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:	Bamcard d.d.				
DBA (doing business as):	BamCard		Business Identifier:		
Contact Name:	Merima Dozic		Title:	Payment Scheme Certification Manager, CISO	
Telephone:	+387 61739583		E-mail:	merima.djozic@bamcard.ba	
Business Address:	Trg Heroja 10/II		City:	Sarajevo	
State/Province:		Country:	Bosnia and Herzegovina	Postal Code:	71000
URL:	www.bamcard.ba				

Part 1b. Qualified PIN Assessor Company Information (if applicable)					
Company Name:	Sovereign Secure Limited				
Lead QPA Contact Name:	Cetin Guldali		Title:	Senior Security Consultant	
Telephone:	+90 533 0 933 100		E-mail:	cetin.guldali@sovereignsecure.co.uk	
Business Address:	79 Market Street		City:	Farnworth	
State/Province:	Greater Manchester	Country:	UK	Postal Code:	BL4 7NS
URL:	https://sovereign-secure.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): N/A

***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): N/A

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*
Data Center	28 Feb, 02 Mar, 04 Mar 2022	Sarajevo, Bosnia and Herzegovina

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:	☐	☒	☐	**Not Applicable Parts:** **1.1, 2.1, 2.4, 3- Bamcard does not have any PED/POI device in the environment under current assessment.** **2.3- "Not-on-us" transactions route through the banks and not reach BamCard environment.**
Control Objective 2:	☐	☒	☐	**Not Applicable Parts:** **6.2- No multi-purpose computing systems were in use. Dedicated stations used for this purpose.** **6.5- There was no asymmetric key used in the environment under current assessment**
Control Objective 3:	☐	☒	☐	**Not Applicable Parts:** **8.4- There was no public key method used in the environment under current assessment.** **9.6- Components or shares of multiple keys were not being sent simultaneously between the same sending and receiving custodians.**
Control Objective 4:	☐	☒	☐	**Not Applicable Parts:** **12.6- No other SCD is used to load key, only HSM s are used for that purpose.** **12-8- Public key cryptography was not used in the environment under current assessment.**
Control Objective 5:	☐	☒	☐	**Not Applicable Parts:** **19.2- Private key cryptography was not used in the environment under current assessment.** **19.3- Public key cryptography was not used in the environment under current assessment** **19.5- A production platform (HSM and server/standalone computer) were not temporarily used for test purposes.** **20.1- Bamcard was not responsible for ATM terminals, and there is no POI terminals in the environment under current assessment.** **20.2- Transaction-originating terminals (for example POI device) were not interfacing with more than one acquiring organization.**

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.)
				20.3, 20.4- Key derivation process were not existing.
Control Objective 6:	☐	☒	☐	**Not Applicable Parts:** **21.3.3- No tokens are in use to store the keys** **23.2- No MFK was used out of its own HSM for any other purposes.** **27- backup keys are not in use.**
Control Objective 7:	☐	☒	☐	**Not Applicable Parts:** **30- No POI in the environment under current assessment.**
Annex A1 – Control Objective 3:	☐	☐	☒	**All not applicable for BamCard**
Annex A1 – Control Objective 4:	☐	☐	☒	**All not applicable for BamCard**
Annex A1 – Control Objective 5:	☐	☐	☒	**All not applicable for BamCard**
Annex A1 – Control Objective 6:	☐	☐	☒	**All not applicable for BamCard**
Annex A2 – Control Objective 3	☐	☐	☒	**All not applicable for BamCard**
Annex A2 – Control Objective 4:	☐	☐	☒	**All not applicable for BamCard**
Annex A2 – Control Objective 5:	☐	☐	☒	**All not applicable for BamCard**
Annex A2 – Control Objective 6:	☐	☐	☒	**All not applicable for BamCard**
Annex A2 – Control Objective 7:	☐	☐	☒	**All not applicable for BamCard**
Annex B – Control Objective 1:	☐	☐	☒	**All not applicable for BamCard**
Annex B – Control Objective 2:	☐	☐	☒	**All not applicable for BamCard**
Annex B – Control Objective 3:	☐	☐	☒	**All not applicable for BamCard**

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:	☐	☐	☒	**All not applicable for Karbil.**
Annex B – Control Objective 5:	☐	☐	☒	**All not applicable for BamCard**
Annex B – Control Objective 6:	☐	☐	☒	**All not applicable for BamCard**
Annex B – Control Objective 7:	☐	☐	☒	**All not applicable for BamCard**

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:	*28/03/2022*	
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 *28/03/2022.*

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 *Bamcard d.d.* 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 *(Service Provider Company Name)* 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 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 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

Merima Đozić

Signature of Executive Officer of Assessed Entity ↑	
Assessed Entity Executive Officer Name:	**Merima Dozic**
Title:	**Payment Scheme Certification Manager, CISO**
Date:	**30/03/2022**

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

Describe the role performed by the QPA and others that participated from within the QPA Company:	*Assessment*

W.Iqbal

Signature of Duly Authorized Officer of QPA Company ↑	*Date: 30/03/2022*
Duly Authorized Officer Name: Wahid Iqbal	*QPA Company:* Sovereign Secure 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.	☒	☐	
Annex A1 – Control Objective 4:	Key-loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.	☒	☐	
Annex A1 – Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	☒	☐	
Annex A1 – Control Objective 6:	Keys are administered in a secure manner.	☒	☐	
Annex A2 – Control Objective 3	Keys are conveyed or transmitted in a secure manner.	☒	☐	

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.	☒	☐	
Annex A2 – Control Objective 5:	Keys are used in a manner that prevents or detects their unauthorized usage.	☒	☐	
Annex A2 – Control Objective 6:	Keys are administered in a secure manner.	☒	☐	
Annex A2 – Control Objective 7:	Equipment used to process PINs and keys is managed in a secure manner.	☒	☐	
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.	☒	☐	