Security
Standards Council

Payment Card Industry (PCI)
PIN Security Requirements

Attestation of Compliance for Onsite Assessments

For use with PIN Security Requirements v3.1

Revision 1.0b

March 2021

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the assessment of the subject entity compliance with the *Payment Card Industry PIN Security Requirements and Test Procedures* (PCI PIN). Complete all sections: The entity is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity requesting the assessment (e.g. Payment Brand) for reporting and submission procedures.

Part 1. Entity and Qualified PIN Assessor (QPA) Information

Part 1a. Entity Organization Information

Company Name:	Compañía Peruana De Medios De Pago S.A.C.				
DBA (doing business as):	Niubiz		Business Identifier:	N/A	
Contact Name:	Alfredo Alva		Title:	Head of Information Security	
Telephone:	+51 985 908 943		E-mail:	aalva@niubiz.com.pe	
Business Address:	Av. José Pardo 831 piso 10		City:	Miraflores	
State/Province:	Distrito de Lima	Country:	Peru	Postal Code:	15074
URL:	https://www.niubiz.com.pe				

Part 1b. Qualified PIN Assessor Company Information (if applicable)

Company Name:	Foregenix Ltd				
Lead QPA Contact Name:	Guilherme Scheibe		Title:	Managing Consultant	
Telephone:	+44 845 309 6232		E-mail:	qa@foregenix.com	
Business Address:	8-9 High Street, 1st Floor		City:	Marlborough	
State/Province:	Wiltshire	Country:	United Kingdom	Postal Code:	SN8 1AA
URL:	https://www.foregenix.com				

Part 2. Executive Summary

Part 2a. Scope Verification

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

Type of service(s) assessed:

☒ PIN Acquirer Payment Processing - POS

☐ PIN Acquirer Payment Processing - ATM

☐ Remote Key Distribution Using Asymmetric Keys – Operations

☐ Certification and Registration Authority Operations

☐ Key-injection Facilities

☐ 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 entity but were NOT INCLUDED in the scope of the PCI PIN Assessment (check all that apply):

Type of service(s) not assessed:

□ PIN Acquirer Payment Processing - POS

□ PIN Acquirer Payment Processing - ATM

□ Remote Key Distribution Using Asymmetric Keys - Operations

□ Certification and Registration Authority Operations

□ Key-injection Facilities

□ Other (specify):

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

Part 2b. Locations

List types of facilities (for example, data centers, key-injection facilities, certification authority operations, etc.) and a summary of locations included in the PCI PIN review.

Type of facility assessed:	Date of Assessment	Location(s) of facility (city, country):
Example: Data Center	*18-20 June, 2019*	*Boston, MA, USA*
Niubiz Main office	7 Jun 2022 15 Jun 2022	Lima, Peru
Telefónica del Perú - Data Centre (Monterrico)	08 Jun 2022	Lima, Peru
Telefónica de Perú - Data Centre (Lince)	17 Jun 2022	Lima, Peru
Siscard - Key Injection Facility and POI Repair	14 Jun 2022	Lima, Peru
Necomplus - Key Injection Facility	14 Jun 2022 15 Jun 2022	Lima, Peru
Hervas - Storage and Distribution of POIs to the KIFs.	11 Oct 2021	Callao, Peru

Part 2c. Summary of Requirements Tested

For each PCI PIN 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*.

Part 2c. Summary of Requirements Tested *(continued)*

PCI PIN Control Objective	Details of Control Objectives Assessed			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Control Objective 1:	☐	☒	☐	3-2. Not Applicable. No non-PCI-approved devices are used.
Control Objective 2:	☐	☒	☐	6-3.x Not Applicable. No printers are used. 6-4. Not Applicable. Key component residues do not exist. 6-5. Not Applicable. Asymmetric keys are not used.
Control Objective 3:	☐	☒	☐	8-4. Not Applicable. Asymmetric keys are not used. 9-6. Not Applicable. Components of multiple keys cannot be conveyed in a single envelope.
Control Objective 4:	☐	☒	☐	12-3. Not Applicable. Key Loading Devices are not operated by Niubiz. KLDs for key injection into POIs at the KIFs were addressed in Annex B. 12-8. Not Applicable. Asymmetric keys are not used. 13-2. Not Applicable. Key loading is only performed in a secure facility. 13-4.3; 13-4.4. Not Applicable. Key Loading Devices are not operated by Niubiz. KLDs for key injection into POIs at the KIFs were addressed in Annex B. 15-2. Not Applicable. Asymmetric keys are not used.
Control Objective 5:	☐	☒	☐	19-2; 19-3. Not Applicable. Asymmetric keys are not used. 19-5. Not Applicable. Production devices are not used for testing. 20-2. Not Applicable. POI devices do not interface with multiple acquirers.
Control Objective 6:	☐	☒	☐	23-1. Not Applicable. Niubiz does not use key variants or any keys with reversible transformation methods 23-2. Not Applicable. MFK variants are not used.

Part 2c. Summary of Requirements Tested *(continued)*				
PCI PIN Control Objective	Details of Control Objectives Assessed			
	Full	Partial	None	Justification for Approach (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
				23-3. Not Applicable. Niubiz does not use key variants or any keys with reversible transformation methods 27-1; 27-2. Not Applicable. Niubiz does not maintain additional backups of keys.
Control Objective 7:	☒	☐	☐	
Annex A1 – Control Objective 3:	☐	☐	☒	Not Applicable. No CAs or Remote key distribution operations exist.
Annex A1 – Control Objective 4:	☐	☐	☒	Not Applicable. No CAs or Remote key distribution operations exist.
Annex A1 – Control Objective 5:	☐	☐	☒	Not Applicable. No CAs or Remote key distribution operations exist.
Annex A1 – Control Objective 6:	☐	☐	☒	Not Applicable. No CAs or Remote key distribution operations exist.
Annex A2 – Control Objective 3	☐	☐	☒	Not Applicable. No CAs or Remote key distribution operations exist.
Annex A2 – Control Objective 4:	☐	☐	☒	Not Applicable. No CAs or Remote key distribution operations exist.
Annex A2 – Control Objective 5:	☐	☐	☒	Not Applicable. No CAs or Remote key distribution operations exist.
Annex A2 – Control Objective 6:	☐	☐	☒	Not Applicable. No CAs or Remote key distribution operations exist.
Annex A2 – Control Objective 7:	☐	☐	☒	Not Applicable. No CAs or Remote key distribution operations exist.
Annex B – Control Objective 1:	☒	☐	☐	
Annex B – Control Objective 2:	☐	☐	☒	Not Applicable. The KIFs do not generate keys. All key generation procedures and handling of key components are performed by Niubiz and were addressed on the main body of the report.
Annex B – Control Objective 3:	☐	☐	☒	Not Applicable. The KIFs do not convey keys in any format. Niubiz keys are loaded into the KLDs and delivery to the KIFs by Niubiz directly. Procedures performed by Niubiz for key conveyance were addressed in the main body of the report.

Part 2c. Summary of Requirements Tested *(continued)*

PCI PIN Control Objective	Details of Control Objectives Assessed			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Annex B – Control Objective 4:	☐	☒	☐	12-1/2/4/5/6/8 13-2/3/5/6/7/8/9 14-4; 15-1/2. Not Applicable. Key loading operations by the KIFs is restricted to POI injection using KLDs, locally in a secure room. No keys are loaded into any other SCDs in any format. No key components or medias with key materials are handled by the KIFs. Procedures performed by Niubiz for key loading were addressed on the main body of the report.
Annex B – Control Objective 5:	☐	☒	☐	18-2/3/8; 19-X; 20-2/6. Not Applicable. The KIFs do not perform key management operations, including handling of key components in any format. BDKs are stored only inside the KLD and never leave the device. POI devices injected only interface with Niubiz. Key injection is performed locally in a secure room. Procedures performed by Niubiz for key management were addressed in the main body of the report.
Annex B – Control Objective 6:	☐	☒	☐	21-X to 28-X (except 22-1.5 and 22-2). Not Applicable. Siscard and Necomplus KIFs do not perform key management operations, including handling of key components in any format.
Annex B – Control Objective 7:	☐	☒	☐	29-4; 29-5 – Not Applicable. Siscard and Necomplus do not use HSMs for the KIF operations. 31-1.X – Not Applicable. Siscard and Necomplus do not use HSMs for the KIF operations. 32-1.3/4 – Not Applicable. Siscard and Necomplus KIFs do not perform key management operations, including handling of key components. 32-8.X – Not Applicable. No remote key distribution exists. Injection is only locally using KLDs.

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:	*02 Sep 2022*	
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 PIN Validation

This AOC is based on results noted in the ROC dated *02 Sep 2022.*

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3c, 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 PIN ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby has demonstrated full compliance with the PCI PIN Security Requirements.

□ **Non-Compliant:** Not all sections of the PCI PIN ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby has not demonstrated full compliance with the PCI PIN Security Requirements.

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 the applicable payment brand(s).

If checked, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement being met
Not Applicable	Not Applicable

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒ The ROC was completed according to the *PCI PIN Security Requirements and Testing Procedures*, Version *3.1*, 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 read the PCI PIN and I recognize that I must maintain PCI PIN 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 PIN requirements that apply.

Part 3b. Assessed Entity PIN Security Attestation

Signature of Executive Officer of Assessed Entity ↑ Signer ID: ERDXI0KOF8...

Assessed Entity Executive Officer Name: *Alfredo Alva*

Title:	*Head of Information Security*
Date:	02 Aug 2022

Part 3c. Qualified PIN Assessor (QPA) Company Acknowledgement	
Describe the role performed by the QPA and others that participated from within the QPA Company:	*Review of all PCI PIN applicable requirements; evaluation of documents, interviews, samples, and observation per the testing procedures; report writing.*

Signature of Duly Authorized Officer of QPA Company ↑	*Date: 02 Sep 2022*
Duly Authorized Officer Name: Leonardo Lima Ferla	*QPA Company:* Foregenix Ltd

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI PIN” 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 PIN Control Objective	Description of Control Objective	Compliant to PCI PIN Control Objective *(Select One)*		Remediation Date and Actions (If “NO” selected for any Control Objective
		YES	NO	
Control Objective 1:	PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.	☒	□	
Control Objective 2:	Cryptographic keys used for PIN encryption/decryption and related key management are created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.	☒	□	
Control Objective 3:	Keys are conveyed or transmitted in a secure manner.	☒	□	
Control Objective 4:	Key-loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.	☒	□	
Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	☒	□	
Control Objective 6:	Keys are administered in a secure manner.	☒	□	
Control Objective 7:	Equipment used to process PINs and keys is managed in a secure manner.	☒	□	
Annex A1 – Control Objective 3:	Keys are conveyed or transmitted in a secure manner.	□	□	Not Applicable
Annex A1 – Control Objective 4:	Key-loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.	□	□	Not Applicable
Annex A1 – Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	□	□	Not Applicable
Annex A1 – Control Objective 6:	Keys are administered in a secure manner.	□	□	Not Applicable
Annex A2 – Control Objective 3	Keys are conveyed or transmitted in a secure manner.	□	□	Not Applicable

PCI PIN Control Objective	Description of Control Objective	Compliant to PCI PIN Control Objective *(Select One)*		Remediation Date and Actions (If “NO” selected for any Control Objective
		YES	NO	
Annex A2 – Control Objective 4:	Key-loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.	□	□	Not Applicable
Annex A2 – Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	□	□	Not Applicable
Annex A2 – Control Objective 6:	Keys are administered in a secure manner.	□	□	Not Applicable
Annex A2 – Control Objective 7:	Equipment used to process PINs and keys is managed in a secure manner.	□	□	Not Applicable
Annex B – Control Objective 1:	PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.	☒	□	
Annex B – Control Objective 2:	Cryptographic keys used for PIN encryption/decryption and related key management are created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.	☒	□	
Annex B – Control Objective 3:	Keys are conveyed or transmitted in a secure manner.	☒	□	
Annex B – Control Objective 4	Key-loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.	☒	□	
Annex B – Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	☒	□	
Annex B – Control Objective 6:	Keys are administered in a secure manner.	☒	□	
Annex B – Control Objective 7:	Equipment used to process PINs and keys is managed in a secure manner.	☒	□	