



Payment Card Industry (PCI) PIN Security Requirements

Attestation of Compliance for Onsite Assessments

For use with PIN Security Requirements v3.x

Version 3.2

May 2025

Document Changes

Date	Version	Description
2019	1.0	Initial release
May 2025	3.2	Modified version number to align with Standard and Program documents v3.x (previously v3.1 Revision 1.0c Feb 2023) Added Part 3d for PCI SSC countersignature (optional; for PIN Service Providers that choose to be listed on the PCI SSC Website) Minor language enhancements for clarity

Contents

Document Changes	i
1 Assessment Information	1
Instructions for Submission	1
2 Report on Compliance	5
3 Validation and Attestation Details	6

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's ("PIN Service Provider") compliance with the *Payment Card Industry PIN Security Requirements and Test Procedures* (PCI PIN). All sections must be completed. The PIN Service Provider 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. PIN Service Provider Information

Company Name:	Yandex.Cloud, LLC				
DBA (doing business as):	Yandex.Cloud	Business Identifier:	Not Applicable		
Contact Name:	Dmitriy Kudinov	Title:	Head of compliance direction		
Telephone:	+7 (965) 358-43-42	E-mail:	dimonk099@yandex-team.ru		
Business Address:	16 Lva Tolstogo str.	City:	Moscow		
State/Province:	Moscow	Country:	Russia	Postal Code:	119021
URL:	cloud.yandex.ru				

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

Company Name:	Deiteriy Co. Ltd.				
Lead QPA Contact Name:	Evgeniy Bezgodov	Business Identifier:	Not Applicable		
Telephone:	+7 (812) 361-61-55	E-mail:	evgeniy.bezgodov@deiteriy.com		
Business Address:	271A pr. Obukhovskoy Oborony	City:	Saint Petersburg		
State/Province:	Saint Petersburg	Country:	Russia	State/Province:	192012
URL:	deiteriy.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): Hardware hosting in the data center

Note: These categories are provided for assistance only, and are not intended to limit or predetermine the list of services that may have been included in the scope of the PCI PIN Assessment. If the PCI PIN Assessment included other services within its scope, or if these categories don't apply to your service, complete "Others." If you're unsure whether a particular service fits within a given category, consult with the applicable payment brand.

Services that are provided by the Service Provider 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 the types of facilities reviewed as part of the PCI PIN Assessment (for example, data centers, key-injection facilities, certification authority operations, etc.) and applicable details of the locations included in the PCI PIN review (e.g. city, country).

Type of facility assessed:	Date of Assessment	Location details:
<i>Example: Data Center</i>	<i>18-20 June, 2025</i>	<i>Boston, MA, USA</i>
Data center	September 26, 2025	Kaluga, Kaluga region, Russia
Data center	September 25, 2025	Sasovo, Ryazan region, Russia
Data center	September 24, 2025	Vladimir, Vladimir region, Russia

Part 2c. Summary of Requirements

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 (defined in Section 3 below).
- **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 each PCI PIN requirement 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 that the sub-requirement was not tested or was 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.

PCI PIN Control Objective	Details of Control Objectives Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Control Objective 1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Control Objective 2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Control Objective 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Control Objective 4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Control Objective 5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Control Objective 6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Control Objective 7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	29-1 – 29.3, 29-4.1 – 29-4.4.4, 30-1 – 30-1.2, , 31-1.2 – 31-1.6, 32-1.2, 32-1.4 – Not tested due to scope of assessment limitation.
Annex A1 – Control Objective 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Annex A1 – Control Objective 4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Annex A1 – Control Objective 5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Annex A1 – Control Objective 6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Annex A2 – Control Objective 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.

Annex A2 – Control Objective 4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Part 2c. Summary of Requirements Tested <i>(continued)</i>				
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 A2 – Control Objective 5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Annex A2 – Control Objective 6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Annex A2 – Control Objective 7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	32-3.1, 32-3.2 – N/A, the secure room has no windows or glass walls.
Annex B – Control Objective 1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Annex B – Control Objective 2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Annex B – Control Objective 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Annex B – Control Objective 4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Annex B – Control Objective 5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Annex B – Control Objective 6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not tested due to scope of assessment limitation.
Annex B – Control Objective 7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	29-1 – 29.3, 29-4.1 – 29-4.4.4, 30-3, 31-1.2 – 31-1.6, 32-1.2, 32-1.4, 32-8 – 32-9.12 – Not tested due to scope of assessment limitation.

2 Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in the ROC.

The assessment documented in this attestation and in the ROC was completed on:	September 26, 2025
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements not tested?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

3 Validation and Attestation Details

Part 3. PCI PIN Validation

This AOC is based on results noted in the PCI PIN Report on Compliance dated September 26, 2025 (the “ROC”). Based on the results documented in the ROC, the signatories identified in Parts 3b-3c, as applicable, assert(s) the following compliance status for the Service Provider (**check one**):

<input checked="" type="checkbox"/>	Compliant: All sections of the ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>Yandex.Cloud, LLC</i> has demonstrated full compliance with the PCI PIN Security Requirements.						
<input type="checkbox"/>	Non-Compliant: Not all sections of the ROC are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI PIN Security Requirements. Target Date for Compliance: DD/MMM/YYYY 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.						
<input type="checkbox"/>	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:						
	<table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td>Not Applicable</td> <td>Not Applicable</td> </tr> <tr> <td>Not Applicable</td> <td>Not Applicable</td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met	Not Applicable	Not Applicable	Not Applicable	Not Applicable
Affected Requirement	Details of how legal constraint prevents requirement being met						
Not Applicable	Not Applicable						
Not Applicable	Not Applicable						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:
(Check all that apply)

<input checked="" type="checkbox"/>	The ROC was completed in accordance with the <i>PCI PIN Security Requirements and Testing Procedures, Version</i> (version number) (the “PCI PIN Standard”), and the instructions therein.
<input checked="" type="checkbox"/>	All information provided in the ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input checked="" type="checkbox"/>	I have read the PCI PIN Standard and I recognize that I must maintain PCI PIN compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	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 Service Provider ↑

Service Provider Executive Officer Name: Dmitry Kudinov

Title: Head of compliance direction

Date: September 26, 2025

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

Describe the role performed by the QPA and others that participated from within the QPA Company:	Assessor
--	----------



Signature of Duly Authorized Officer of QPA Company ↑	Date: September 26, 2025
---	--------------------------

Duly Authorized Officer Name: Evgeniy Bezkodov	QPA Company: Deiteriy Co. Ltd.
--	--------------------------------

Part 3d. PCI SSC Acceptance (optional*)

* Applicable only if the Service Provider chooses to be listed on the List of PIN Service Providers on the Website.

PCI SSC does not assess or validate PIN Service Providers for compliance with the *PIN Security Requirements*. The signature below and subsequent listing of PIN Service Provider on the List of PCI PIN Service Providers signifies that the applicable QPA Company has determined that the PIN Service Provider complies with the *PIN Security Requirements*, that the QPA Company or PIN Service Provider has submitted a corresponding AOC to PCI SSC, and that the AOC, as submitted to PCI SSC, has satisfied all applicable quality review requirements as of the time of PCI SSC's review.

Signature of PCI Security Standards Council ↑	Date ↑
---	--------

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI PIN Standard” 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 Standard 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.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
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.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Control Objective 3:	Keys are conveyed or transmitted in a secure manner.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Control Objective 4:	Key-loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Control Objective 6:	Keys are administered in a secure manner.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Control Objective 7:	Equipment used to process PINs and keys is managed in a secure manner.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Annex A1 – Control Objective 3:	Keys are conveyed or transmitted in a secure manner.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Annex A1 – Control Objective 4:	Key-loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Annex A1 – Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Annex A1 – Control Objective 6:	Keys are administered in a secure manner.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Annex A2 – Control Objective 3	Keys are conveyed or transmitted in a secure manner.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable

PCI PIN Control Objective	Description of Control Objective	Compliant to PCI PIN Standard 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.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Annex A2 – Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Annex A2 – Control Objective 6:	Keys are administered in a secure manner.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Annex A2 – Control Objective 7:	Equipment used to process PINs and keys is managed in a secure manner.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
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.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Annex B – Control Objective 3:	Keys are conveyed or transmitted in a secure manner.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Annex B – Control Objective 4	Key-loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Annex B – Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Annex B – Control Objective 6:	Keys are administered in a secure manner.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable
Annex B – Control Objective 7:	Equipment used to process PINs and keys is managed in a secure manner.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not Applicable