Payment Card Industry
3-D Secure (PCI 3DS)

Attestation of Compliance

NETS Estonia AS (Estonia)

Section 1: 3DS Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the 3DS entity's assessment with the *PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server* (PCI 3DS Core Security Standard). Complete all sections. The 3DS entity is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the payment brands for PCI 3DS reporting and submission procedures.

Part 1. 3DS Entity and 3DS Assessor Information

Part 1a. 3DS Entity Organization Information

Company Name:	Nets Estonia AS	DBA (doing business as):	
Contact Name:	Paavo Sild	Title:	IT Director
Telephone:	+372 6711 477	E-mail:	paavo.sild@estcard.ee
Business Address:	Tartu mnt 63	City:	Tallinn
State/Province:	Harjumaa	Country:	Estonia	Zip:	10115
URL:	www.nets.eu		

Part 1b. 3DS Assessor Company Information

Company Name:	Compliance Control Ltd.		
Lead 3DS Assessor Contact Name:	Ivan Tverdokhlebov	Title:	Chief Executive Officer
Telephone:	+7 (926) 576-7095	E-mail:	ivan@compliance-control.ru
Business Address:	Revolutsionnaya street blg 3, office 306	City:	Volokolamsk
State/Province:	Moscow Reg.	Country:	Russia	Zip:	143600
URL:	www.compliance-control.ru		

Part 2. Executive Summary

Part 2a. 3DS Functions

Identify the 3DS Function(s) covered by this 3DS assessment (Check all that apply)	Details of EMVCo Letter of Approval (LOA):
☐ 3DS Server (3DSS)	LOA reference number: Date of LOA issued by EMVCo: Name of product LOA issued for:
☐ Access Control Server (ACS)	LOA reference number: Date of LOA issued by EMVCo: Name of product LOA issued for:
☐ Directory Server (DS)	LOA reference number: Date of LOA issued by EMVCo: Name of product LOA issued for:
☒ Other *(As defined by a payment brand)*	VISA approved 3DS solution is in use: PKK_ACS_J11 reference number: 3DNETW405

Note: If your organization performs 3DS functions that are not covered by this assessment, consult the applicable payment brand about validation for the other functions.

Part 2b. Description of 3DS Business

How and in what capacity does your business provide/manage 3DS functions?	Annual 3DS transactions volume is approx. 1.000.000

Part 2c. Locations

List types of facilities (for example, corporate offices, data centers) and a summary of locations covered by the PCI 3DS assessment.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
Example: Data Center	*3*	*Boston, MA, USA*
Head office	1	Tallin, Estonia
Data Center #1	1	Tallin, Estonia
Data Center #2	1	Saue vald, Estonia

Part 2d.

Not used for this AOC

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 3DS environment (3DE).* • *Critical system components within the 3DE, such as 3DS servers, databases, web servers, etc., and any other necessary 3DS components, as applicable.*	3DS environment is isolated with firewall network, consist of Web Application and DB servers operating in cluster mode. Connections to 3DE are provided within e-commerce channels only.
Does your business use network segmentation to affect the scope of your 3DS environment?	☒ Yes ☐ No

Part 2f. Third-Party Service Providers	
Does your company share 3DS data with any third-party service providers (for example, payment processors, gateways)?	☐ Yes ☒ No
Does your company rely on any third party for any PCI 3DS requirements, or for support or maintenance of the 3DS environment?	☐ Yes ☒ No

If Yes:

Name of service provider:	Description of services provided:

Part 2g. Summary of requirements tested to the PCI 3DS Security Standard	
Did the 3DS entity leverage a PCI DSS assessment to meet the PCI 3DS Part 1: Baseline Security Requirements?	☒ Yes ☐ No

Identify the appropriate assessment result for each high-level PCI 3DS requirement. Complete the table as follows:

- *If the results of a PCI DSS assessment have been verified as meeting all the PCI 3DS Part 1 Requirements:*
  - Select "In Place per PCI DSS" for the 3DS Part 1 Requirements.
  - Select the appropriate finding for each PCI 3DS Part 2 Requirement.
- *If a PCI DSS assessment is not being leveraged to meet all the PCI 3DS Part 1 Requirements:*
  - Select the appropriate finding for each 3DS Part 1 and Part 2 Requirement.

When determining the appropriate finding for each high-level 3DS requirement, the following principles apply:

1. If the finding for any requirement or sub-requirement is "Not in Place", select "Not in Place" for the high-level requirement.
2. If the finding for any requirement or sub-requirement is "N/A" and all other requirements are "In Place", select "In Place" for the high-level requirement..
3. If the finding for any requirement or sub-requirement is "In Place w/CCW" and all other requirements are "In Place", select "In Place w/CCW" for the high-level requirement.
4. If the findings include one or more requirements or sub-requirements as "N/A", and one or more as "In Place w/CCW", and all other requirements are "In Place", select "In Place w/CCW" for the high-level requirement.
5. If all requirements and sub-requirements are identified as "In Place", select "In Place" for the high-level requirement.

Summary of Findings		In Place per PCI DSS		In Place	In Place w/CCW	N/A	Not in Place
Part 1: Baseline Security Requirements							
P1-1	Maintain security policies for all personnel	☒	OR	☐	☐	☐	☐
P1-2	Secure network connectivity			☐	☐	☐	☐
P1-3	Develop and maintain secure systems			☐	☐	☐	☐
P1-4	Vulnerability management			☐	☐	☐	☐
P1-5	Manage access			☐	☐	☐	☐
P1-6	Physical security			☐	☐	☐	☐
P1-7	Incident response preparedness			☐	☐	☐	☐
Part 2: 3DS Security Requirements							
P2-1	Validate scope			☒	☐	☐	☐
P2-2	Security governance			☒	☐	☐	☐
P2-3	Protect 3DS systems and applications			☒	☐	☐	☐
P2-4	Secure logical access to 3DS systems			☒	☐	☐	☐
P2-5	Protect 3DS data			☒	☐	☐	☐
P2-6	Cryptography and key management			☒	☐	☐	☐
P2-7	Physically secure 3DS systems			☒	☐	☐	☐

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite PCI 3DS assessment, which is documented in an accompanying 3DS Report on Compliance (ROC).

The assessment documented in this attestation and in the 3DS ROC was completed on:	**May 12, 2020**
Was PCI DSS used to meet PCI 3DS Part 1: Baseline Security Requirements?	☒ Yes ☐ No
Have compensating controls been used to meet any PCI 3DS requirement?	☐ Yes ☒ No
Were any PCI 3DS requirements identified as being not applicable (N/A)?	☒ Yes ☐ No
Were any PCI 3DS requirements unable to be met due to a legal constraint?	☐ Yes ☒ No

Section 3: Validation and Attestation Details

Part 3. PCI 3DS Validation

This AOC is based on results noted in the 3DS ROC dated *May 12, 2020.*

Based on the results documented in the 3DS 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 3DS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby **Nets Estonia AS** has demonstrated full compliance with the PCI 3DS Core Security Standard.
☐	**Non-Compliant:** Not all sections of the PCI 3DS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(3DS Entity Company Name)* has not demonstrated full compliance with the PCI 3DS Core Security Standard. **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 applicable 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

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The 3DS ROC was completed according to the PCI 3DS Core Security Standard, Version *1.0*, and was completed according to the instructions therein.
☒	All information within the above-referenced 3DS ROC and in this attestation fairly represents the results of my assessment in all material respects.
☒	I have read the PCI 3DS Core Security Standard and I recognize that I must maintain 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 3DS requirements that apply.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Sikich LLP*

Part 3b. 3DS Entity Attestation

Signature of 3DS Entity Executive Officer ↑	*Date:* **May 12, 2020**
3DS Entity Executive Officer Name: **Paavo Sild**	*Title:* **IT Director**

Part 3c. 3DS Assessor Acknowledgement

Signature of Duly Authorized Officer of 3DS Assessor Company ↑	*Date:* **May 12, 2020**
Duly Authorized Officer Name: **Ivan Tverdokhlebov**	*Title:* **Chief Executive Officer**
3DS Assessor Company: **Compliance Control Ltd.**	

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI 3DS 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 3DS Requirement		Compliant to PCI 3DS Requirements *(Select One)*		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	**NO**	
P1	Maintain security policies for all personnel	☒	☐	
	Secure network connectivity	☒	☐	
	Develop and maintain secure systems	☒	☐	
	Vulnerability management	☒	☐	
	Manage access	☒	☐	
	Physical security	☒	☐	
	Incident response preparedness	☒	☐	
P2	Validate scope	☒	☐	
	Security governance	☒	☐	
	Protect 3DS systems and applications	☒	☐	
	Secure logical access to 3DS systems	☒	☐	
	Protect 3DS data	☒	☐	
	Cryptography and key management	☒	☐	
	Physically secure 3DS systems	☒	☐	