PCI Security Standards Council®

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2

April 2016

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:	Ingenico e-Commerce Solutions BVBA/SPRL		DBA (doing business as):	Ingenico e-Commerce Solutions	
Contact Name:	Stefaan Lemaire		Title:	Head of Information Security	
Telephone:	+32 (0) 2 286 96 11		E-mail:	Stefaan.Lemaire@ecom.ingenico.com	
Business Address:	Woluwedal/Boulevard de la Woluwe 102		City:	Brussels/Bruxelles	
State/Province:	N/A	Country:	Belgium	Zip:	B-1200
URL:	http://payment-services.ingenico.com				

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

Company Name:	Advantio Ltd.				
Lead QSA Contact Name:	Oleg Aksyonenko		Title:	Managing Consultant	
Telephone:	+380 67 7016691		E-mail:	oleg.aksyonenko@advantio.com	
Business Address:	Block 4, Harcourt Centre Harcourt Road		City:	Dublin	
State/Province:	N/A	Country:	Republic of Ireland	Zip:	D2
URL:	www.advantio.com				

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:	Ingenico e-Commerce Payment Platform, Managed Services provided to other Ingenico group entities
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): Software Development service	**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): TravelHub		

***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:	Not applicable

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:	Not applicable

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Ingenico e-Commerce Solutions is the name of the Payment Service Provider previously known as Ogone and processes transactions for more than 64,000 clients across about 240 countries. Ingenico e-Commerce Solutions makes available APIs and payment pages to its merchants and white-labelled Payment Service Provider. Ingenico e-Commerce Solutions processes exclusively Card-Not-Present (CNP) transactions with an annual volume of over 500 million transactions through more than 200 connected acquiring banks. Ingenico e-Commerce Solutions processes cardholder data including PANs, expiration dates, service codes and card verification code/value though no Track-2, PINs and PIN blocks for the purposes of authorization. PANs and expiration dates are processed by Ingenico e-Commerce Solutions for the purposes of settlement and clearance. Whilst limited chargeback processing is supported, the process does not involve cardholder data. Ingenico e-Commerce Solutions transmits, processes and stores cardholder data only in order to provide the services, which are part of the business. Any cardholder data storage is reduced to minimum needed.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Ingenico e-Commerce Solutions BVBA/SPRL provide managed IT services to other Ingenico entities. These services include IT support, managed security services, application development and support and may indirectly impact the security of cardholder data.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
Example: Retail outlets	*3*	*Boston, MA, USA*
Head Office	1	Brussels/Bruxelles, Belgium
Data Centers	3	Zaventem, Nossegem, Belgium; Saint Denis, France

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☒ Yes □ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Ingenico Payment Platform	4.115	Ingenico e-Commerce Solutions	□ Yes ☒ No	Not applicable, in-house developed application
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	

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 cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	All connections into and out the CDE, including the Internet and corporate office network. All application servers, including processing servers responsible for transaction authorization and settlement. All database servers, including the ones storing cardholder data. All DMZ servers, including web servers and TLS load balancers responsible for receiving transaction data. All components that provide security, management or monitoring services for the CDE or could otherwise impact security of the CDE. All network devices, such as firewalls, routers, proxies, used to segment the environment through logical VLANs.
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes □ No

Part 2f. Third-Party Service Providers	
Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated? If Yes: Name of QIR Company: QIR Individual Name: Description of services provided by QIR:	☐ Yes ☒ No
Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☒ Yes ☐ No

If Yes:

Name of service provider:	**Description of services provided:**
TNS, LYRA	Network provider/transmitter
AsiaPay, FirstData, NETS, Paypal, SITA aero	Payment Gateway
Equinix SAS, Interxion Belgium, Mobistar	Co-location, unmanaged hosting
Ingenico Financial Services, Ingenico Group (AXIS)	Payment Processor
Ingenico ePayments North Campus (GlobalCollect)	Payment Service Provider

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

Part 2g. Summary of Requirements Tested

For each PCI DSS 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.*

Name of Service Assessed:	Ingenico e-Commerce Payment Platform

PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☒	□	□	
Requirement 2:	□	☒	□	**2.1.1 N/A (Wireless is not used within IES CDE); 2.6 N/A (Ingenico e-Commerce Solutions is not a shared hosting provider)**
Requirement 3:	□	☒	□	**3.4.1 N/A (Disk encryption is not used); 3.5.1 N/A (The assessment was completed prior to the 31st January 2018); 3.6.6 N/A (No manual clear-text cryptographic key-management operations)**
Requirement 4:	□	☒	□	**4.1.1 N/A (Wireless is not used within IES CDE)**
Requirement 5:	□	☒	□	**5.1.2 N/A (All operating systems in use are considered commonly affected by malware)**
Requirement 6:	□	☒	□	**6.4.6 N/A (The assessment was completed prior to the 31st January 2018)**
Requirement 7:	☒	□	□	
Requirement 8:	□	☒	□	**8.1.5 N/A (No remote access to IES CDE by vendors); 8.3.1 N/A (The assessment was completed prior to the 31st January 2018); 8.5.1 N/A (Ingenico e-Commerce Solutions does not have remote access to customer premises)**
Requirement 9:	□	☒	□	**9.1.2 N/A (No publicly accessible network jacks within IES CDE); 9.8.1 N/A (No cardholder data storage in paper format); 9.9, 9.9.1, 9.9.2, 9.9.3 N/A (No devices**

				that capture payment card data via direct physical interaction with the card within IES CDE)
Requirement 10:	□	☒	□	10.8, 10.8.1 N/A (The assessment was completed prior to the 31st January 2018)
Requirement 11:	□	☒	□	11.1.1 N/A (No authorised wireless access points within or connected to IES CDE); 11.3.4.1 N/A (The assessment was completed prior to the 31st January 2018)
Requirement 12:	□	☒	□	12.3.9 N/A (No vendor remote access to IES CDE); 12.4.1, 12.11, 12.11.1 N/A (The assessment was completed prior to the 31st January 2018)
Appendix A1:	□	□	☒	N/A (Ingenico e-Commerce Solutions is not a shared hosting provider)
Appendix A2:	□	☒	□	A2.1 N/A (No POS POI terminals within IES CDE)

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:	*15 September 2017*	
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 DSS Validation

This AOC is based on results noted in the ROC dated *15 September 2017.*

Based on the results documented in the 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 DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Ingenico e-Commerce Solutions BVBA/SPRL* has demonstrated full compliance with the PCI DSS.

☐ **Non-Compliant:** Not all sections of the PCI DSS 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 DSS.

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
9.1.1.c	Advantio Ltd. reviewed extracts from applicable Belgian and French legislation about maximum permitted CCTV footage retention period of 30 days: French Law: La loi n78-17 du 6 janvier 1978 Belgian Law: 21 mars 2007 - loi reglant l'installation et l'utilisation de cameras de surveillance

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒ The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2*, 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 confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.

☒ I have read the PCI DSS and I recognize that I must maintain PCI DSS 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 DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)

☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Qualys*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* **15 September 2017**
Service Provider Executive Officer Name: **Stefaan Lemaire**	*Title:* **Head of Information Security**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	*Full onsite Level 1 service provide assessment.*

Signature of Duly Authorized Officer of QSA Company ↑	*Date: 15 September 2017*
Duly Authorized Officer Name: Martin Petrov	*QSA Company:* Advantio Ltd.

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	*Not applicable*

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS 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 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 a firewall configuration to protect cardholder data	☒	□	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	□	
3	Protect stored cardholder data	☒	□	
4	Encrypt transmission of cardholder data across open, public networks	☒	□	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	□	
6	Develop and maintain secure systems and applications	☒	□	
7	Restrict access to cardholder data by business need to know	☒	□	
8	Identify and authenticate access to system components	☒	□	
9	Restrict physical access to cardholder data	☒	□	
10	Track and monitor all access to network resources and cardholder data	☒	□	
11	Regularly test security systems and processes	☒	□	
12	Maintain a policy that addresses information security for all personnel	☒	□	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	□	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS	☒	□	