Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

Revision 2

September 2022

Document Changes

Date	Version	Description
September 2022	3.2.1 Revision 2	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.

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:	Adumo Online (Pty) Ltd		DBA (doing business as):	Adumo Online	
Contact Name:	Willem De Swart		Title:	System Administrator Lead	
Telephone:	+27 21 555 3260		E-mail:	willem.deswardt@adumoonline.com	
Business Address:	Unit 207, 2nd Floor, Block Two Northgate Park, Section Road Brooklyn		City:	Cape Town	
State/Province:	Western Cape	Country:	South Africa	Zip:	7405
URL:					

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	SecuriCentrix				
Lead QSA Contact Name:	Adrian Dirksen		Title:	Information Security Consultant	
Telephone:	+2772 590 9377		E-mail:	Adrian.dirksen@securicentrix.com	
Business Address:	Dock Junction, Cnr Dock and Stanley Rd, V&A Waterfront		City:	Cape Town	
State/Province:	Western Cape	Country:	South Africa	Zip:	8001
URL:	https://www.securicentrix.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:	MyGate and Mercury Payment Gateway	
Type of service(s) 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):		

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

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Adumo Online processes use the in-house developed application for the card not present or eCommerce transactions over the internet, secured over a TLS v1.2 channel from the merchant to the cardholder data environment for processing and transmitted to the acquiring banks via an IPSEC VPN tunnel (SHA256 & SHA512 hashing and AES 256-bit encryption) for upstream authorisation. Cardholder data, including CV2, PAN, Expiry Date, and Cardholder Name is received and transmitted over a secure TLS v1.2 channel. Received cardholder data is encrypted using AES 256-bit encryption, PAN is truncated using application code techniques with only the first six (6) and last four (4) digits visible, PAN is also hashed using a SHA256 and SHA512 hashing algorithms. Cardholder data is stored hashed and encrypted in the SQL and PostgreSQL Database to allow existing customers recurring payments, for fraud checks and reconnaissance reporting. CV2 retrieved in the PHP as a stateless service, once the object is completed it is run through a shutdown process and is null and void and can't be retrieved again. This confirms that CV2 is not stored in memory.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	As a Payment Service Provider, Adumo Online capture, store and transmit cardholder data functioning as a gateway to their customer to process non-card present or eCommerce transactions to the acquiring banks for upstream authorisation. Encrypted and hashed cardholder data such as PAN is stored securely to allow customers to make recurring payments, for fraud checks and reconnaissance reporting. The eCommerce payments are securely transmitted to BankServ and Cardinal Commerce for fraud checks.

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	Cape Town, WP, SA
AWS Cloud	2	Cape Town, af-south-1a and af-south-1b regions

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	Not Applicable	Not Applicable	☐ Yes ☐ No	Not Applicable

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.*	The Adumo Online (Pty) Ltd cardholder data environment is hosted in the PCI DSS certified AWS cloud Cape Town, af-south-1a and af-south-1b regions. The cloud data centres host the physical devices and are responsible for the physical security. AWS Security Groups and FortiGate Firewalls are in the CDE to provide segmentation of the CDE from external networks, wireless networks, and the Corporate Office. The Corporate Office is physically segregated via co-location and logically segregated from the CDE via dedicated AWS Security Groups. MS SQL and PostgreSQL databases are in the cardholder data environment and store the truncated PAN, where the first six (6) and last four (4) digits of the PAN are visible, AES-256-bit encrypted PAN, or SHA256 or SHA512 hashed PAN. The CDE Ubuntu Linux and Windows Server systems are hosted as EC2 instances, that provides the platform to receive and transmit cardholder data securely. Cardholder data is securely received from merchant online stores and transmitted securely to the Acquiring Banks for upstream authorisation. The in-house PHP and Java developed MyGate and Mercury web applications provide API and hosted web page integration to merchants and the backend Platform and Product applications are used to switch merchant received ecommerce payment transactions to the Acquiring Bank securely. Cardholder data is secured during transmission over a secure TLS v1.2 channel. AES 256-bit encryption is used to encrypt received cardholder data using Hashicorp Vault, an Encryption as a Service solution. AWS Elastic Load Balancers are implemented in front of the Web Application directing traffic over HTTPS to intended internal subnets in the VPC, additionally traffic passes through AWS WAF & Shield for network intrusion detection and prevention.

	CloudWatch and AlienVault perform logging and monitoring of all systems in the environment and for intrusion detection of network and operating systems. Trend Micro is deployed on all servers in the CDE performing host intrusion detection and file integrity monitoring.
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:**
AWS	AWS is a PCI compliant cloud hosting service provider. AWS hosts the Adumo Online (Pty) Ltd cardholder data environment in the Cape Town, af-south-1a and af-south-1b regions.
Sequel Support	Sequel Support is a database support provider that provides Adumo Online (Pty) Ltd support of their MS SQL and PostgreSQL databases.
Silicon Overdrive	Silicon Overdrive is contracted and assisted with the migration and setup of the cardholder data environment systems in AWS, additionally provides continuous support for Adumo Online (Pty) Ltd systems.
Ideal Solutions	Ideal Solutions is a development company and provides services to assist with the build of the new Mercury platform internal to Adumo Online (Pty) Ltd.

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:	MyGate and Mercury Payment Gateway

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:	☐	☒	☐	**Requirement 1.2.2 –** Not Applicable, Adumo Online does not use routers in their CDE.
Requirement 2:	☐	☒	☐	**Requirement 2.1.1.x –** Not Applicable, Adumo Online Ltd does not use wireless networks in their CDE. **Requirement 2.6 –** Not Applicable, Adumo Online Ltd is not a Shared Hosting Provider.
Requirement 3:	☐	☒	☐	**Requirement 3.2.a, b –** Not Applicable, Adumo Online is not an issuer and does not support issuing services. **Requirement 3.4.c –** Not Applicable, Adumo Online does not backup or store data to removable media. **Requirement 3.4.1 –** Not Applicable, Adumo Online does not use disk encryption in the CDE. **Requirement 3.6.a –** Not Applicable, Adumo Online does not share cryptographic keys with customers. **Requirement 3.6.2.a, b –** Not Applicable, Adumo Online does not require that cryptographic keys be distributed. **Requirement 3.6.6 a, b –** Not Applicable, Adumo Online (Pty) Ltd does not perform clear-text cryptographic key management operations.
Requirement 4:	☐	☒	☐	**Requirement 4.1.1 –** Not Applicable, Adumo Online does not use wireless technologies in their CDE.

				Requirement 4.2.a – Not Applicable, Adumo Online does not share unprotected PAN by any means end user messaging technology.
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	**Requirement 6.4.6 -** Not Applicable, Adumo Online have not experienced any significant changes in the last 12 months.
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**Requirement 8.1.3.b –** Not Applicable, Adumo Online does not use physical authentication methods to access the CDE. **Requirement 8.5.1 –** Not Applicable, Adumo Online does not have access to customer environments.
Requirement 9:	☐	☒	☐	**Requirement 9.7.x –** Not Applicable, Adumo Online does not perform backups to removeable media. **Requirement 9.8.x –** Not Applicable, Adumo Online does not perform backups to removeable media or does not print any forms of cardholder. **Requirement 9.9.x –** Not Applicable, Adumo Online does not manage, support, or provide Point-of-Sale or Point-of-Interaction terminal devices.
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	**Requirement 11.2.3.a -** Not Applicable, Adumo Online have not experienced any significant changes in the last 12 months. **Requirement 11.2.3.b –** Not Applicable, Adumo Online did not require a rescan for internal and external vulnerabilities to be performed. **Requirement 11.2.3.c -** Not Applicable, Adumo Online use external resources to perform penetration test. **Requirement 11.3.1.b -** Not Applicable, Adumo Online use external resources to perform penetration test. **Requirement 11.3.2.b -** Not Applicable, Adumo Online use external resources to perform penetration test
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	
Appendix A2:	☐	☐	☒	

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:	19 January 2023	
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 19 January 2023

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 **Adumo Online (Pty) Ltd** 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

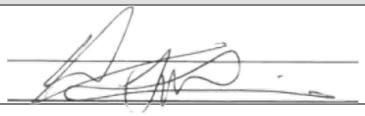
Signatory(s) confirms:

(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 *Qualys*

Part 3b. Service Provider Attestation



Signature of Service Provider Executive Officer ↗	*Date:* **19 January 2023**
Service Provider Executive Officer Name: **Willem De Swardt**	*Title:* **System Administrator Lead**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	The QSA assessment included the review of all PCI relevant policies, processes, procedures, and standards. The QSA interviewed relevant staff, observed processes, system settings and configuration files to ensure that PCI controls and requirements are achieved.

Signature of Duly Authorized Officer of QSA Company ↗	*Date:* **19 January 2023**
Duly Authorized Officer Name: **Adrian Dirksen**	*QSA Company:* **SecuriCentrix**

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

If an ISA(s) If no ISA in the assessment, then simply include Not Applicable here. 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.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

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 a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐