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:	NETS Estonia A/S		
DBA (doing business as):	NETS Estonia	Business Identifier:	2858201-4
Contact Name:	Zafer Balkan	Title:	IT Security and Compliance Specialist
Telephone:	+372 5191 0910	E-mail:	zafer.balkan@nexigroup.com
Business Address:	Tartu maantee 63	City:	Tallinn
State/Province:	Harju County	Country:	Estonia	Postal Code:	10115
URL:	https://www.nets.eu/		

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

Company Name:	Foregenix Limited		
Lead QPA Contact Name:	Paolo Basilio	Title:	Global Head of Practice
Telephone:	+44 845 309 6232	E-mail:	pbasilio@foregenix.com
Business Address:	8-9 High Street	City:	Marlborough
State/Province:	Wiltshire	Country:	United Kingdom	Postal Code:	SN8 1AA
URL:	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:	N/A

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*
Head office and cryptographic key management	2 June 2021	Tallinn, Estonia
Data centre	3 June 2021	Harju maakond, Estonia
Data centre	3 June 2021	Tallinn, Estonia

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

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.)

PCI PIN Control Objective	**Full**	**Partial**	**None**	**Justification for Approach**
Control Objective 1:	☐	☒	☐	**1-1 Not Applicable. Nets does not directly manage or handle POI devices.** **2-4 Not Applicable. Nets does not directly manage or handle POI devices** **3-2 Not Applicable. Nets only acquires PIN-based transactions through PTS approved POI devices.**
Control Objective 2:	☐	☒	☐	**6-3, 6-5 Not Applicable. Nets does not handle asymmetric keys.**
Control Objective 3:	☐	☒	☐	**8-4 Not Applicable. Nets does not handle asymmetric keys.** **9-6 Not Applicable. Nets never sends components of multiple keys simultaneously.**
Control Objective 4:	☒	☐	☐	
Control Objective 5:	☐	☒	☐	**19-5 Not Applicable. There is no business rationale to justify the use of a production HSM for testing purposes.** **20-2 Not Applicable. All POI devices interface with Nets only.**
Control Objective 6:	☐	☒	☐	**27-1 to 27-2 Not Applicable. Nets currently does not make backups of keys.**
Control Objective 7:	☐	☒	☐	**29-1 Not Applicable. Nets does not directly manage POI devices and KLDs in the key loading process as this is performed by third party Key Injection Facilities (KIF).** **30-1 to 30-2 Not Applicable. Nets does not manage or handle POI devices.**
Annex A1 – Control Objective 3:	☐	☐	☒	**Not Applicable. Nets does not perform remote key injection using asymmetric techniques.**
Annex A1 – Control Objective 4:	☐	☐	☒	**Not Applicable. Nets does not perform remote key injection using asymmetric techniques.**
Annex A1 – Control Objective 5:	☐	☐	☒	**Not Applicable. Nets does not perform remote key injection using asymmetric techniques.**

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 A1 – Control Objective 6:	☐	☐	☒	**Not Applicable. Nets does not perform remote key injection using asymmetric techniques.**
Annex A2 – Control Objective 3	☐	☐	☒	**Not Applicable. Nets does not operate a CA/RA.**
Annex A2 – Control Objective 4:	☐	☐	☒	**Not Applicable. Nets does not operate a CA/RA.**
Annex A2 – Control Objective 5:	☐	☐	☒	**Not Applicable. Nets does not operate a CA/RA.**
Annex A2 – Control Objective 6:	☐	☐	☒	**Not Applicable. Nets does not operate a CA/RA.**
Annex A2 – Control Objective 7:	☐	☐	☒	**Not Applicable. Nets does not operate a CA/RA.**
Annex B – Control Objective 1:	☐	☐	☒	**Not Applicable. Nets does not operate a KIF.**
Annex B – Control Objective 2:	☐	☐	☒	**Not Applicable. Nets does not operate a KIF.**
Annex B – Control Objective 3:	☐	☐	☒	**Not Applicable. Nets does not operate a KIF.**
Annex B – Control Objective 4:	☐	☐	☒	**Not Applicable. Nets does not operate a KIF.**
Annex B – Control Objective 5:	☐	☐	☒	**Not Applicable. Nets does not operate a KIF.**
Annex B – Control Objective 6:	☐	☐	☒	**Not Applicable. Nets does not operate a KIF.**
Annex B – Control Objective 7:	☐	☐	☒	**Not Applicable. Nets does not operate a KIF.**

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:	*23 May 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 *23 May 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: **N/A** 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
N/A	N/A

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 *3.0*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of 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 ↑

Assessed Entity Executive Officer Name:	Zafer Balkan
Title:	Security and Compliance Manager
Date:	30.05.2022

Part 3c. Qualified PIN Assessor (QPA) Company Acknowledgement

Describe the role performed by the QPA and others that participated from within the QPA Company:	*The Qualified PIN Assessor (QPA) interviewed all staff members and tested all security requirements applicable to Nets, in the process collecting evidence and artefacts to support and substantiate compliance with the standard.*

Signature of Duly Authorized Officer of QPA Company ↑	*Date:* 25 May 2022
Duly Authorized Officer Name: Paolo Basilio	*QPA Company:* Foregenix Limited

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. Nets does not operate a CA/RA.
Annex A1 – Control Objective 4:	Key-loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.	☐	☒	Not Applicable. Nets does not operate a CA/RA.
Annex A1 – Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	☐	☒	Not Applicable. Nets does not operate a CA/RA.
Annex A1 – Control Objective 6:	Keys are administered in a secure manner.	☐	☒	Not Applicable. Nets does not operate a CA/RA.
Annex A2 – Control Objective 3	Keys are conveyed or transmitted in a secure manner.	☐	☒	Not Applicable. Nets does not operate a CA/RA.

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. Nets does not operate a CA/RA.
Annex A2 – Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	☐	☒	Not Applicable. Nets does not operate a CA/RA.
Annex A2 – Control Objective 6:	Keys are administered in a secure manner.	☐	☒	Not Applicable. Nets does not operate a CA/RA.
Annex A2 – Control Objective 7:	Equipment used to process PINs and keys is managed in a secure manner.	☐	☒	Not Applicable. Nets does not operate a CA/RA.
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.	☐	☒	Not Applicable. Nets does not perform direct key injection.
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.	☐	☒	Not Applicable. Nets does not perform direct key injection.
Annex B – Control Objective 3:	Keys are conveyed or transmitted in a secure manner.	☐	☒	Not Applicable. Nets does not perform direct key injection.
Annex B – Control Objective 4	Key-loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.	☐	☒	Not Applicable. Nets does not perform direct key injection.
Annex B – Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	☐	☒	Not Applicable. Nets does not perform direct key injection.
Annex B – Control Objective 6:	Keys are administered in a secure manner.	☐	☒	Not Applicable. Nets does not perform direct key injection.
Annex B – Control Objective 7:	Equipment used to process PINs and keys is managed in a secure manner.	☐	☒	Not Applicable. Nets does not perform direct key injection.