.6.3 - Not Applicable as these requirements are best practice. 9.2.3 - Not Applicable as Ezetap does not take physical media backup of cardholder data. 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3 , 9.4.4 , 9.4.5, 9.4.5.1 - Not Applicable as there are no media in the scoped environment. 9.4.6 Not Applicable as there is no hard copy material storing Card data in scoped environment. 9.4.7 Not Applicable as there is no electronic media in the scoped environment. 9.5.1.2.1 Not Applicable as this requirement is best practice. 10.4.1.1, 10.4.2.1, 10.7.1, 10.7.2 – Not Applicable as this requirement is best practice. 11.2.2 Not Applicable as there is no wireless network in the scoped environment 11.3.1.1, 11.3.1.2, 11.4.7, 11.5.1.1, 11.6.1 - Not Applicable as this requirement is best practice. 12.3.1, 12.3.4, 12.5.2.1, 12.5.3, 12.6.2, 12.6.3.1, 12.6.3.2, 12.10.4.1 , 12.10.7 - Not Applicable as these requirement are best practice. 12.3.2, 12.3.3 Not Applicable as customized approach is not used for any of the requirements. Entire Appendix A1 - Not Applicable as assessed Ezetap is not a shared hosting service provider. Entire Appendix A2 - Not Applicable as the scoped Ezetap environment does not involve transaction and/or maintenance of POI/POS terminals.
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 1.3.2**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*			2023-08-11
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*			2023-11-24
Were any requirements in the ROC unable to be met due to a legal constraint?			☐ Yes ☒ No
Were any testing activities performed remotely? If yes, for each testing activity below, indicate whether remote assessment activities were performed:			☒ Yes ☐ No
• Examine documentation	☒ Yes	☐ No	
• Interview personnel	☒ Yes	☐ No	
• Examine/observe live data	☒ Yes	☐ No	
• Observe process being performed	☒ Yes	☐ No	
• Observe physical environment	☒ Yes	☐ No	
• Interactive testing	☒ Yes	☐ No	
• Other: Not Applicable	☐ 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 *(Date of Report as noted in the ROC 24th November 2023)*.

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 *(*Ezetap Mobile Solutions Pvt. 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 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

Hilal Lone
Authenticated through Leegality.com (MBowouJ)
Hilal Lone
Date: Wed Dec 13 11:34:59 IST 2023

Signature of Service Provider Executive Officer ↗	Date: 24th November 2023
Service Provider Executive Officer Name: Hilal Lone	Title: Senior Director, Information Security and Compliance

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:

Raghvendra Shukla

Signature of Lead QSA ↗	Date: 24th November 2023
Lead QSA Name: Raghvendra Shukla	

Himanshu

Signature of Duly Authorized Officer of QSA Company ↗	Date: 24th November 2023
Duly Authorized Officer Name: Himanshu Mishra	QSA Company: Panacea InfoSec Pvt. 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	☒	☐