



# **Payment Card Industry Data Security Standard**

---

## **Attestation of Compliance for Report on Compliance – Service Providers**

**Version 4.0.1**

Publication Date: August 2024

# **PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers**

**Entity Name: IXOPAY GmbH**

**Date of Report as noted in the Report on Compliance: 03.12.2024**

**Date Assessment Ended: 02.12.2024**

## Section 1: Assessment Information

### Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures* ("Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

#### Part 1. Contact Information

##### Part 1a. Assessed Entity (ROC Section 1.1)

Company name:	IXOPAY GmbH
DBA (doing business as):	IXOPAY
Company mailing address:	Vorgartenstrasse 206c, 1020 Vienna, Austria
Company main website:	<a href="https://www.ixopay.com">https://www.ixopay.com</a>
Company contact name:	John Noltensmeyer
Company contact title:	CISO
Contact phone number:	+43-1-353-0505
Contact e-mail address:	<a href="mailto:j.noltensmeyer@ixopay.com">j.noltensmeyer@ixopay.com</a>

##### Part 1b. Assessor (ROC Section 1.1)

Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.

PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not applicable
Qualified Security Assessor	
Company name:	Dot.Bit d.o.o.
Company mailing address:	Stubicka 48A, 10110 Zagreb, Croatia
Company website:	<a href="https://dotbit.eu">https://dotbit.eu</a>
Lead Assessor name:	Branimir Pacar
Assessor phone number:	+385 99 2265696
Assessor e-mail address:	<a href="mailto:branimir.pacar@dotbit.eu">branimir.pacar@dotbit.eu</a>
Assessor certificate number:	QSA: 203-884, 3DS QSA:1100-141, QPA:1300-201

## Part 2. Executive Summary

### Part 2a. Scope Verification

Services that were **INCLUDED** in the scope of the Assessment (select all that apply):

Name of service(s) assessed:

Payment Processing and payment card tokenization

Type of service(s) assessed:

**Hosting Provider:**

- Applications / software
- Hardware
- Infrastructure / Network
- Physical space (co-location)
- Storage
- Web-hosting services
- Security services
- 3-D Secure Hosting Provider
- Multi-Tenant Service Provider
- Other Hosting (specify):

**Managed Services:**

- Systems security services
- IT support
- Physical security
- Terminal Management System
- Other services (specify):

**Payment Processing:**

- POI / 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): Payment Processing and payment card tokenization

**Note:** These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.

## Part 2. Executive Summary *(continued)*

### Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were **NOT INCLUDED** in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	Not applicable	
Type of service(s) not assessed:		
<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services:</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<b>Payment Processing:</b> <input type="checkbox"/> POI / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		
Provide a brief explanation why any checked services were not included in the Assessment:	Not applicable	

### Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	<p>IXOPAY hosts and maintains a solution that allows clients to vault sensitive primary account numbers (PANs) and tokenize them. Cardholder data is directly transmitted to the IXOPAY Vault via the iframe payment form or the direct server-to-server API. The token is returned to the merchant for future reference.</p> <p>Merchants may utilize their tokens to initiate one-off payments, or use them for recurring payments at any time of their choosing. IXOPAY also offers encryption and tokenization of PAN data in bulk to satisfy migration needs of its clients.</p>
---	---

<p>Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.</p>	<p>.IXOPAY is a payment orchestration platform, that handles large volumes of cardholder data on a daily basis. Besides direct transmission, processing, storage, and the implementation of controls and processes to protect such data handling, IXOPAY has no further involvement in the security of cardholder data.</p>
<p>Describe system components that could impact the security of account data.</p>	<p>IXOPAY GmbH provides the payment orchestration solution to the customers and provides the payment service that requires them to collect cardholder data. Cardholder data is only temporarily stored while transaction is being processed except in the case of recurring transactions where the PAN number is stored for a longer period of time. No sensitive data is stored after the transaction was authorized.</p> <p>PAN is stored only in an encrypted form as part of the tokenization mapping table. All encryption operations utilize Hashicorp Vault and HSM.</p>

## Part 2. Executive Summary *(continued)*

### Part 2c. Description of Payment Card 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 POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*
- *System components that could impact the security of account data.*

IXOPAY is receiving cardholder data through APIs. All connections are sent through the load balancer and are forwarded to the front-end web servers. The web servers are encrypting the primary account number and sensitive authentication data (CVVs) using an HSM system before storage. The entry is stored together with a randomly generated token, which is later used for identification of the transaction. The token generation is not based upon any cardholder data. Knowledge of a token does not provide any information about the underlying payment data. After the data has been encrypted it is stored in the database.

The authorization of transactions is initiated by the payment gateway and the merchant using the payment token. The authorization is received on the load balancers, forwarded to a separate tier of web servers, which decrypt the data from the database using the HSM and prepare the transaction for processing at the payment processor. The result will be returned to the payment gateway and the merchant.

After decryption of the cardholder data, sensitive authentication data (CVV) will be deleted and is no longer stored in the database. Encrypted PANs are only stored for recurring transactions.

Indicate whether the environment includes segmentation to reduce the scope of the Assessment.

(Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)

Yes  No

### Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Data center	2	Vienna, Austria
Corporate office	1	Vienna, Austria

---




## Part 2. Executive Summary *(continued)*

### Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions\*?

Yes  No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
Not applicable				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD

\* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

## Part 2. Executive Summary *(continued)*

### Part 2f. Third-Party Service Providers (ROC Section 4.4)

For the services being validated, does the entity have relationships with one or more third-party service providers that:

<ul style="list-style-type: none"> <li>• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> <li>• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)</li> </ul>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
<ul style="list-style-type: none"> <li>• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).</li> </ul>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

#### If Yes:

Name of Service Provider:	Description of Services Provided:
ACI Worldwide (Germany) GmbH - Pay.On Adyen N.V. Bankart D.O.O. Cardtech Card & POS Service GmbH (Concardis) CashFlows Europe Limited CKB Bank CKO Technology Services Ltd DBA Checkout.com Clearhaus A/S Coriunder Limited Credorax Bank Ltd Pay Plug (Dalenys Payment) Diners E-Comprocessing Ltd. E-xact Transactions EBANX S.A. ECommPay LTD.DBA: ECommPay IT; EmerchantPay via IPG Europe Limited Worldline SE Germany Euronet Worldwide Europe EFT Fivespot Kenya Limited DBA iPayAfrica	Payment processing
Flutterwave Technology Solutions Ltd. GlobalConnect Services BV (Ingenico) Inatec Payment AG DBA Powercash21 JPMorgan Chase & Co Kount Inc KSG Kartenverrechnungs- und Service GmbH DBA CardComplete	Payment processing

<p>Mercury Processing Services International d.o.o DBA NestPay MultiSafepay B.V. Network Merchants, LLC (aka NMI) Paydoo Payments UAB Monext SAS Paymentwall B.V. Paysafe Processing Ltd PXP Financial Group Ltd (DBA PXP Accept GmbH) Qualpay Inc. Safecharge International Group Ltd. Secure Trading Limited (dba Trust Payments) Shimotomo Sia Decta DBA DECTA Worldline SA Spredly, Inc. Stripe Inc TabaPay, Inc Transact.eu Truevo Technologies Limited Ukrainian Processing Center (UPC) Vindicia Inc. WorldPay (UK) Ltd.</p>	
<p>Silverflow B.V. VÖB-ZVD Processing GmbH DBA Deutsche Bank Braintree, a PayPal Service Market Pay Denmark AltPayNet Corp. Zooz Mobile Ltd DBA PaymentsOs / PayU Payone GmbH Wpay Pty Ltd Valitor hf. Francisco Sancha 12 Mastercard Payment Gateway Services 2C2P Pte. Ltd. GlobalBlue SA Payfort / Amazon Payment Services PAYGENT Co., Ltd. Nexi Payments S.p.A Eftex Pty Ltd Mercado Libre, Inc. Areeba Iraq Areeba Verto Cybersource Corporation First Atlantic Commerce Ltd. Tillpayments</p>	<p>Payment processing</p>

Infibeam Avenues Limited Alignet JCC Payment Systems Limited Sub1 S.A. Maxpay limited	
NextLayer	Data center provider

**Note:** Requirement 12.8 applies to all entities in this list.

## Part 2. Executive Summary (continued)

### Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either “Not Applicable” or “Not Tested,” complete the “Justification for Approach” table below.

**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 Processing and payment card tokenization

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.

- 2.2.5 Not applicable, Ixopay is not using insecure services, protocols or daemons
- 2.3.1 Not applicable, Ixopay does not have wireless networks in PCI DSS scope.
- 2.3.2 Not applicable, Ixopay does not have wireless networks in PCI DSS scope.
- 3.3.1.1 Not applicable, Ixopay does not receive any track data.
- 3.3.1.3. Not applicable, Ixopay does not receive any PIN data.
- 3.3.3 Not applicable, Ixopay is not an issuer and does not support issuing services.
- 3.4.2 Not applicable, this is a future dated requirement.
- 3.5.1.1 Not applicable, this is a future dated requirement.
- 3.5.1.2 Not applicable, Ixopay does not use disk level encryption for protecting PAN.
- 3.5.1.3 Not applicable, Ixopay does not use disk level encryption for protecting PAN.
- 4.2.1.2 Not applicable, Ixopay does not have any wireless networks connected to the cardholder data environment.
- 4.2.2 Not applicable, Ixopay does not use end-user messaging technologies for sending PANs.
- 5.2.3.1 Not applicable, this is a future dated requirement.
- 5.3.2.1 Not applicable, this is a future dated requirement.
- 5.3.3 Not applicable, Ixopay does not use removable media in cardholder data environment.
- 6.4.3 Not applicable, this is a future dated requirement.
- 7.2.4 Not applicable, this is a future dated requirement.
- 7.2.5 Not applicable, this is a future dated requirement.
- 7.2.5.1 Not applicable, this is a future dated requirement.
- 8.2.3 Not applicable, Ixopay does not have a remote access to customers premises
- 8.2.7 Not applicable, Ixopay does not have third parties that are accessing cardholder data environment.
- 8.3.10 Not applicable, this is a future dated requirement.
- 8.3.10.1 Not applicable, this is a future dated requirement.
- 8.5 Not applicable, this is a future dated requirement.
- 8.6.1 Not applicable, this is a future dated requirement.
- 8.6.2 Not applicable, this is a future dated requirement.
- 8.6.3 Not applicable, this is a future dated requirement.

	<p>9.2.2 Not applicable, there are no publicly accessible network jacks within the facility.</p> <p>9.2.3 Not applicable, there are no wireless access points in facility hosting cardholder data environment.</p> <p>9.4.1.1 Not applicable, Ixopay does not have offline media backups with cardholder data.</p> <p>9.4.1.2 Not applicable, Ixopay does not have offline media backups with cardholder data.</p> <p>9.4.1 Not applicable, Ixopay does not have offline media backups with cardholder data.</p> <p>9.4.3 Not applicable, Ixopay does not have media with cardholder data that is sent outside the facility.</p> <p>9.4.4 Not applicable, Ixopay does not have media with cardholder data that is sent outside the facility.</p> <p>9.4.6 Not applicable, Ixopay does not have any hard copy materials containing cardholder data.</p> <p>9.5.1 Not applicable, Ixopay does not have any POI devices.</p> <p>9.5.1.1 Not applicable, Ixopay does not have any POI devices.</p> <p>9.5.1.2 Not applicable, Ixopay does not have any POI devices.</p> <p>9.5.1.2.1 Not applicable, Ixopay does not have any POI devices.</p> <p>9.5.1.3 Not applicable, Ixopay does not have any POI devices.</p> <p>11.3.1.2 Not applicable, this is a future dated requirement.</p> <p>11.4.7 Not applicable, Ixopay is not a multitenant service provider.</p> <p>11.5.1.1 Not applicable, this is a future dated requirement.</p> <p>11.6.1 Not applicable, this is a future dated requirement.</p> <p>12.3.1 Not applicable, this is a future dated requirement.</p> <p>12.3.2 Not applicable, Ixopay is not using customized approach.</p> <p>12.5.3 Not applicable, this is a future dated requirement.</p> <p>12.6.3.1 Not applicable, this is a future dated requirement.</p> <p>12.6.3.2 Not applicable, this is a future dated requirement.</p> <p>12.10.4.1 Not applicable, this is a future dated requirement.</p> <p>12.10.7 Not applicable, this is a future dated requirement.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>Not applicable</p>

## Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

Date Assessment began: <b>Note:</b> <i>This is the first date that evidence was gathered, or observations were made.</i>	2024-09-12
Date Assessment ended: <b>Note:</b> <i>This is the last date that evidence was gathered, or observations were made.</i>	2024-12-02
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No



## Section 3 Validation and Attestation Details

### Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC 2024-12-03)*.

Indicate below whether a full or partial PCI DSS assessment was completed:

- Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.
- Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)*:

**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby IXOPAY GmbH has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.

**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements.

**Target Date** for Compliance: YYYY-MM-DD

An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.

**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.

This option requires additional review from the entity to which this AOC will be submitted.

*If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

### Part 3. PCI DSS Validation *(continued)*


#### Part 3a. Service Provider Acknowledgement

**Signatory(s) confirms:**



(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

#### Part 3b. Service Provider Attestation

	
Signature of Service Provider Executive Officer <sup>↑</sup>	Date: 2024-12-03
Service Provider Executive Officer Name: John Noltensmeyer	Title: CISO

#### Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	<input checked="" type="checkbox"/> QSA performed testing procedures.
	<input type="checkbox"/> QSA provided other assistance. If selected, describe all role(s) performed:
	
Signature of Lead QSA <sup>↑</sup>	Date: 2024-12-03
Lead QSA Name: Branimir Pacar	
	
Signature of Duly Authorized Officer of QSA Company <sup>↑</sup>	Date: 2024-12-03
Duly Authorized Officer Name: Tomislav Zivkovic	QSA Company: Dot.Bit d.o.o.

#### Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	<input type="checkbox"/> ISA(s) performed testing procedures.
	<input type="checkbox"/> ISA(s) provided other assistance. If selected, describe all role(s) performed:

## Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement below. For any “No” responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain network security controls	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

*Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: [https://www.pcisecuritystandards.org/about\\_us/](https://www.pcisecuritystandards.org/about_us/)*