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:	LINKAPI TECNOLOGIA S.A.		DBA (doing business as):	LinkApi	
Contact Name:	Enio Moraes		Title:	CIO / DPO	
Telephone:	+55 12 99224-7327		E-mail:	enio.moraes@semantix.ai	
Business Address:	Avenida Eusébio Matoso, 1.375, 13º andar, conjunto 1301, Pinheiros.		City:	São Paulo	
State/Province:	SP	Country:	Brazil	Zip:	05423-180
URL:	https://www.semantix.ai/linkapi-agora-e-semantix				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Insside Información Inteligente SRL				
Lead QSA Contact Name:	Marcelo A. Martinez		Title:	QPA / QSA Sr. Managing Consultant	
Telephone:	+54 (11) 5273-8800		E-mail:	mmartinez@insside.net	
Business Address:	Billinghurst 1656		City:	CABA	
State/Province:	Buenos Aires	Country:	Argentina	Zip:	1425
URL:	www.insside.net				

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	
Type of service(s) 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): Processing and translating card transaction data
☐ 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):		

***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:	E-commerce services	
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:	The e-commerce solution is not LinkApi responsibility, because LinkApi does not provide the e-commerce solution. LinkApi only provides an infrastructure with message translate to any e-commerce solution, where it is possible receives any transaction information, independent of the message format and to be send and understood to acquirers, sub-acquirers and payment gateways.	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	LinkApi is a technology company working like an API integration and management platform. The company provides a specific solution to connect any market solution and translate the card transaction information received by an external solution, according to the type of message format, to a specific code that can be understood by acquires and processors. LinkApi only processes and transmits cardholder data and does not store it. The card data (full PAN, CVV, CVC, expiration data and cardholder name) is captured by LinkApi's Clients, through e-commerce application that is not a LinkApi solution (e-commerce solution is never provided by LinkApi), that encrypt the data during the transmitting (HTTPS with TLSv1.2) and sends the authorization request to LinkApi environment via Internet connection (HTTPS with TLSv1.2). The authorization request is received and processed via API OCC and sends the authorization requesting to sub-acquires and acquires in a secure connection (HTTPS with TLSv1.2). LinkApi s does not store any PAN or sensitive data to persistent storage. There is no retention of clear-text cardholder data even in volatile memory, once the authorization process is finished the PAN card data is purged of volatile memory by automatic process. LinkApi works as a bridge between the customer and the payment gateway. In this way, it only transmits transactions securely, using Microsoft Azure PaaS Services infraestructure.
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