



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:	Ingenico eCommerce Solutions BVBA / SPRL	DBA (doing business as):	Not Applicable.		
Contact Name:	Stefaan Lemaire	Title:	Head of Information Security Management		
Telephone:	+32477271304	E-mail:	Stefaan.Lemaire@ingenico.com		
Business Address:	Leonardo Da Vincilaan 3	City:	Brussels		
State/Province:	Not Applicable.	Country:	Belgium	Zip:	1930
URL:	https://ingenico.be				

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

Company Name:	Trustwave				
Lead QSA Contact Name:	Leonardo Polvora	Title:	Principal Security Consultant		
Telephone:	+44 (0) 845-456-9611	E-mail:	lpolvora@trustwave.com		
Business Address:	Westminster Tower, 3 Albert Embankment	City:	London		
State/Province:	Not Applicable.	Country:	United Kingdom	Zip:	SE1 7SP
URL:	http://www.trustwave.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: Payment Processing – Internet, Payment Gateway/Switch, Clearing and Settlement, 3-D Secure Hosting Provider, System security services, IT support, Software development, Fraud and Chargeback, Merchant Services

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

Payment Processing:

- POS / card present
- Internet / e-commerce
- MOTO / Call Center
- ATM
- Other processing (specify):

- | | | |
|---|--|--|
| <input type="checkbox"/> Account Management | <input checked="" type="checkbox"/> Fraud and Chargeback | <input checked="" 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 checked="" type="checkbox"/> Clearing and Settlement | <input checked="" type="checkbox"/> Merchant Services | <input type="checkbox"/> Tax/Government Payments |
| <input type="checkbox"/> Network Provider | | |
| <input type="checkbox"/> 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: 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 eCommerce Solutions BVBA / SPRL (IECS) is a Level 1 Payment Service Provider.

IECS receive, transmits and processes cardholder data (PAN, cardholder name, expiry, card security codes (CVV2, CVC2, CID, CAV2)) as part of its services. Cardholder data (PAN, cardholder name, expiry, card security codes (CVV2, CVC2, CID, CAV2)) are received from merchants and/or clients (white-labelled Payment Service Providers) via API integrations or from the cardholder via payment pages over TLS v1.2.

IECS processes cardholder data (PAN, cardholder name, expiry, card security codes (CVV2, CVC2, CID, CAV2)) for the purposes of authorization. Authorization of transactions may be performed in real-time or via a batch file received from the merchant / client via a dedicated IPsec VPN. IECS stores cardholder data (card security codes (CVV2, CVC2, CID, CAV2)) temporarily in a database, encrypted prior to authorization during the authorization process to establish authorization operations and destroys the data upon completion of authorization processing.

IECS stores cardholder data (PAN) for transaction historical purposes and in order to support service operations in a database encrypted, truncated and hashed.

IECS processes and transmits cardholder data (PAN and expiry) for the purposes of settlement and clearance. Settlements transactions are transmitted to the relevant acquirer over TLS v1.2.

IECS supports fraud and chargeback processing but the process does not include cardholder data.

IECS transmits, processes and stores cardholder data only 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.

Not Applicable. IECS is not otherwise involved, nor has the ability to 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):
Data Centers	3	1 in Saint-Denis, Paris, France 2 in Brussels, Belgium
Head office	1	Zavantem, Belgium

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 ePayment Platform	4.132.271.0	Ingenico eCommerce Solutions BVBA / SPRL	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Not Applicable.

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.

The in-scope IECS environments and zones in the data centers were included in the assessment.

The following logical environments and all systems and procedures which support these zones were included:

- DC 1 – Brussels PCI Production Environment
- DC 2 – Brussels PCI Production Environment
- DC 3 – Paris PCI Production Environment

The IPsec VPN tunnels and private lines with Acquiring banks and other Ingenico group entities, the remote access IPsec VPNs and the entities Internet e-commerce TLS traffic were included as part of the assessment.

The following elements were included and reviewed during the assessment:

- Payment applications
- Databases
- Operating systems
- Firewalls
- Loadbalancers
- Routers

- Switches
- HSMs
- Workstations
- Application Servers
- Web Servers
- Web Application Firewall
- Intrusion Prevention systems
- FIM
- SIEM
- Anti-malware solution
- Network monitoring and configuration management
- DB monitoring tool
- Firewall monitoring and auditing tool
- RHEL Subscriptions and content Management
- Linux configuration management
- Windows configuration management
- Configuration management
- Code repository
- Web application security testing
- Application Log viewer
- Multi-factor authentication solution, OTP generator
- Remote Secure Shell
- Backup management
- SAN fabric management and monitoring
- Personal Firewall Software
- Change control and asset management
- Monitoring infrastructure
- Key store / encryption

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? Yes No

If Yes:

Name of QIR Company:	Not Applicable.
QIR Individual Name:	Not Applicable.
Description of services provided by QIR:	Not Applicable.

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:
Ingenico France SAS	Physical Hosting Provider
Interxion Belgium	Physical Hosting Provider
Orange/mobistar	Physical Hosting 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:	Payment Processing – Internet, Payment Gateway/Switch, Clearing and Settlement, 3-D Secure Hosting Provider, System security services, IT support, Software development, Fraud and Chargeback, Merchant Services
----------------------------------	--

PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirement 1.2.3: IECS do not use wireless networks.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirement 2.1.1: IECS do not use wireless networks. Requirement 2.2.3: IECS do not use insecure protocols. Requirement 2.6: IECS is not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirement 3.4.1: IECS do not use disk encryption Requirement 3.6: IECS do not shares keys with their customers. Requirement 3.6.2: IECS do not distribute encryption keys. Requirement 3.6.6: IECS do not use manual clear-text cryptographic keys.
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirement 4.1.1: IECS do not use wireless networks.
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirement 6.4.6: IECS did not have any significant change that occurred within the past 12 months.
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirement 8.1.5: IECS do not allow third parties to access their CDE. Requirement 8.2.2: IECS do not allow non-face-to-face password resets. Requirement 8.5.1: IECS do not have remote access to customer premises.
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirement 9.6: IECS do not allow media distribution. Requirement 9.6.2: IECS do not allow media distribution. Requirement 9.6.3: IECS do not allow media distribution. Requirement 9.8.1: IECS do not have any other media present than hard disks. Requirement 9.9: IECS do not operate POI devices nor a Point of Sale. Requirement 9.9.1: IECS do not operate POI devices nor a Point of Sale. Requirement 9.9.2: IECS do not operate POI devices nor a Point of Sale. Requirement 9.9.3: IECS do not operate POI devices nor a Point of Sale.
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirement 11.1.1: IECS do not allow nor authorize wireless access points within or connected to their CDE. Requirement 11.2.3: IECS did not have any significant changes that required additional scans
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirement 12.3.9: IECS do not allow vendors nor business partners to access their CDE remotely.
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Appendix A1: IECS is not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Appendix A2: IECS do not operate POI devices nor a Point of Sale using SSL nor early TLS.

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:	<i>November 18, 2019</i>	
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 type="checkbox"/> Yes	<input checked="" 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

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *November 18, 2019*.

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**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>Ingenico eCommerce Solutions BVBA / SPRL</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>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 (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures, Version 3.2.1</i> , 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 my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS 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 DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)

<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Qualys</i>

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 3b. Service Provider Attestation



Signature of Service Provider Executive Officer ↑

Date: 3/12/2019

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:

Leonardo Polvora, Principal Security Consultant, was the Lead Assessor and Writer of the Report on Compliance.



Signature of Duly Authorized Officer of QSA Company ↑

Date: 03/12/2019

Duly Authorized Officer Name: Leonardo Polvora

QSA Company: Trustwave

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.

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify 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	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting 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"/>	

