Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

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:	Nets Estonia AS		DBA (doing business as):	Nets Estonia AS	
Contact Name:	Zafer Balkan		Title:	Security and Compliance Manager	
Telephone:	+372 5191 0910		E-mail:	zafer.balkan@nexigroup.com	
Business Address:	Tartu mnt 63		City:	Tallinn	
State/Province:	Harju county	Country:	Estonia	Zip:	10115
URL:	www.nets.eu				

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

Company Name:	Foregenix Ltd				
Lead QSA Contact Name:	Claudio Adami		Title:	QSA, SSA	
Telephone:	+39 3891714645		E-mail:	cadami@foregenix.com	
Business Address:	1st Floor, 8-9 High Street		City:	Marlborough	
State/Province:	Wiltshire	Country:	United Kingdom	Zip:	SN8 1AA
URL:	www.foregenix.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:	Payment Gateway, Authorization, Clearing and Settlement, Chargeback and Fraud services, Issuing, Account Management, Card Data Preparation	
Type of service(s) assessed:		
Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
□ Applications / software	□ Systems security services	☒ POS / 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		
□ Security services		
☒ 3-D Secure Hosting Provider		
□ Shared Hosting 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): Card Data Preparation		

***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.	Nets Estonia AS is a PCI Level 1 Service Provider Nets Estonia AS provide acquiring and issuing services in the form of authorization switching to card brands, back office processing, card personalization, chargeback processing and merchant help desk services. Authorization switching to card brands: An authorization message containing full Track 2 data is received either over the Internet or leased lines (for the partners ELISA/Elion) encapsulated over TLS 1.2 AES 256-bit encrypted traffic. The message is handed over to the payment application, which contains the business logic to decide whether to accept/decline or route to the issuer. If the decision is to route the message to the issuer, then the application formulates the message and opens a new TCP connection towards the relevant issuer. After the authorization message has reached the issuer, an authorization response message is sent back from the issuer. The described processing path is relevant both for card-present and card-not-present transactions (MOTO, e-commerce) originating from the interchange network and for authorization messages that contain an online PIN or do not contain an online PIN. The same message path is also used for ATM messages originated from the interchange network. Clearing and Settlement service - an internal financial transaction data validation, calculation and, finally, preparation of different outputs towards all financial institutions involved. The data includes the following: cardholder name, PAN and expiration date collected and stored encrypted in the database using Oracle Table Space Encryption AES 128-bit with key management using Oracle Wallet. The resulting files are then transmitted using SFTP AES 128-bit over leased lines towards the financial institutions. Fraud & Chargeback services are manually operated services. Workers involved in the process receive cardholder data via different communication channels over either SFTP AES 128-bit over the Internet or private leased lines; cardholder data (cardholder name, PAN, expiration date) is parsed and stored encrypted in the Oracle database using table space encryption AES 128-bit. The message

flow in the form of records in files is initiated and compiled from the database.

Merchant Help Desk services - involves activities of manipulating the merchant location and terminal configuration data in the acquiring service database which is protected using Oracle table space encryption AES 128-bit. This service does not involve any activities directly related to cardholder data.

Data preparation for card production:

Preparing the necessary data for card production (SAD and PAN) in the form of flat files and sending to the relevant card production company (over a file transfer mechanism) under IPsec VPN with AES 256-bit encryption.

Card Production microservices using APIs over Kubernetes container orchestration.

Request for PAN and CV2 is transmitted from the bank's internal network over TLS 1.3 with RSA 2048-bit encryption.

The PAN, expiration date, Bank ID and CV2 are returned (only in memory) to the API requester (Bank).

Acquiring services:

Providing acquiring services in the form of forwarding CHD to the relevant payment brand or acquiring bank on either on-premises servers (Visa/Mastercard) or over HTTPS to the relevant brand over TLS 1.2 with AES 256-bit encryption via dedicated MPLS lines.

3D Secure:

As part of the acquiring services, Nets Estonia provides 3D Secure validation services as well. The initial request is received from the Mastercard Directory server as an XML message over the Internet using TLS 1.2 with AES 128-bit encryption (Mastercard Directory servers whitelisted). The Initial response is given based on the ACS server's predefined PAN range definitions.

An additional 3DS flow is serving e-com merchants a redirect mechanism.

Cardholder data (Cardholder Name, PAN, CV2, Expiry Date) lands on web-page over the Internet using TLS 1.2 with AES 128-bit encryption.

	Cardholder is validated by the ACS (Acquiring services) server and the response is sent back to the merchant system over the Internet using TLS 1.2 with AES 128-bit encryption. STORAGE DETAILS: Nets Estonia AS does not use any offsite media storage companies. Nets Estonia AS stores cardholder data for: • Statement preparation • Settlement and clearing • Chargeback Cardholder Data stored: PAN, expiration date, cardholder name. • Card production: Cardholder Data stored: Account data (cardholder data and sensitive authentication data) is temporary stored for card production purposes. Protection of PAN during storage: Cardholder data at rest is protected using both database tablespace encryption using AES 128-bit (Oracle TDE) and HP storage level encryption using AES 256-bit; all card holder data is stored on mounted drives based in the central storage.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Not Applicable. The services assessed are not otherwise involved in the processing of cardholder data.

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 offices	1	Tartu mnt 63, Tallinn, Estonia
Primary data center	1	REDACTED
Secondary data center	1	

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)

REDACTED

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.*	Nets Estonia AS environment is located in two data centers. Segmentation is based on separation of system components into different logical locations on the network. Routing between these logical locations is restrictive and is granted based on the approval from the business. REDACTED

	REDACTED

	REDACTED

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:**
Visa	Transaction processing
Mastercard	Transaction processing
American Express	Transaction processing
Telia Eesti AS	Data center

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:	Payment Gateway, Authorization, Clearing and Settlement, Chargeback and Fraud services, Issuing, Account Management, Card Data Preparation

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 2:	☐	☒	☐	**2.1.1 - N/A no wireless networks transmitting account data** **2.2.3 - N/A no insecure services are used** **2.6 - - N/A not a shared hosting provider**
Requirement 3:	☐	☒	☐	**3.6 - N/A crypto keys are not shared with customers for transmission or storage of cardholder data.** **3.6.2 - N/A crypto-keys are not distributed**
Requirement 4:	☐	☒	☐	**4.1.1 - N/A no wireless networks transmitting account data**
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.1.5 - N/A no vendor accounts**
Requirement 9:	☐	☒	☐	**9.6 - N/A no media distribution** **9.6.2 - N/A no media distribution** **9.6.3 - N/A no media distribution** **9.9 - N/A no POS POI in the environment** **9.9.1 - N/A no POS POI in the environment** **9.9.2 - N/A no POS POI in the environment** **9.9.3 - N/A no POS POI in the environment**
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	**N/A Not a shared hosting provider**
Appendix A2:	☐	☐	☒	**N/A No use of Early TLS**

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:	01 Dec 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 DSS Validation

This AOC is based on results noted in the ROC dated 01 Dec 2022.

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 ***Nets Estonia AS*** 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 Sikich LLP*.*

Part 3b. Service Provider Attestation	
Signature of Service Provider Executive Officer ↑	*Date: 01 December 2022*
Service Provider Executive Officer Name: Zafer Balkan	*Title: Security and Compliance Manager*

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	Full PCI DSS v3.2.1 onsite assessment. This include scope validation, evidence gathering and validation of cardholder data processes and storage. Reporting and QA were conducted offsite.
Claudio Adami Digitally signed by Claudio Adami DN: O=Foregenix Ltd, CN=Claudio Adami, E=cadami@foregenix.com Reason: I am the author of this document Location: Date: 2022.12.01 14:30:35+01'00' Foxit PDF Reader Version: 12.0.2	
Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 01 December 2022
Duly Authorized Officer Name: Claudio Adami	*QSA Company:* Foregenix Ltd.

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

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**

[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.

		YES	NO	(If “NO” selected for any Requirement)
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	☒	☐	